

LANDesk® Management Suite 8.8

User's Guide




LANDesk[®]
An Avocent[®] Company



Copyright © 2002-2007, LANDesk Software Ltd. All rights reserved. LANDesk, Peer Download, and Targeted Multicast are either registered trademarks or trademarks of LANDesk Software, Ltd. or its affiliates in the United States and/or other countries. Avocent is a registered trademark of Avocent Corporation. Other brands and names are the property of their respective owners.

LANDesk and Avocent do not warrant that this document is error free and each retains the right to make changes to this document or related product specifications and descriptions at any time without notice. LANDesk and Avocent do not assume any obligation to update the information contained herein. This document is provided "AS IS" and without any guaranty, warranty, or license, express or implied, including but not limited to: fitness for a particular purpose, merchantability, non infringement of intellectual property, or other rights of any third party. Any LANDesk or Avocent products referenced in this document are not intended for use in medical, life saving, or life sustaining applications. Third parties may have intellectual property rights relevant to this document and the technologies discussed herein.

Contents

Cover	1
Contents	3
Introduction to LANDesk Management Suite 8	10
What's new in LANDesk Management Suite 8.....	10
What you can do with Management Suite 8.....	19
Where to go for more information.....	20
Using the console	21
Console overview	21
Starting the console.....	22
Changing the core server connection.....	22
Understanding the network view	23
Creating groups.....	26
Device icons	28
Viewing managed devices in the All Devices group.....	29
Shortcut menus	29
Configuring the network view with column sets	31
Toolbar options.....	33
Using console tools	34
Dockable tool windows.....	34
Saving window layouts.....	35
Find bar	36
Status bar	36
Viewing device properties	36
Monitoring devices for network connectivity.....	39
Hardware configuration	41
Intel* vPro support.....	41
Configuring Intel* vPro devices	43
Changing the password for Intel* vPro devices	52
Configuring System Defense policies.....	53
Intel* vPro Agent Presence configuration	55
Intel* Centrino Pro wireless support.....	57
Role-based administration	59
Role-based administration overview	59
Managing LANDesk users.....	61
Managing groups.....	64
Understanding rights	66
Creating scopes.....	72
Assigning rights and scope to users.....	75
Configuring services	76
Selecting a core server and database with General settings.....	76
Configuring the Inventory service.....	77
Configuring the scheduler service	80
Configuring preferred server credentials.....	82
Configuring the custom jobs service	82
Configuring the Multicast service	84
Configuring the OS deployment service.....	84
Configuring device agents	86
Working with agent configurations	86
Agent security and trusted certificates	90

Uninstalling device agents.....	93
Using LANDesk Server Manager and LANDesk System Manager with LANDesk Management Suite	93
Supported Linux/UNIX distributions	94
Installing Linux agents.....	95
Installing UNIX agents.....	98
Using the inventory scanner with Linux/UNIX	101
Console integration.....	103
Database queries.....	104
Queries overview.....	104
Query groups.....	104
Creating database queries	105
Running database queries	107
Importing and exporting queries.....	107
LDAP queries	108
Configure LDAP Directories	108
About the Directory manager window	109
More about the Lightweight Directory Access Protocol (LDAP).....	112
Managing inventory.....	114
Inventory scanning overview	114
Viewing inventory data	116
Tracking inventory changes	117
Using custom data forms.....	118
Using an off-core inventory server	121
Reports	123
Reports overview.....	123
Running and viewing reports.....	125
Publishing reports.....	126
Creating custom reports.....	129
Importing and exporting reports	134
Creating .CSV files	134
Scripts and tasks.....	136
Managing scripts	136
Scheduling tasks	137
Using the default scripts.....	142
Using the rollup core to globally schedule tasks	143
Using the local scheduler	144
Remote control	151
Using the remote control viewer.....	151
Changing device remote control security	157
Using remote control logging.....	158
Customizing the viewer and remote control agents	159
Troubleshooting remote control sessions	161
Software distribution.....	162
Software distribution overview.....	162
Setting up the delivery server.....	166
Distributing a package.....	170
Using MSI distribution packages.....	181
Distributing software to Linux devices.....	184
Troubleshooting distribution failures.....	185
Policy-based management.....	186
About policy-based management.....	186

Configuring policies	187
Setting up a package-building computer	191
Package-building overview	191
Running the Package Builder wizard	193
Uninstalling software distribution packages	194
Software license monitoring	197
Monitoring software license compliance	198
Creating product and vendor aliases	208
Editing software inventory	209
Exporting and importing software license monitoring data	212
Unmanaged device discovery	216
Unmanaged device discovery overview	216
Discovering unmanaged devices with UDD	217
Using extended device discovery (ARP and WAP)	219
What happens when a device is discovered	223
Deploying LANDesk agents to unmanaged devices	224
Restoring client records	225
OS deployment	226
OS deployment overview	226
OS image guidelines	228
Customizing images with Setup Manager and Sysprep	230
Agent-based deployment	231
Creating imaging scripts	232
Modifying scripts	234
Multicasting OS images	234
Viewing image status reports	236
PXE-based deployment	237
Using PXE representatives	237
Bootting devices with PXE	239
Understanding the PXE boot options	240
Troubleshooting	243
Provisioning	244
Creating provisioning templates	250
Provisioning - boot media	251
Sharing templates	251
Update templates	253
Importing installation scripts	254
Provisioning template variables	255
Provisioning Included templates	269
Provisioning Included By templates	269
Template properties	270
Provisioning history	270
Provisioning group	271
Profile migration	272
Profile migration overview	272
Profile content	273
Creating migration scripts with the OS Deployment/Migration Tasks wizard	278
Creating user-initiated profile migration packages	279
Running user-initiated profile migration packages	280
Executive dashboard	281
Executive dashboard overview	281
Configuring the executive dashboard	284

Managing local accounts	285
Local accounts overview	285
File replicator	289
Using the file replicator	289
Scheduling replication from the command-line	291
Managing Macintosh devices	294
LANDesk for Macintosh overview	294
Agent Configuration for Macintosh devices.....	295
Inventory for Macintosh devices.....	300
Software Distribution for Macintosh devices	302
Managed scripts for Macintosh devices	305
Remote control for Macintosh devices	306
Reporting for Macintosh devices.....	307
Scheduled tasks for Macintosh devices	307
Software license monitoring for Macintosh devices	307
Security and Patch Manager for Macintosh devices	308
Local scheduler for Macintosh devices	309
Managing a Macintosh device.....	309
Using the Mac remote control viewer	311
Security and Patch Manager	315
Looking ahead: What to do after configuring devices for LANDesk Security management	316
Security and Patch Manager overview.....	316
Role-based administration with Security and Patch Manager	319
Understanding and using the Security and Patch Manager tool window	321
Configuring devices for security scanning and remediation.....	330
Managing security content and patches.....	334
Downloading security content and patch updates.....	334
Viewing security and patch content.....	337
Searching for vulnerabilities by CVE names	337
Using filters to customize item lists	338
Viewing security information for a scanned device	338
Purging unused definitions	338
Working with patches	339
Downloading patches	339
Uninstalling patches	340
Using custom definitions	341
Creating custom definitions and detection rules	341
Scanning and remediating devices	346
Scanning devices for security risks	347
Remediating devices with detected security risks.....	355
Remediation methods	361
What happens on a device during remediation.....	364
Viewing security and patch information for scanned devices	364
Other security management tasks.....	367
Creating a scheduled reboot task.....	367
Using security alerts	367
Using security reports.....	368
LANDesk Network Access Control (NAC)	369
LANDesk Network Access Control overview	370
Understanding and selecting a LANDesk NAC solution	376
Using the LANDesk DHCP solution	379
Quickstart task list for setting up LANDesk DHCP	390

Setting up and configuring a remediation server.....	396
Setting up a LANDesk DHCP server.....	400
Configuring the LANDesk DHCP server with the LANDesk DHCP Manager tool	403
Using the Cisco NAC solution	413
Quickstart task list for setting up LANDesk integrated Cisco NAC	425
Setting up and configuring a dedicated posture validation server	429
Configuring compliance security criteria and publishing LANDesk NAC settings.....	433
Managing LANDesk NAC compliance security	445
Using the LANDesk IP Security solution	452
Using the LANDesk 802.1X solution	461
LANDesk Antivirus	474
LANDesk Antivirus overview	474
Configuring devices for LANDesk Antivirus protection.....	478
Updating virus definition files.....	480
Evaluating virus definition files with a pilot test	481
Backing up virus definition files	482
Scanning devices for viruses.....	482
Enabling real-time antivirus protection (file, email)	484
Configuring antivirus scan options with antivirus settings.....	485
What happens on a device during an antivirus scan.....	490
Viewing antivirus activity and status information.....	492
Using antivirus alerts	492
Generating antivirus reports	493
Viewing antivirus information in the Web console executive dashboard	493
LANDesk Host Intrusion Prevention System.....	494
LANDesk HIPS overview.....	495
Configuring devices for LANDesk HIPS protection	498
Protecting managed devices with LANDesk HIPS.....	500
Configuring LANDesk HIPS protection options with HIPS settings	501
What happens on a device configured with LANDesk HIPS.....	508
Viewing HIPS activity information.....	509
LANDesk Agent Watcher	511
LANDesk Agent Watcher overview	511
Enabling, configuring, and disabling Agent Watcher monitoring.....	513
Using Agent Watcher reports	515
Connection control manager.....	517
Using connection control configurations to restrict network access.....	518
Using device control configurations to restrict USB device access	521
Configuring alerts	528
Deploying configurations	528
Troubleshooting CCM	529
Asset manager add-on.....	531
Asset Manager overview	532
Accessing Asset Manager in the Web console	535
Managing assets	535
Working with computer assets	537
Working with software assets.....	540
Managing contracts	542
Managing invoices.....	543
Managing projects	543
Managing global lists.....	544
Creating new types.....	547

Using a details summary	548
Adding details	549
Adding detail tables	553
Managing detail templates	554
Adding detail templates	555
Using an item list	555
Adding items to the database	556
Using asset alert dates	557
Associating items	560
Importing items	561
Exporting items	562
Using Asset Manager reports	564
Monitoring with alerts	567
Using alerts	567
Configuring alert rulesets	571
Deploying alert rulesets	576
Viewing alert rulesets for a device	577
Viewing the alert log	578
Handheld Manager	579
Installing Handheld Manager	580
Using Handheld Manager	583
LANDesk Application Virtualization	591
LANDesk Inventory Manager	594
Appendix A: Additional inventory operations and troubleshooting	595
Scanning custom information	595
Specifying the software scanning interval and history	596
Appendix B: Additional OS deployment and profile migration information	606
Additional OS deployment procedures	606
Adding network adapter drivers to the Windows PE boot environment	612
Using the LANDesk imaging tool for DOS	613
Using the LANDesk imaging tool for Windows	616
Understanding the Windows PE preboot environment	619
Appendix C: Additional software distribution information	625
Scripting guide for .CFG files	625
Processing custom scripts	630
Troubleshooting .CFG files and their packages	633
Scripting guide for deployment scripts (.INI) files	634
Understanding software distribution error codes	636
Files used in script-based software distribution	640
Appendix D: Additional security scanner information	643
Appendix E: Context-sensitive help	649
LANDesk Antivirus help	649
Handheld Manager help	665
Inventory help	666
Local accounts management help	670
Configuring the LANDesk Management Gateway	671
Managed device help	673
OS deployment and Profile migration wizard help	697
Reports help	711
Role-based administration help	714
Scheduled tasks help	717
Security and Patch Manager help	722

Software distribution help	755
Using the Distribution package dialog	755
Using the Delivery methods dialog	759
Software license monitoring help	772
Unmanaged Device Discovery help	777

Introduction to LANDesk Management Suite 8

LANDesk® Management Suite 8 consists of tools you can use to help manage your Windows*, NetWare*, Macintosh*, Linux*, and UNIX* devices. Use these tools to distribute software packages, monitor software usage, deploy OS images and migrate profiles, remote control devices, detect and remediate security risks, and complete many other management tasks.

In this chapter, you'll learn more about Management Suite 8, including:

- What's new in this release
- What you can do with Management Suite 8
- Where to go for more information

What's new in LANDesk Management Suite 8

LANDesk Management Suite 8, version 8.8 adds these enhancements:

- **New quickstart guides and wizards:** New LANDesk Management Suite quickstart guide (in the same folder on the CD as the documentation PDFs) to help new users get started with Management Suite. The Windows console also includes quickstart wizards to help step you through some important configuration tasks.
- **Software license monitoring:** You can now deny application launch for specific Active Directory or LANDesk groups.
- **Application policies:** Improved Web-based software deployment portal that runs on managed devices. The portal can run at logon and it shows users available policies. You can now include multiple packages in a single policy and you can apply multiple policies to a single target. You can also now make policies both required and optional, so users can optionally reapply a policy. You can now associate an uninstall package with a policy, so when a policy no longer applies, the associated uninstall package runs.
- **Software distribution:** Package shares now support HTTP authentication for Windows devices. You can also now install packages as the logged-in user or system.
- **Local scheduler:** Local scheduler configuration has been redesigned and now includes a randomizer for start times and new execution filters, such as screensaver active, desktop locked or unlocked, no user logged in, and so on.
- **New LANDesk alerting system:** Replaces AMS (alert management system) from earlier releases. Enterprise-scalable alert system that categorizes alerts for easier use. Leverages the Avocent Management Platform.
- **Mac improvements:** Mac OS X 10.5 (Leopard) support. Application, package, driver, and plug-in information is now gathered through the System Profiler. Agent uninstaller is now moved to the core server to prevent users from removing the management agents.
- **New Macintosh remote control viewer:** New Macintosh remote control viewer application that can control both Macintosh and Windows devices.

- **Reports:** New return on investment report to help show the value of LANDesk products in your organization. The report captures successful software distributions, antivirus and spyware handling, patch deployment, and remote control sessions. You can associate a cost with each of these and view a graphical savings report.
- **LANDesk Intel vPro support:** OEM-enabled AMT provisioning without IT intervention. End-user notification of AMT policy enforcement on system.
- **Provisioning:** Over 100 provisioning templates (70 of which are Dell-specific). New action handlers including join a domain, recursive copy and delete, and pause. You can now provision ESX hosts. Improved Vista support.
- **Automated patch deployment with LANDesk Process Manager:** LDMS 8.8 includes a limited version of LANDesk Process Manager 4.1. Process Manager enables you to fully automate the deployment of security updates and patches. You configure the required settings from the Download Updates dialog in Security and Patch manager. A brief tutorial, ProcessManagerTutorial.exe is also available from this dialog, or it can be launched from \Program Files\LANDesk\ManagementSuite.
- **Enhanced LANDesk HIPS capabilities:** Administrators can configure more HIPS options in the main console and deploy them to managed devices, including: buffer overflow protection, whitelists (applications allowed to execute on managed devices), file protection rules, and more.
- **Enhanced Security and Patch Manager features:** You can now add custom products to your custom vulnerability definitions and perform test scans on pilot groups of target devices. Also, you can use definition group settings to automate how security content (definitions and patches) that matches specified type and severity criteria are downloaded, their scan status, and the download location.
- **New LANDesk Antivirus information views:** LANDesk Antivirus has new views in the Antivirus activity and status window including: antivirus activity by virus, quarantined infections by computer and by virus, and trusted items by computer that shows what an end user has added to their trusted items list. Also, you can schedule security scans to run at a random time in order to ensure devices that aren't connected to the network during the regularly scheduled scan time are scanned when they reconnect to the network.
- **LANDesk 802.1X Network Access Control scanning and remediation:** LANDesk 802.1X NAC now allows you to not only scan 802.1X-enabled devices and enforce authentication, but also determine health status according to your compliance security policies, allow access to healthy devices, block access and quarantine unhealthy devices, and perform remediation on those devices in order to achieve healthy status and network access.
- **WAP device discovery with the extended device discovery tool:** The extended device discovery tool now lets you configure devices to listen for WAP signals (in addition to ARP broadcasts) to discover wireless access point (WAP) devices within range of your network. You can use both the ARP-based discovery and WAP-based discovery methods.
- **Enhanced Connection Control Manager features:** CCM now includes an encryption utility you can use to protect confidential data. Also, you can make USB storage devices and CD/DVD devices read only.

LANDesk Management Suite 8, version 8.7.3 (SP3) adds these enhancements:

- **Provisioning** : A full working version of the provisioning component is included in SP3. The provisioning interface is now enabled by default. See [Provisioning](#).
- **Application virtualization**: Added support for LANDesk Application Virtualization, a LANDesk Management Suite add-on product that is sold separately by LANDesk Software. LANDesk Application Virtualization uses Thinstall technology to virtualize an application, storing it in a single self-contained executable with the application and .DLL/device driver dependencies. When you use LANDesk Application Virtualization with Management Suite, you can deploy and manage virtualized applications. See [LANDesk Application Virtualization](#).
- **LANDesk HIPS**: LANDesk Host Intrusion Prevention System (HIPS) provides an additional layer of protection that proactively secures systems and applications from zero-day attacks. Using customized rules and file certifications HIPS monitors applications and blocks prohibited actions and behaviors, allowing you to protect the file system, registry, system startup, and even detect stealth rootkits. See [LANDesk HIPS](#).
- **New LANDesk Trusted Access solutions**: Two additional network access control solutions offer greater flexibility in implementing compliance security. LANDesk IP Security leverages built-in certificate-based authentication by assigning its own signed certificates to postured devices that either allow or deny access to the network. LANDesk 802.1X is a Radius proxy solution that can be implemented on a network with an 802.1X infrastructure in order to provide authentication by validating an active standard LANDesk agent on devices connecting to the network.
- **Enhanced LANDesk Antivirus capabilities**: LANDesk Antivirus is supported on additional device platforms including: Windows XP 64-bit, Windows Vista 32-bit and 64-bit. Install and update tasks can be configured with reboot settings. Also, administrators can configure LANDesk Antivirus client options so that end users can view and create local scheduled antivirus scan tasks on their own machines.
- **Improved OSD Windows PE management**: You can now add and remove drivers in Windows PE boot environments.
- **Macintosh OSD support**: Macintosh OS deployment support is included in SP3. For more information, download the operating system deployment for Macintosh white paper from <http://www.landesk.com/support/downloads/Resource.aspx?pvid=66&rtid=9>.
- **Windows Vista additional console support**: You can now install additional consoles on Windows Vista 32-bit.
- **Improved Management Gateway hardware support**: The Management Gateway now prompts for drivers for unrecognized network and storage devices.
- **Asset Manager global filters**: LANDesk Administrators can now control user access to asset information by creating a filter based on a global list and then assigning the filter to users.

LANDesk Management Suite 8, version 8.7.2 (SP2) adds these enhancements:

- **Provisioning:** A preview of the Provisioning component is included in SP2.
- **New agent configuration RBA right:** Lets users view the agent configuration tool, create and edit agent configurations, and schedule agent configuration tasks.
- **IP address-only rollup:** Rollup Utility has a new option (enabled through a registry key) to only roll up IP addresses. This can be helpful in environments that need up-to-date IP address info, such as help desks.
- **Macintosh:** Inventory scanner now uses encryption and delta scanning. Support for custom data via XML files. Support for software license monitoring automatic application discovery.
- **OS deployment:** Added dialogs allowing users to add drivers to a windows PE image, resize a Windows PE image, and change the wallpaper in a Windows PE image. Added support for Windows Vista images in the Windows PE boot environment.
- **Software distribution:** Added a **Published distribution packages** item to the **Distribution packages** tree. This contains published distribution packages from a rollup core. LDAP groups are now resolved at the device rather than through a query, so administrators don't have to wait for a query to resolve.
- **Security and Patch Manager:** Forward vulnerability scan results to a rollup core in order to facilitate real-time status. Extended Device Discovery (EDD) is no longer required on remote devices in order to monitor their LANDesk services and agents with Agent Watcher.
- **Connection control manager:** Administrators can use a password to override the blocked USB devices on a managed device.

LANDesk Management Suite 8, version 8.7.1 (SP1) adds these enhancements:

- **New software distribution job deferral options:** Distribution jobs can have user-configured deferral times, a dialog on managed devices indicating job success or failure, and customizable deferral dialog text. See [About the feedback and timing page](#).
- **Improved task targeting:** You can now use LDAP group objects as task targets.
- **New software license monitoring automatic product generation:** The inventory scanner now gathers information on installed applications and uses that information to automatically add monitorable products to software license monitoring. Also, file version is now used to identify product files. See [Associating files with products](#).
- **Compliance security scans:** With Security and Patch Manager you can create and configure compliance-specific security scans that check target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task, a policy, and even initiated by LANDesk Antivirus when a virus is detected that can't be removed or quarantined.
- **Enhanced LANDesk Antivirus capabilities:** LANDesk Antivirus now lets you: scan target devices for risky software (via an extended database); automatically detect and uninstall certain third-party antivirus products when deploying LANDesk Antivirus to managed devices; automatically quarantine a device that has a virus that can't be removed; as well as configure LANDesk Antivirus client options so that end users can pause antivirus scans, temporarily disable real-time file protection, right-click files and folders to run an antivirus scan, and add and remove files and folders they don't want to scan to their trusted items list.

- **Enhancements for managing Macintosh devices:**
 - Hardware scans now include chassis type, primary owner, memory slots, and LDAP locations (version 10.3 and later).
 - Inventory now uses 9535 protocol. The new protocol should be faster, more reliable, and more secure than using ports 1760 and 1761.
 - Remote control feature **Reduce the color depth** now supported.
 - Security and patch manager now support stage and repair, multi-cast for patch remediation, policy-base remediation, policy-based security scanning, and custom vulnerability support (detection and remediation for files only)

LANDesk Management Suite 8, version 8.7 adds these enhancements:

- **New global scheduler:** Scheduled tasks on a rollup core are automatically delegated to source core servers for processing. See [Using the rollup core to globally schedule tasks](#)
- **Rollup core replication:** Replicate rollup core queries, distribution package configurations, and delivery method configurations to source core servers. See [Replicating rollup core data to source cores](#).
- **Console grouping:** You can now create custom package and scheduled task groups to help organize your configurations.
- **Dynamic preferred servers:** Provides load-balancing and fault tolerance for enterprise package distribution. Also supports credentials for UNC package locations so there's no more need for null-session shares. See [Configuring preferred package servers](#).
- **Software distribution run from source:** You can now configure devices to install a package from the source without downloading the entire package locally first. Provides native support for deploying applications like Microsoft Office* in the way that Microsoft recommends. See [Running packages from the source server](#).
- **Software distribution Linux dependencies:** When you create a Linux RPM-based distribution package, you can now view Linux file/library dependencies defined by that RPM package. You can then configure dependent packages to be installed automatically.
- **New OS deployment preboot environments:** Microsoft Windows PE and Linux are now supported as OS deployment preboot environments. Windows PE supports Microsoft XImage and the new .WIM format. These two environments can potentially image much faster than DOS-based imaging. See [OS deployment](#).
- **Refined remote control rights:** Management Suite RBA now supports refined remote control rights, so you can limit on a per-user basis the ability to access individual remote control features like file transfer and program execution. You can also limit remote control access by time of day. See [Role-based administration](#).
- **Extended device discovery:** Provides real-time ARP-based discovery of network devices. Allows you to discover devices on the network even if they're firewalled or otherwise unpingable. See [Using extended device discovery](#).
- **Database and inventory server improvements:** New database support for Oracle 10g* and Microsoft SQL Server* 2005. New multithreaded inventory service, and the option of running the inventory service on a computer other than the core server. See [Using an off-core inventory server](#).
- **Handheld and Embedded Device Manager improvements:** New support for Windows Mobile* 5 and new thin client platform support. See [Handheld manager](#).
- **Software license monitoring:** On-demand compliance calculation and reporting substantially increases the console performance.

- **LANDesk Antivirus:** LANDesk Antivirus is available in both LANDesk Management Suite and LANDesk Security Suite as a fully integrated security management tool (requires a security content subscription). LANDesk Antivirus protects your managed devices with on-demand, configurable antivirus scans as well as real-time file and email protection. Automate the tasks of downloading the most current virus definition (pattern) file updates, and scanning managed devices for known viruses and suspicious files. Antivirus alerts and reports are available. You can also view antivirus results for scanned devices in the console and in the LANDesk Executive Dashboard. See [Using LANDesk Antivirus](#).
- **LANDesk Agent Watcher:** Actively monitors the status of LANDesk agent services and files on managed devices. With Agent Watcher, you can configure which critical services and files are monitored. Agent Watcher reverses and reports unauthorized changes. See [Using LANDesk Agent Watcher](#).

LANDesk Management Suite 8, version 8.6.1 adds these enhancements:

- **New executive dashboard tool:** Consists of a series of widgets (informative charts, diagrams, dials, and meters that enables executives to monitor the health or status of their business, including vulnerabilities, security threats, spyware, licensing, usage statistics, and so on). This enhanced visibility of the business allows executives and IT managers to make informed management decisions and quickly respond to critical issues. See [Using the executive dashboard](#).
- **Enhanced software distribution:** Software distributions can include preliminary and final packages that get distributed as a single task. These additional packages can be useful when you need to run commands or programs before or after the main package. See [Using multiple distribution packages in a task](#).
- **Enhanced connection control manager:** You can now apply different connection control configurations based on whether a computer is connected to a listed or unlisted network. See [Applying device configurations to network connections](#).
- **Improved LANDesk DHCP trusted access:** DHCP routing and posture validation functionality have been consolidated on a single LANDesk DHCP server, making this solution even more cost efficient and easy to implement. New features included with the LANDesk DHCP trusted access solution let you configure network access control at specific platform levels with operating system filters, view scanned device health status, and monitor the DHCP server and send notifications. Additionally, Macintosh devices can now be scanned for compliance with your security policies, and detected security exposures remediated if necessary, before being allowed access to the corporate network. See [Using the LANDesk DHCP solution](#).

LANDesk Management Suite 8, version 8.6 adds these enhancements:

- **New LANDesk® Trusted Access™ tool:** Adds endpoint compliance security to your network. Lets you configure custom compliance security policies using the Security and Patch Manager tool, and enforces those policies on devices attempting to access your network through a posture validation process. Healthy devices are granted access while unhealthy devices are quarantined, where they can be remediated and granted full access or given limited network access. Trusted access requires additional hardware and software setup and a strong practical knowledge of network routing and DHCP services. LANDesk offers two trusted access solutions: a Cisco NAC integrated solution, and a LANDesk DHCP server-based solution.
- **Enhanced Security and Patch Manager:** New enhancements to the Security and Patch Manager tool include: real-time spyware detection and removal, frequent security scanning for high-risk threats, antivirus support via scanner and pattern file checking, firewall state detection and configuration, configurable security threat definitions through custom variables, vulnerability supercedence and dependencies notification, security scanning by custom groups, ability to divide scheduled repair jobs into staging and deployment tasks, custom alerting, new reports, additional security content types, additional supported languages, and more.
- **New LANDesk Management Gateway:** The Management Gateway lets you manage users that are outside of your corporation, without putting holes in your firewall. Includes support for remote control, software distribution, inventory, software license monitoring, and more.
- **Improved software distribution:** Support for Linux RPM software distribution. Task targeting has been improved so you can target combinations of queries, device groups, and specific devices. Management Suite automatically resolves duplicates so the same device won't get the job multiple times if it's targeted more than once.
- **Improved remote control:** Improved keyboard mapping, so special characters that you type locally appear on the target device correctly. Improved remote screen blanking is now part of the mirror driver. Other applications won't override the screen blanking once it's enabled. Remote controlling devices running older agent versions now works better from the Web console.
- **Improved connection control manager:** Includes more granular control of USB devices, including the ability to create custom rulesets. Supports Bluetooth* restrictions.
- **New report engine:** Integration of Active Reports for producing reports (Crystal reports is no longer supported).
- **Enhanced reports tool:** Additional predefined reports provided. Create custom report templates with the report designer. Added a charting tool to provide a graphical representation of the data. Schedule reports to be published and e-mailed to recipients. See [Using reports](#).
- **New local accounts management:** An administrative tool used to manage the users and groups on local machines on your network. From the console, you can add and delete users and groups, add and remove users from groups, set and change passwords, edit user and group settings, and create tasks on devices. See [Managing local accounts](#).

LANDesk Management Suite 8, version 8.5 adds these enhancements:

- **Improved software distribution:** Redesigned software distribution interface makes it much easier to create distribution packages and package delivery methods. Package chaining enables administrators to define package dependencies and automatically install prerequisite software packages. Expanded task status reporting provides greater insight into deployment status, successes, and failures. See [Using software distribution](#).
- **Redesigned and expanded Security and Patch Manager tool:** This tool is now installed by default with Management Suite to let you scan managed devices, as well as core servers and console machines, for LANDesk software updates. You can also create your own custom security definitions to scan devices for specific, potentially threatening conditions. In order to take full advantage of the tool's security scanning and remediation capabilities (including protection from known vulnerabilities for Windows, Macintosh, and Linux; spyware; Windows configuration security threats; and more), you must purchase a separate LANDesk Security Suite content subscription. With the appropriate subscription, you can download the latest known vulnerability definitions and required patches and use them to create and run custom security scan and remediation tasks, all from the Management Suite console. Configure whether the security scanner displays on end user devices during scan and repair processes, device reboot options, and the level of user interaction. You can also view comprehensive security and patch information for scanned devices. See [Using the Security and Patch Manager tool](#).
- **New Connection Control Manager tool:** Monitors and restricts access to managed devices through network connections and I/O devices. You can restrict the network IP addresses that devices are allowed to connect with, and you can also restrict the use of devices that allow data access to the device, such as ports, modems, drives, USB ports, and wireless connections. See [Using connection control manager](#).
- **Improved remote control:** Application layer remote control provides greater stability and improved performance. New remote control viewer is easier to use, offers "view only" support, and provides screen draw tools for remote training and problem resolution. See [Administering remotely](#).
- **New report publishing:** Report publishing capabilities enable you to schedule and automatically generate reports in .HTML, .PDF, .DOC, .RTF and .XLS formats, and publish those reports to a secure file share where they can be viewed by anyone to whom you've provided the required access credentials. See [Using reports](#).
- **Enhanced inventory:** The inventory scanner now supports SMBIOS 2.1 and above, and provides greater detail, including memory and expansion slot data, network adaptor settings, drive information, and plug-and-play monitor details.
- **Improved software license monitoring:** Expanded software license monitoring features include predefined applications list and compliance tracking by group, department, and organizational unit. See [Using software license monitoring](#).
- **New software portal:** Gives users self-service access to policy-based application packages from their own desktop. See [Using the local software deployment portal](#).
- **New LANDesk file replicator:** Allows you to easily replicate data hosted on Web servers. See [Using the file replicator](#).

LANDesk Management Suite 8, version 8.1 adds these enhancements:

- **Enhanced inventory:** Launch an immediate inventory scan on a device by right-clicking the device and clicking **Inventory**. Also, the inventory scanner now collects the operating system language on devices.
- **Improved software distribution:** Software distribution now works better through firewalls, and you can now disable task completion on software distribution jobs, so if the job fails it isn't automatically retried.
- **Improved Web console:** Use software license monitoring from the Web. See [Monitoring software license compliance](#).
- **Enhanced application policy management reliability:** Whenever a device checks with the core server for tasks or policies, the core server updates that device's IP address in the core database, avoiding problems with outdated IP addresses that may be part of an old inventory scan.
- **Improved scheduled task support:** Provide multiple logins for the scheduler service to authenticate with when running tasks on devices that don't have Management Suite agents. This is especially useful for managing devices in multiple Windows domains. See [Configuring the scheduler service](#).
- **New custom local scheduler tasks:** Use the Management Suite local scheduler on devices to remotely schedule a recurring task. See [Configuring local scheduler scripts](#).
- **Enhanced remote control:** Store detailed remote control logs in the database. Log information includes who initiated the remote control session and the remote control tasks (file transfers, chat, and so on) they did on the device. Also, remote control sessions now pass 3rd mouse button/wheel movement to devices. See [Using remote control logging](#).
- **Enhanced unmanaged device discovery:** Generate reports on the unmanaged devices on your network. For more flexibility, you can now use an Unmanaged Device Discovery task to rediscover managed devices. This is useful if you've reset your database. See [Restoring client records](#).
- **New LANDesk Asset Manager 8 Add-on:** Record and keep track of your critical IT assets such as hardware, software, office equipment, and other physical assets, in addition to invoices, lease agreements, and other associated business documents and information. Create and use customized data entry forms to add items to the database. Reconcile the existence and location of IT assets with financial records. See [Using the Asset Manager add-on](#).
- **Improved Patch Manager 8 Add-on:** You can now create custom vulnerability definitions to check for security risks before a patch is available. Also, you can scan for vulnerabilities on Mac OS X and Sun Solaris devices. See [Using the Security and Patch Manager tool](#).

LANDesk Management Suite 8, version 8.0 adds these enhancements:

- **Improved database:** New single database schema with improved data integrity and scalability.
- **Role-based administration:** Add Management Suite users and configure their access to Management Suite tools and managed devices based on their administrative role in your network. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform. See [Role-based administration](#).
- **Software Distribution improvements:** Enhancements include byte-level checkpoint restart for interrupted downloads, peer download, dynamic bandwidth throttling that limits distribution bandwidth when devices need network bandwidth, and multi-file MSI multicast package support. See [Using Targeted Multicasting with software distribution](#) and ["About byte-level checkpoint restart and dynamic bandwidth throttling"](#).
- **New Unmanaged Device Discovery feature:** Discover unknown and unmanaged devices on your network through a directory service, domain discovery, or layer 3 ping sweep. Alerts notify you of newly discovered devices. Schedule device discovery so you can constantly be aware of new devices. See [Using Unmanaged Device Discovery](#).
- **Enhanced device security:** Certificate-based model allows devices to only communicate with authorized core servers and consoles. See [Agent security and trusted certificates](#).
- **New on-demand remote control:** Optional and highly secure on-demand remote control model only loads the remote control agent on devices for the duration of an authorized remote control. See [Deploying remote control](#).
- **New reports:** Over 50 new predefined Management Suite service reports for planning and strategic analysis. See [Managing inventory and reports](#).
- **New console interface:** New console design with dockable tool windows, network view, custom layouts, and more. See [Using the LANDesk Management Suite console](#).
- **Additional Macintosh computer feature support:** Targeted Multicast, Application Policy Management, and Software License Monitoring for Mac OS* X devices. See [Managing Macintosh devices](#).

What you can do with Management Suite 8

With Management Suite 8, you can:

- Use the LANDesk Management Suite console to configure and manage your network. See [Using the LANDesk Management Suite console](#).
- Create and manage queries on inventory data and LDAP directories. See [Using queries](#).
- Manage inventories, track inventory changes, create forms to gather custom data from devices, and view detailed reports. See [Managing inventory](#) and [Using reports](#).
- Diagnose and troubleshoot problems on remote devices from the console. You can remote control, reboot, execute files, and transfer files to devices. See [Administering remotely](#).
- Quickly distribute software to all of your network users. See [Using software distribution](#).
- Use a Web-based console to access key Management Suite features from anywhere you have a browser. See [Using the Web console](#).

- Monitor software licenses and compliance, and track software usage and denial trends. Also edit the core database's software list, LDAPPL3.INI, that the inventory scanner uses to identify device applications. See [Using software license monitoring](#).
- Deploy OS images and migrate user profiles. See [Using OS deployment](#) and [Using profile migration](#).
- Create application policies based on core database queries. Devices targeted by policies automatically receive application sets. See [Using policy-based distributions](#).

Where to go for more information

Refer to the *LANDesk Management Suite Installation and Deployment Guide* for:

- Finding out system requirements
- Installing Management Suite
- Activating the core server
- Upgrading from previous versions of Management Suite
- Installing LANDesk add-on products

Using the console

LANDesk Management Suite provides a full range of system management tools that let you view, configure, manage, and protect devices on your network. All of these tasks can be performed via a single console. This chapter introduces the console interface and describes how to configure and navigate the console's network view and tool windows.

Read this chapter to learn about:

- "Console overview" on page 21
- "Starting the console" on page 22
- "Changing the core server connection" on page 22
- "Understanding the network view" on page 23
 - "Creating groups" on page 26
 - "Device icons" on page 28
 - "Viewing managed devices in the All Devices group" on page 29
 - "Shortcut menus" on page 29
 - "Configuring the network view with column sets" on page 31
 - "Toolbar options" on page 33
- "Using console tools" on page 34
- "Dockable tool windows" on page 34
- "Auto hide" on page 35
- "Saving window layouts" on page 35
- "Find bar" on page 36
- "Status bar" on page 36
- "Viewing device properties" on page 36
- "Configuring agent discovery" on page 37
- "Monitoring devices for network connectivity" on page 39

Console overview

The power of the console is that you can perform all critical network management functions from one convenient location, freeing you from the need to go to each managed device to perform routine maintenance or to troubleshoot problems. From a single console, you can distribute and update software or configuration settings, diagnose hardware and software issues, deploy OS images and migrate user profiles, use role-based administration to control user access to both features and devices, use remote control features to train end users or resolve problems.

You can have multiple core servers and databases to accommodate your specific network management needs. For information on installing a core server and console, additional consoles, Web console, and managing multiple core servers and databases, refer to the *Installation and Deployment Guide* (this guide is available as a printable PDF document).

Continue reading this chapter to learn how to navigate and use the console to view and organize devices and access the various management tools. (Each tool, such as software distribution, remote control, security and patch Manager, etc, are described in-depth in subsequent chapters in this guide.)

Starting the console

To start the console

1. Click **Start | Programs | LANDesk | LANDesk Management Suite**. (The actual program name may be different depending on the LANDesk product that's installed and the license used to activate your core server.)
2. Enter a valid user name and password.

If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

3. Select the core server you want to connect to. The user must have proper authentication credentials to that core server.
4. Click **OK**.

The console opens with the layout (size, position, open tool windows, etc.) that was being used the last time this user logged out.

For additional consoles, the credentials you use to log into Management Suite must match the credentials used for any drives you have mapped to the core server. Otherwise, you might see a "Multiple connections" error in the console login dialog.

About the Login dialog

Use this dialog to launch the console and connect to a core server.

- **Username:** Identifies a LANDesk user. This might be an administrator user or some other type of user with restricted access (see "Role-based administration" on page 59). The user must be a member of the LANDesk Management Suite group on the core server. Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).
- **Password:** The user's password. (**Note:** If a LANDesk Administrator changes the password of another user, for example an additional console user, the new password does not take affect until that user reboots their console. At that point, the user would enter their new password to log into the console.)
- **Core server:** Specifies the core server you want to connect to. This drop-down list is the same as the core server drop-down list available on the console toolbar.

Changing the core server connection

The console lets you view and manage the contents of any database associated with a core server that you can connect to on your network. This allows you to create databases for different sites, organizational units, or logical internal networks.

You can only be connected to one core server at a time.

To change core server connections

1. Select a core server from the **Core** drop-down list located on the console toolbar. Or, enter a core server name in the text box and press **Enter**.

The server is searched for on your network. If found, you're prompted to log in at the standard Login dialog.

2. Enter a valid user name and password.

Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

Once you've connected to a core server, its name is automatically added to the **Core** drop-down list in the toolbar.

Understanding the network view

The network view is the main window of the console and is the starting point for most functions. This is where you view device's inventory data, create queries to search for and group devices, select devices to remote control, and so on.

The network view window is always open and contains two panes. The left-hand pane shows a hierarchical tree view of the core server/database you're currently connected to and its **Devices**, **Queries**, and **Configuration** groups. You can expand or collapse the tree objects as needed. The right-hand pane in the network view displays a detailed list of the selected group's devices, queries, or configuration items, depending upon which type of group you've selected.

Group icons

The following icons are used to represent different group types in the network view:

- **Blue folder:** Indicates public and private groups.
- **Double yellow folders:** Indicates public groups that contain a comprehensive list of items of a specific type, such as **All Devices**.

You can resize the network view window and its panes and columns, but you can't close it. The network view window is not dockable like the tools windows.

Role-based administration

The devices you can view and manage in the network view, and the management tools you can use, are determined by the access rights and device scope assigned to you by the administrator. For more information, see "Role-based administration" on page 59.

The **Network View** contains the following groups and subgroups:

Core

The **Core** object identifies the core server you're currently connected to. The **Core** object is located directly under the network view root and can be collapsed and expanded.

Core object name syntax

The syntax for the core object name is:

Server Name\Database Instance

Devices

The **Devices** group contains the following device subgroups.

- **My devices:** Lists devices for the currently logged-in user, based on the user's scope. A user can create device subgroups only under **My devices**. Users can add devices to their **My devices** group, or any of its subgroups, by copying them from the **Public devices** and **All devices** groups. Users can also click and drag devices from **Public devices** and **All devices** into their **My devices** group.

Dragging and dropping items in the network view

When you click an item in order to drag it to another group in the network view, the cursor indicates where you can and can't drop the item. As you move the cursor over a group object, a plus-sign (+) indicates that you can add the item to that group; and a cross-out sign indicates that you can't add the item to that group.

- **Public devices:** Lists devices an administrator (a user with the LANDesk Administrator right) has added from the **All devices** group. An administrator sees all of the devices in this group, while other users see only the devices allowed by their scope. Also, only an administrator can create a subgroup under **Public devices**.
- **All devices:** Lists all devices that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). For an administrator, **All devices** lists all managed devices that have been scanned into the core database. Devices configured with the standard LANDesk agent automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner.

For regular users, All Devices is a composite of their user's **My devices** and **Public devices** groups.

Administrators and users can run asset reports on the devices in this group.

You can also manually add computers to the network view by right-clicking the **All devices** group, selecting, clicking **Insert new computer**, filling in the device and network information, and clicking **OK**. These computers also appear in the User added computers subgroup under the Configuration group.

- **User devices:** Lists all of the devices in the core database, organized into user subgroups. User subgroups are named with user login IDs (i.e., computername\user account, or domain\user account). Each user group contains the devices that appear in that user's **My devices** group.

Note that ONLY administrators can see the **User devices** group and its subgroups. Other users do not see the **User devices** group at all.

Queries

The **Queries** group contains the following query subgroups.

- **My queries:** Lists queries either created by the currently logged-in user, or added to the user's **User queries** group by an administrator. A user can create, modify and delete query groups and queries under their **My queries** group. They can also copy queries to this group from the **Public queries** group.

Any query a user runs is limited to the range of devices defined by the user's scope. For example, if a user's scope is **All machines**, the query will search all devices in the core database, but if the user's scope is restricted to 20 machines, only those 20 machines will be searched by the query. For more information on creating queries, see "Creating database queries" on page 105.

- **Public queries:** Lists queries that an administrator, or a user with the Public Query Management (PQM) right, has added. Only users with the LANDesk Administrator right or the PQM right can add, modify, or delete query groups or queries in the **Public queries** group. However, all users can see the queries in this group, and can copy them to their own **My queries** group.
- **All queries:** Lists all queries that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). **All queries** is a composite of the user's **My queries** and **Public queries** groups.
- **User queries:** Lists all queries in the core database, organized into subgroups by user. User subgroups are named with their login IDs (i.e., computername\user account, or domain\user account). Each user group contains the queries that appear in that user's **My queries** group.

Note that ONLY administrators can see the **User queries** group and its subgroups. Other users do not see the **User queries** group at all.

Administrators can use this group to run a user's queries against that user's scope, as if they were that user. In this way, an administrator can preview exactly the results a user will see when they run a query.

Configuration

The **Configuration** group contains the following configuration groups.

- **PXE holding queue:** Lists PXE holding queues and the devices that are waiting in the PXE holding queue. For more information, see "Using the PXE holding queue" on page 242.

- **Multicast domain representatives:** Lists configured multicast domain representatives that can be used for software distribution load balancing. For more information, see "Using Targeted Multicast with software distribution" on page 178.
- **PXE representatives:** Lists devices configured as PXE representatives that can deploy OS images to devices in their subnet. For more information, see "Using PXE representatives" on page 237.
- **Pending unmanaged client deployments:** Lists devices that have been discovered by the Unmanaged Device Discovery tool, and are waiting for an agent configuration task. For more information, see "Unmanaged device discovery" on page 216.
- **User added computers:** Lists computers that have been added manually to the network view via the Insert new computer dialog (right-click the **All devices** group).

Creating groups

Groups help you organize devices and queries in the console's network view. You can create groups to organize network devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a marketing group for all devices in the marketing department or a group that includes all devices running a specific OS.

Rules for creating groups

- **My devices and My queries:** Administrators and all other users can create groups under **My devices** and **My queries**.
- **Public devices:** Only administrators can create groups under **Public devices**.
- **Public queries:** Only administrators or users with the Public Query Management (PQM) right can create groups under **Public queries**.
- **All devices and All queries:** There are no subgroups in **All devices** or **All queries**. Users, including administrators, cannot create groups under **All devices** or **All queries**.
- **User devices:** Only administrators can create groups under the user-specific subgroups in **User devices**.
- **User queries:** Only administrators, and users with the Public Query Management (PQM) right, can create groups under the user-specific subgroups in **User queries**.

To create a group

1. In the console's network view, right-click the parent group (such as **My devices**), and then click **New group**. Or, select the parent group, and then click **Edit | My Devices | New Group**.
2. Type in a name for the new group, and then press the **Enter** key.

You can right-click groups to perform various tasks, based on the type of group. For example, if you created a device subgroup, its shortcut menu lets you:

- Add devices
- Create a new subgroup
- Run an inventory report
- View as a report
- Cut

- Copy
- Paste
- Remove
- Rename









For more information on right-click features, see "Shortcut menus" on page 29 below.



Device icons

Device icons display in the console's network view and show the current agent and health status of a device.

You can update the agent and health status for devices one at a time as you select them in the network view, or for all of the visible devices in the network view at the same time. You can also update a device's status by selecting it and clicking the Refresh toolbar button. For information on configuring how agent discovery is handled, see "Configuring agent discovery" on page 37 later in this chapter.

The following table lists the possible device and status icons and what they mean:

Icon	Type and description
	Server: Represents a server device.
	Windows device: Represents a Windows device.
	Macintosh device: Represents a Macintosh device.
	Handheld device: Represents a handheld device.
The status icons below can display next to the device icons listed above, depending on the device's current configuration and status.	
	Not available: Indicates the device is not currently available to the console.
	Unknown: Indicates the status of the device is not currently known. This icon appears briefly while the device status is being updated.
	Standard LANDesk agent: Indicates the standard LANDesk agent is loaded on the device.
	Remote control: Indicates the remote control agent is loaded on the device.

Icon	Type and description
	Warning: Indicates a health warning for the device. A health status icon can appear only if the LANDesk System Manager agent is loaded on the device.
	Critical: Indicates a critical health status for the device. A health status icon can appear only if the LANDesk System Manager agent is loaded on the device.

Icon display quality

These are high-color icons and require at least a 16-bit color-depth setting. If the icons in your console appear out of focus, change your color settings in the Windows Display Properties.

If your firewall blocks UDP packets

If you manage devices through a firewall that blocks UDP packets, you won't be able to use these device shortcut menu features: **Wake Up**, **Shut Down**, **Reboot**, and **Inventory Scan**.

Viewing managed devices in the All Devices group

Devices running LANDesk agents automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during a device's initial agent configuration. Once a device is scanned into the core database it is considered to be a managed device. In other words, it can now be managed by that core server. For more information on setting up devices, see "Configuring device agents" on page 86.

Because the **All devices** group is populated automatically, via an inventory scan, you may never need to manually discover devices. However, to discover devices not already in the core database, you can scan the network for devices with the unmanaged device discovery tool. For more information, see "Unmanaged device discovery" on page 216.

When connected to a particular core server, the administrator can see every device managed by that core server. Regular users, on the other hand, are restricted and can only see the devices that reside within their assigned scope (a scope is based on either a database query or a directory location). For more information, see "Role-based administration" on page 59.

Shortcut menus

Shortcut (context) menus have been significantly expanded for all items in the console, including groups, devices, queries, scheduled tasks, scripts, reports, and so on. Shortcut menus provide quick access to an item's common tasks and critical information.

To view an item's shortcut menu, select and right-click the item.

Available options in the shortcut menu

Options that appear in a device's shortcut menu, as well as options that are disabled or dimmed, may differ depending upon the device platform and upon which LANDesk agents are installed on the device.

For example, when you right-click a managed device in the network view, its shortcut menu will typically display the following options:

- **Inventory:** Displays all of the device's inventory data scanned in the core database.
- **Inventory history:** Displays inventory data changes for the attributes you've selected for tracking. You can print the inventory history or export it to a .CSV file.
- **Remote control:** Opens a remote control session with the device.
 - **Chat:** Opens a remote chat session with the device.
 - **File transfer:** Opens the file transfer dialog where you can transfer files to and from the device.
 - **Remote execute:** Lets you browse to and execute a batch file or application on the device.
- **Wake up:** Remotely wakes up a device whose BIOS supports Wake on LAN* technology.
- **Shut down:** Remotely shuts down the device.
- **Reboot:** Remotely reboots the device.
- **Inventory scan:** Runs an inventory scan on the device.
- **Scheduled tasks and policies:** Displays the device's current scheduled tasks and application management policies.
- **Add to new group:** Adds a copy of the device to a new user-defined group under the **My Devices** group. You're prompted to enter a name for the new group.
- **Add to existing group:** Lets you select the group where you want to add a copy of the device.
- **Group membership:** Displays all of the groups where the device is currently a member.
- **Run inventory report:** Opens the Reports dialog where you can select from a list of reports to run on the device. Double-click the report name to run it.
- **Update Agent Watcher settings:** Opens the Update Agent Watcher settings dialog where you can enable/disable real-time monitoring of specific LANDesk agents and services, choose an Agent Watcher settings or configure a new one, and specify a time interval to check for changes in the selected setting.
- **Security and patch information:** Opens the Security and patch information dialog that displays detailed vulnerability scan and remediation data for the device: including detected vulnerabilities and other security risks, installed patches, and repair history.
- **Security and patch scan now:** Opens a dialog that lets you select a scan and repair settings, and then click **OK** to perform an immediate security scan on the device.
- **LANDesk Antivirus scan now:** Opens a dialog that lets you select a LANDesk Antivirus settings, and then click **OK** to perform an immediate antivirus scan on the device.
- **Manage local users and groups:** Opens the Local users and groups dialog that lets you remotely manage a Windows device's local users and groups.
- **Cut:** Removes items from a user-defined group. You can't cut items from the "All" groups.
- **Copy:** Creates a copy of the item that you can add to a another group.
- **Paste:** Places the item you've cut or copied into a user-defined group.
- **Remove:** Removes the item from a user-defined group.
- **Delete:** Deletes the item from the "All" group AND from any other group it's a member of at the time.
- **Properties:** Displays the device's inventory summary, device information, agent status, and remote control settings.

This guide does not cover every item type's possible shortcut menu. We recommend that you right-click any item to see the options that are available.

Configuring the network view with column sets

Column sets allow you to customize the inventory data that displays in the right pane of the network view, for both device lists and query results lists. Each column in a column set represents a unique attribute (or component) from the scanned inventory. For example, the default column set that displays in the network view is comprised of the Device Name, Type, and OS Name attributes.

Use the Column Set Configuration tool (**Tools | Administration | Column Set Configuration**) to create as many column sets as you like. Then, to apply a column set, drag the desired column set to device groups and query objects in the network view tree.

Column sets window

Note: The Column Sets window replaces the Manage Column Configuration dialog found in previous versions.

The Column sets window organizes column sets into three categories:

- **My column sets:** Column sets created by the currently logged-in user.
- **Public column sets:** Column sets created by an administrator, or predefined column sets.
- **All column sets** (only visible to an administrator): Column sets created by all LANDesk users.

A user can copy a column set from the Public Column Sets group into their own My Column Sets group and then modify the column set properties.

You can create subgroups under the **My column sets** object to further organize your column sets.

Creating column sets

The **Column configuration** dialog is where you create column sets. Each column represents a single inventory attribute or component that has been scanned into the core database. Columns appear from left to right in the network view in the order that they appear in the Columns list.

To create a column set

1. Click **Tools | Administration | Column Set Configuration**.
2. Select the **My column sets** object (or the **Public column sets** object), and then click the **New** toolbar button.
3. In the **Column Configuration** dialog, enter a name for the new column set.

4. Select inventory attributes from the list and add them to the Columns list by clicking **Add to columns**. Remember to select attributes that will help you identify the devices in the device list or returned by the query.
5. (Optional) You can customize how and where the columns appear in the network view by directly editing a component's heading, alias, and sort order fields; or by removing or moving the selected component up or down in the list with the available buttons.
6. (Optional) You can specify more precise qualifying data for software components. Select the software component, click the **Qualify** button, and then select a primary key value from the list of available values. For more information, see "Using the qualify option with software components" on page 32.
7. Click **OK to save the column set**.

Restoring the original default columns

To restore the default columns in the network view, simply create a custom column set that includes the Device Name, Type, and OS Name attributes, and then apply it to device groups and query objects. Or, you can use the predefined column set named Original in the My column sets group.

Applying column sets to device groups and queries

Once you've created a column set, you can drag it to a devices group or subgroup, or to a specific query object in a queries group or subgroup. The device list, or query results list, displays the inventory data specified by the selected column set in the right pane of the network view.

Note that for device lists, once a column set is applied to a group it persists even when you select different device groups. However, for query results lists, the column set must be reapplied when changing between various queries.

You can also right-click a column set to access its shortcut menu and perform common tasks, as well as view and edit its properties. The shortcut menu includes the following options:

- Add to new group
- Add to existing group
- Group Membership
- Set as default
- Cut
- Copy
- Remove
- Rename
- Properties

Using the qualify option with software components

When creating column sets that include software components, you can specify a qualifier for those software components by choosing a specific primary key value. A software qualifier lets you more precisely identify the data you want a query to search for and display in that software component's column. For example, you can configure the column set to display version information for only one specific application by selecting that application's executable file name as the qualifier.

To specify a software component's qualifier, select the software component in the Columns list, click the **Qualify** button, and then select a value from the list of available primary key values.

As with the Alias field, once you select a primary key value and add it to the software component's Qualifier field, you can manually edit it by clicking in the field.

About the Column Configuration dialog

Use this dialog to create a new column configuration.

- **Name:** Identifies the column configuration.
- **Inventory attributes:** Lists each of the inventory objects and attributes scanned into the core database. Expand or collapse objects by clicking the box to the left of the object.
- **Add to columns:** Moves the selected inventory attribute into the columns list. If you select an entire inventory component, all of the inventory attributes contained in that component are added to the columns list.
- **Columns:** Lists the inventory attributes in the order they will appear, from left to right, in the network view.
- **Qualify:** Lets you specify a precise data qualifier for the selected software component. For more information, see "Using the qualify option with software components" on page 32.
- **Remove:** Removes the selected attribute from the list.
- **Move up:** Moves the selected attribute up one position.
- **Move down:** Moves the selected attribute down one position.
- **OK:** Saves the current column configuration and closes the dialog.
- **Cancel:** Closes the dialog without saving any of your changes.

Toolbar options

The console includes a toolbar that provides one-click access to common network view operations and some basic console configuration options. The toolbar buttons are dimmed when an item in the network view is selected that does not support that operation.

You can enable text descriptions for toolbar buttons by clicking **View | Show toolbar text**.

The console toolbar includes the following buttons:

- **Cut:** Removes items from the network view and stores them temporarily on the clipboard. If you accidentally cut an item, use the paste command to restore it. You must restore the deleted item before you perform any other command.
- **Copy:** Copies items from one location in the network view to another.
- **Paste:** Pastes items you've cut or copied.
- **Delete:** Permanently removes the item. You can't restore items you delete from the network view.
- **Refresh:** Updates the selected group or item in the network view. You can also collapse and expand a group to update its items. You can also click **View | Refresh** to update the currently selected item in the network view.
- **Refresh scope:** Updates the selected group or item in the network view, based on the currently logged-in user's scope (as defined in the Users tool).

- **Layout:** Lists your saved window layouts. Select a layout from the drop-down list to restore the console to that layout configuration. If you want to save your current layout, click the **Save the current layout** button.
- **Core:** Lists core servers you have connected to before (which makes them appear in this list). You can select a core server from the list, or type the name of a core server and press **Enter**. That core server is searched for on your network, and if found you're prompted to log in with a valid user name and password.

Using console tools

Tools are available through both the Tools menu and the Toolbox. To enable the **Toolbox**, click **View | Toolbox**.

A LANDesk Administrator sees all of the tools in both the Tools menu and the **Toolbox**. Other LANDesk users will see only the tools (features that are allowed by their assigned rights). Tools dependent on rights that a user hasn't been granted don't appear at all in the Tools menu or in the **Toolbox** when that user is logged in to the console. For example, if a user doesn't have the Reports right, the Reports tool does not appear in either the **Tools** menu or the **Toolbox**.

When you click a tool name, the tool's window opens in the console. Tool windows can be resized, docked, floating, hidden, and closed. You can have multiple tool windows open at the same time, docked or floating. See the next section for more information on manipulating tool windows.

Dockable tool windows

Dockable windows is a console feature that lets you open as many of the tools as you want and move them in and out of the main console window.

Note: You can save console layouts you've designed and prefer for certain management tasks, and restore a saved layout whenever you need it. For more information, see "Saving window layouts" on page 35 later in this chapter.

When you open multiple tool windows, they're tabbed in a single window. The active tool window displays on top, with a tab for each open tool running along the side or bottom. Click a tab to display that tool window. You can dock the tabbed tools window or drag it so that it is floating outside of the console window.

Docking a tool window means attaching it to one of the edges of the console. The window is said to be in a docked state if it is currently attached to an edge of the console. You can also undock the tools window and have it free-floating outside of the console. You can dock windows horizontally or vertically in the console.

To dock a tool window

1. Click the window's title bar and drag the window to an edge of the console
2. When the docking rectangle (dim outline of the window appears indicating that the window will be docked), release the mouse button. The window attaches to that edge of the console.

Note that only tool windows (those windows accessible from the **Tools** menu or **Toolbox**) can exist as docked windows, floating windows, or tabbed windows. The network view window can be resized but can't be tabbed with other windows, floated outside the console, or closed.

If you minimize and then restore the main console window, then all docked and floating windows, including tabbed windows, are also minimized and restored with it.

Auto hide

The tool windows also support the auto hide feature. Auto hide is a push pin button in the upper right-hand corner of a window that lets you hold a window in place or hide it.

When the push pin is in (i.e., the pin points down), the window is pinned in place and auto hide is temporarily disabled. When the push pin is out (i.e., the pin points to the left) the window goes into auto hide mode when the cursor moves off of the window. Auto hide minimizes and docks the window along one of the edges of the console and displays a tab in its place.

The **Toolbox** also supports auto hide.

Saving window layouts

Layouts are saved console configurations, meaning the position and size of the network view, the **Toolbox**, and all open tool windows. You can use window layouts to save and restore customized console configurations that are especially useful for certain tasks or users.

To change the layout of the console, select a saved layout from the **Layout** drop-down list on the main toolbar.

To save your current layout

1. Configure the console interface the way you want it.
2. Click the **Disk** button next to the **Layout** drop-down list on the toolbar.
3. Enter a unique name for the layout.
4. Click **OK**.

About the Manage window layouts dialog

Use this dialog to manage saved window layouts and to reset the console window to the previous layout.

- **Saved layouts:** Lists all of your saved layouts.
- **Reset:** Returns the console window to the previous layout.
- **Delete:** Removes the selected layout.
- **Rename:** Lets you change the name of the selected layout.

Find bar

Find lets you search for items in a list containing a specific word or phrase. The **Find** bar is available in the network view and tool windows that contain flat lists of items. For example, the **Find** bar appears when you're viewing the:

- All Devices group
- All Queries group
- Pending Unmanaged Client Deployments group
- Unmanaged Device Discovery tool window
- All Asset Reports

To search for an item with the Find bar

1. Select the **All devices** group. The **Find** bar appears at the top of the list.
2. In the **Find** text box, type any text you want to search for.
3. From the **In column** drop-down list, select the column you want to search
4. Click the **Search** toolbar button.

The resulting list displays only those items that matched your search criteria.

Status bar

The status bar at the bottom of the console displays the following information (from left to right):

- Number of selected items in a listing
- Current job name and status
- Name of the currently logged-in user
- Days until the core server will attempt to contact the licensing server

The status bar is always visible.

Viewing device properties

In the console's network view, you can quickly view information about a device by right-clicking the device in the device list and selecting **Properties**.

More detailed information about the device is available in its inventory data. You can view inventory data in the network view columns (which are configurable), or by right-clicking the device and selecting **Inventory** to open the full **Inventory** window.

About the Device properties dialog

Use this dialog to view useful information about the selected device. The dialog includes three tabs: **Inventory**, **Device**, and **Agents**. Click each one to view related information.

Inventory tab

The **Inventory** tab contains a summary of the device's inventory data. For more details, see "Viewing a summary inventory" on page 116.

Device tab

The **Device** tab contains basic information about a device, including its location and identity on the network. This tab also appears when you manually insert a device (from the **All devices** group's shortcut menu, click **Insert new computer**).

- **Device:**
 - **Name:** The name that appears in the core database and network view for the device.
If you are manually inserting a device, you can make this a user-friendly name. If you enter nothing here, the default device name will be the Windows computer name.
 - **Type:** The type of device, such as Windows 2000 Server or XP Workstation.
- **Network:**
 - **IP Name:** The Windows computer name for the device.
 - **IP address:** The IP address assigned to the device.
 - **Physical address:** The physical address of the device.

Agents tab

The **Agents** tab contains information about the current status of agents and remote control settings for the device.

- **Common Base Agent status:** Indicates whether the standard LANDesk agent (Common Base Agent) is loaded on the device.
- **LANDesk System Manager status:** Indicates whether the LANDesk System Manager agent is loaded on the device. This agent will only be loaded if you have LANDesk System Manager installed on your core server, and if you've deployed the System Manager agent to this device. For more information, see "Configuring device agents" on page 86.
- **Remote control agent status:** Indicates whether the remote control agent is loaded on the device. If this agent is not loaded on the device, remote control operations (such as file transfer and chat) are not available.
- **Security type:** Indicates the remote control security model used for the device. Options include: Local template, Windows NT security/local template, and Certificate-based/local template.
- **Allow:** Shows the remote control operations that are allowed on the device. These operations were enabled by the device agent configuration.
- **Settings:** Indicates how remote control operates when you attempt to interact with the device.

Configuring agent discovery

Agent discovery is the process used to find managed devices that have the standard LANDesk agent or remote control agent installed. These two agents provide the following capability:

- **The standard LANDesk agent:** Enables the PDS (ping discovery service). If the standard LANDesk agent is installed on a device, you can schedule software distributions and device setup configurations.
- **Remote control:** Lets you remotely access and control a device.

Agent discovery uses TCP/IP to verify agents running on the devices.

IP addresses are used as search criteria in order to perform standard LANDesk agent discovery with TCP/IP. LANDesk looks for the standard LANDesk agent and remote control agent on devices within a specific range of IP addresses. This range of addresses is implied by the IP network address you supply.

If you don't designate subnet network addresses when searching on TCP/IP, discovery is performed only on the network segment where the console initiating the discovery resides. For example, if you've installed four consoles, each residing on a different network segment, you would have to initiate four scans, one from each of the four consoles.

On network segments where consoles don't exist, you **MUST** use subnet network addresses to access the information on that network segment.

Note on firewalls: If you have one or more firewalls on your network, agent discovery can't be used to search outside firewalls, because firewalls generally limit the flow of packet traffic to designated ports.

To configure agent discovery options

1. Click **Configure | Agent discovery options**.
2. Select whether you want agent discovery to update agent status for only the selected item in the network view, or all visible items in the network view.
3. Specify the agent status refresh rate.
4. Configure how you want to discover the remote control agent, and prioritize the address resolution methods.
5. Specify how long agent discovery will attempt to discover the remote control agent on the device before timing out.
6. Click **OK**.

About the Agent discovery options dialog

Use this dialog to configure the following agent discovery options.

- **Gather agent status:**
 - **For selected items only:** Specifies that a device's agent status is updated as the device is selected in the network view. This option generates the least amount of network traffic and is the default.
 - **For visible items in network view:** Specifies that all visible devices in the network view will have their agent status updated according to the refresh rate. As new devices become visible, their agent status (and health) are updated.
- **Agent and health status refreshes every < > minutes:** Indicates whether agent status is automatically updated. You can specify the refresh rate.
- **Discovery methods:** Indicates how the agent is discovered.
 - **IP address:** Uses the core database to retrieve the computer's stored IP address.

- **Domain Name Service (DNS):** Resolves the computer's ID name with the DNS server when verifying the remote control agent. If you do not have a DNS server, clear this option.
- **Move up and Move down:** Moves the selected method up or down in the Discover agent using list. Methods are tried in the order they appear in the list.
- **Timeout:** Sets the timeout value before the remote control agent discovery fails for each checked address resolution method.

Monitoring devices for network connectivity

Device monitoring lets you regularly monitor the connectivity of any of your managed devices.

Ping settings are specific to the device you've selected. When a device stops responding to a ping (when it goes offline), AMS alerts are generated to notify you. You can also configure alerts to inform you when devices come back online.

About the Configure device monitoring dialog

Use this dialog to configure the following device monitoring options.

- **Monitor these devices:** Lists the devices that are currently being monitored.
- **Add:** Opens the **Add monitored devices** dialog where you can search for and select managed devices that you want to monitor.
- **Remove:** Deletes the selected device from the list.
- **Ping frequency:** Control when and how the ping operation occurs. These settings can be applied to each device individually.
 - **Ping every:** Schedules a periodic ping at the specified minute interval.
 - **Schedule daily at:** Schedules a daily ping at a specific time.
 - **Retries:** Specifies the number of ping retries.
 - **Timeout:** Specifies the number of seconds until ping retries will timeout.
- **Alert settings:** Opens the Configure Alerts dialog where you can set up AMS alerting to notify you when the device goes offline or online. Alert Settings includes its own online Help that you can access by clicking the Help button.
- **OK:** Saves your changes and closes the dialog.
- **Cancel:** Closed the dialog without saving your changes.

Configuring device monitoring alerts

If you want device monitoring to notify you when managed devices come online or go offline, you have to first configure the alert settings.

To configure device monitoring alert settings

1. In the **Configure device monitoring** dialog, click **Alert settings**.
2. In the **Configure alerts** dialog, expand the **Device monitor** tree.
3. Select the alert you want to configure and click **Configure**.
4. Select an alert action and click **Next**.
5. Select the device you want the alert action performed on. Don't select the device you're monitoring, because if it goes offline, it won't be able to process the alert action.
6. Finish the alert configuration wizard.

Note: When you configure alert settings, they apply to all of the devices you're monitoring.

Hardware configuration

Intel* vPro support

Server Manager supports devices using Intel* vPro technology, a hardware and firmware technology that enables remote device management and security. Intel vPro uses out-of-band (OOB) communication for access to devices regardless of the state of the operating system or power to the device.

In this product, the term "Intel vPro" refers to technologies provided on for desktop computers with Intel* vPro (release 3.0) and notebooks with Intel* Centrino Pro (release 2.6). This product also supports devices with Intel* Active Management Technology (Intel* AMT) release 1.0, Intel vPro release 2.0, 2.1, and 2.2, and Intel Centrino Pro release 2.5. The process for provisioning devices with different releases of Intel vPro varies according to the release numbers. The information in this section applies to all versions except as noted.

The following table lists Intel vPro features supported in version 8.8 of this product in different releases of Intel vPro.

Feature	Intel AMT 1.0	Intel vPro 2.0/2.1/2.2	Intel Centrino Pro 2.5/2.6	Intel vPro 3.0
Provision devices	Yes	Yes	Yes	Yes
System Defense	No	Yes	Yes	Yes
Enhanced System Defense	No	No	No	Yes
Agent Presence	No	Yes	Yes	Yes
Wireless profile & device management	No	No	Yes*	No
Serial-over-LAN & IDE redirection	Yes	Yes	LAN connection: Yes Wireless mode: Yes, if wireless profile exists	Yes
Remote configuration (zero touch provisioning)	No	2.0/2.1: No 2.2: agent-based only	2.5: No 2.6: agent-based only	Yes

*A wireless profile is required for wireless management of Intel Centrino 2.5 notebooks. For Intel Centrino 2.6 notebooks, a wireless profile is required only to use Serial-over-LAN and IDE redirection features; other wireless management features can be used whether or not a wireless profile exists on the notebook.

The Hardware configuration tool includes the following features for managing Intel vPro devices:

- [Automatic generation of provisioning IDs \(PID/PPS pairs\) \(release 2.x/3.0\)](#)
- [Changing the password for managed devices](#)
- [Configuring and enabling System Defense policies \(release 2.x/3.0\)](#)
- [Configuring and enabling Agent Presence monitoring \(release 2.x/3.0\)](#)
- [Enhanced System Defense \(release 3.0\)](#)
- [Wireless support for Intel Centrino Pro notebooks \(release 2.5/2.6\)](#)

Managing devices with or without management agents

When devices are configured with Intel vPro, a limited number of management features are available even if the device does not have a LANDesk agent installed. As long as devices are connected to the network and have standby power, they can be discovered and can be added to inventory to be managed with other devices on the network.

If a device has Intel vPro but no management agent installed, it can be discovered, added to the inventory database, and viewed in the **My devices** list. Management features that are available for Intel vPro-configured devices include:

- **Inventory summary:** A subset of the normal inventory data can be queried and viewed in real time for the device even if the device is powered off.
- **Event log:** A log with Intel vPro-specific events, showing severity and description of the events, can be viewed in real time.
- **Remote boot manager:** Power cycling and several boot options can be initiated from the remote management console, regardless of the state of the device's OS or power. The options available are dependent on support for the options on the device. Some devices may not support all boot options.
- **Force vulnerability scan and disable OS network:** If a device appears to have malicious software running, a vulnerability scan can be run at the next reboot; if necessary, the device's OS-level network access can be disabled to prevent unwanted packets from being spread on the network.
- **System Defense:** The Intel vPro System Defense feature enforces network security policies on managed devices. Enhanced System Defense (release 3.0) adds heuristic filtering rules to prevent malicious software attacks on the network.

Other Server Manager management options are available only when a management agent is installed on the device. For more information about management options, see [Managing Intel vPro devices](#).

Intel AMT version 1.0 provisioning requirements

Devices can be discovered as Intel AMT 1.0 devices only after you have accessed the Intel AMT Configuration Screen on the device's BIOS and changed the manufacturer's default password to a secure password. (Refer to the manufacturer's documentation for information on accessing the Intel AMT Configuration Screen). If you have not done this, the devices will be discovered but not identified as Intel AMT devices, and you will not be able to view the same inventory summary information as you otherwise would.

In order for the core server to authenticate with discovered Intel AMT devices, the username/password credentials you enter in the device BIOS must match the credentials that you enter in the Configure Services utility.

When an Intel AMT device is added to the core database to be managed, Server Manager automatically provisions it in the mode you select in the Configure Services utility, regardless of whether it has already been provisioned. Small business mode provides basic management without network infrastructure services and is non-secure, while Enterprise mode is designed for large enterprises and uses DHCP, DNS, and a TLS certificate authority service to ensure secure communication between the managed device and the core server.

When you provision an Intel AMT device in Enterprise mode, the core server installs a certificate on the device for secure communication. If another computer attempts to access the Intel AMT functionality on the device, it will not succeed because it does not have a matching certificate.

Configuring Intel* vPro devices

Devices equipped with Intel vPro* functionality should be configured when they are first set up and powered on, to enable Intel vPro features. This process includes several security measures to ensure that only authorized users have access to the Intel vPro management features.

Intel vPro devices communicate with a provisioning server on the network. This provisioning server listens for messages from Intel vPro devices on the network and allows IT staff to manage servers through out-of-band communication regardless of the state the device's OS is in. Server Manager acts as a provisioning server for Intel vPro devices and includes features that help you provision devices when you set them up. You can then manage the devices with or without additional Server Manager management agents.

This section outlines a recommended process for configuring new Intel vPro devices. During this process you will use Server Manager to generate a set of provisioning IDs (PID and PPS). These IDs are entered in the device BIOS to ensure a secure connection with the provisioning server during the initial provisioning process. This "one-touch" process can be used to configure devices with release 2.0, 2.1, 2.2, 2.5, 2.6, and 3.0.

Devices with release 2.2, 2.6, and 3.0 can also be configured using remote configuration (also referred to as zero-touch provisioning). This process does not require the transfer of PID/PPS IDs, but is initiated automatically after the device's "hello" packet is received by the provisioning server (core server) or after a LANDesk management agent is deployed on the Intel vPro device. An Intel Client Setup certificate from an authorized certificate vendor must be installed on the core server to use remote configuration.

For devices with Intel vPro release 3.0, a "bare metal" or agentless remote configuration is also supported.

Devices with Intel AMT version 1.0 use a similar process but don't use the PID and PPS keys. See the notes at the end of this section for details.

Note that the information in this section is a general description of the Intel vPro configuration process. However, individual manufacturers implement Intel vPro functionality in different ways and there may be differences in such areas as accessing the Intel AMT or ME BIOS screens, resetting the device to factory mode (unprovisioning), or in the way that PID/PPS key pairs are provided. Consult the documentation and support information provided by device manufacturers before you begin the configuration process.

This chapter includes information about:

- [One-touch provisioning for Intel vPro devices](#)
- [Importing and exporting key files using a USB drive](#)
- [Using static IP addresses with Intel vPro devices](#)
- [Remote configuration \(zero-touch provisioning\)](#)
- [Discovering Intel AMT 1.0 devices](#)

One-touch provisioning for Intel vPro devices

This section describes the process of using one-touch provisioning for Intel vPro 2.0, 2.1, 2.2, and 3.0 devices, as well as Intel Centrino Pro 2.5 and 2.6 notebooks.

When an Intel vPro 2.x/3.0 device is received, the IT technician assembles the computer and powers it on. After powering on the device, the technician logs in to the BIOS-based Intel ME (Management Engine) Configuration Screen and changes the default password (admin) to a [strong password](#). This allows access to the Intel AMT Configuration Screen.

In the Intel AMT Configuration Screen, the following pre-provisioning information is entered:

- A provisioning ID (PID)
- A pre-provisioning passkey (PPS) , also known as a pre-shared key (PSK)
- The IP address of the provisioning server
- Port 9971 as the port for communicating with the provisioning server
- Enterprise mode should be selected
- The host name of the Intel vPro device

The PPS is shared by the provisioning server and the managed device, but cannot be transmitted on the network for security purposes. It needs to be entered manually on the device (at the Intel AMT Configuration Screen). PID/PPS pairs are generated by Server Manager and stored in the database. You can print a list of generated ID pairs for use in provisioning, or you can export the ID pairs to a key file on a USB drive.

The IT technician should enter the IP address of the Server Manager core server for the Provisioning Server and specify port 9971. Otherwise, by default, the Intel vPro device sends a general broadcast that can be received only if the configuration server is listening on port 9971.

The default username and password for accessing the Intel AMT Configuration Screen are "admin" and "admin". The username stays the same, but the password must be changed during the provisioning process to a strong password. The new password is entered in the Configure Services utility that is included with Server Manager, as described in the procedural steps below. After each device is configured you can change the password individually per device, but for provisioning purposes you use the password that is found in Configure Services.

After the above information is entered in the Intel AMT Configuration Screen, the device sends "hello" messages when it is first connected to the network, attempting to communicate with the provisioning server. If this message is received by the provisioning server, the provisioning process will begin as the server establishes a connection with the managed device.

When the core server receives the hello message and verifies the PID, it provisions the Intel vPro device to TLS mode. TLS (Transport Layer Security) mode establishes a secure channel of communications between the core server and the managed server while the provisioning is completed. This process includes creating a record in the database with the device's UUID and encrypted credentials. When the device's data is in the database, the device appears in the list of unmanaged devices.

When an Intel vPro device has been provisioned by the core server, it can be managed using only Intel vPro functionality. To do this, you can select it in the list of unmanaged devices and add it to your managed devices. You can also deploy Server Manager management agents to the device to use additional management features.

The recommended process for provisioning Intel vPro 2.x devices is as follows. Specific instructions for items 1 and 2 are given in the following procedural steps. If you choose to provision devices with a key file on a USB drive, steps 3-5 below are replaced with the steps described in the section below titled Important and exporting key files using a USB drive.

1. Run the Configure Services utility to specify a new, strong password for provisioning Intel vPro devices. (See detailed steps below).
2. Use Server Manager to generate a batch of Intel vPro provisioning IDs (PID and PPS). Print the list of keys or export them to a USB drive. (See detailed steps below).
3. Log in to the device's Intel ME Configuration Screen from the BIOS and change the default password to a strong password.
4. Log in to the Intel AMT Configuration Screen. Enter a PID/PPS key pair from the list of provisioning IDs that you printed. Enter the IP address of the core server (provisioning server), and specify port 9971. Make sure Enterprise mode is selected for provisioning. Enter the host name of the Intel vPro device.
5. Exit the BIOS screen. The device will begin sending "hello" messages.
6. The core server receives a "hello" message and checks the PID against the list of generated keys. If there is a match, it provisions the device.
7. The device is added to the unmanaged device discovery list.
8. Select the device and add it to your managed devices (click **Target** on the toolbar, click the **Manage** tab, then click **Move**). You can choose to manage it as an agentless device, or you can deploy management agents to it for additional management features.

To set the Intel vPro password in Configure Services

1. On the core server, click **Start | LANDesk | Configure Services**.
2. Click the **Intel vPro Configuration** tab.
3. Type **admin** as the password under **Current Intel vPro Credentials**.

4. Type a [strong password](#) under **Provision with new Intel vPro Credentials**.
5. Click **OK**.

The new password must be entered here before you can generate a batch of provisioning IDs.

To generate a batch of Intel vPro provisioning IDs

1. Click **Configure | Intel vPro options | ID Generation**.
2. Type the number of IDs to generate (generally the number of devices you plan to provision).
3. If you want to use a different prefix for the PIDs, type it in the **PID prefix** text box. This prefix can only contain uppercase alphabetic characters and numerals in the ASCII character set. You can enter a maximum of 7 characters for a prefix.
4. Type a batch name to identify this group of generated IDs.
5. Click **Generate IDs**.
6. After the IDs have been generated, click **Print ID list** to print the list of IDs. (Only the IDs currently shown in the list are printed.) Your browser's print feature opens automatically.
7. To view all IDs that have been previously generated, select **Show all** in the **View batch IDs** drop-down list.
8. To view one batch of generated IDs, select the batch name in the **View batch IDs** drop-down list.

The provisioning keys are stored in the database for future reference as you provision new Intel vPro devices. As the devices are provisioned and the provisioning keys are consumed, the **Generate Intel vPro IDs** page will display shading for the IDs that have been consumed, so you can track which IDs have been used.

A PID prefix is added for your convenience in identifying the IDs as PIDs, but you are not required to use a prefix. We recommend using 0-4 characters; you can use a maximum of 7 characters for the prefix.

To identify batches of provisioning keys, specify a batch name. This should be a descriptive name that indicates which devices the IDs apply to. For example, you could generate batches for each organization in your company and name the batches Development, Marketing, Finance, and so forth. If you later want to view the generated IDs, you type the batch name and click **View batch IDs** to see a list with only those IDs.

Errors in the provisioning process

If you enter a PID and PPS that are not paired correctly (i.e., the PPS should be paired with a different PID), you will see an error message in the alert log and provisioning will not continue with that device. You will need to restart the device and re-enter a correct PID/PPS pair in the Intel AMT Configuration Screen.

If, as you type a PID or PPS, the Intel AMT Configuration Screen displays an error message, you have mis-typed the PID or PPS. A checksum is performed to ensure that the PID and PPS are correct.

Strong passwords

Intel vPro requires the use of a strong password to enable secure communications. Passwords should meet these requirements:

- At least 8 characters long
- Includes at least one number character (0-9)
- Includes at least one non-alphanumeric ASCII character (such as !, &, %)
- Contains both upper- and lowercase Latin characters, or non-ASCII characters (UTF+00800 and above)

Importing and exporting key files using a USB drive

You can generate provisioning IDs and export them to a key file for use in provisioning Intel vPro devices with a USB drive. The exported IDs are saved to a setup.bin file that you can copy to a USB drive. With that USB drive you can automatically populate the PID/PPS fields in the Intel AMT BIOS as you provision new Intel vPro devices before you discover and manage them.

If a device manufacturer provides you with a set of provisioning IDs for the Intel vPro devices you have purchased, you can import those provisioning IDs into the core database so that the core server will recognize those devices as Intel vPro devices and discover them automatically.

These two processes are described below.

Exporting provisioning IDs for use with a USB drive

Server Manager generates provisioning IDs (PID/PPS pairs) that you use to provision new Intel vPro devices. You can print a list of the generated IDs and enter them manually when you provision each device. Alternately you can export the IDs to a setup.bin key file, save that file on a USB drive, and then use the USB drive to provision the devices. This can reduce errors in provisioning because you don't need to type the IDs manually at each device.

The USB drive you use must be in FAT-16 format for this process to work.

The setup.bin file is created with a specific key file format defined by Intel. When you provision the new Intel vPro device, you connect the USB drive to the device and reboot it. During the boot process a pair of provisioning IDs (PID and PPS) is taken from the setup.bin file and entered into the device's Intel AMT BIOS. When the device sends its "hello" message on the network, the core server will recognize it and be able to communicate securely with it because the provisioning IDs are found in the core database.

To export a batch of provisioning IDs for use with a USB drive

1. Click **Configure | Intel vPro options | Import/Export**.
2. Select **Export AMT IDs to setup.bin file**.
3. For Intel vPro 2.5, 2.6, or 3.0 devices, enter the password you use to access the Intel ME Configuration Screen.
4. Type a number in the **Number of IDs** text box to specify how many IDs to export.

5. Specify the location of the setup.bin file. Click **Browse** and select the drive and path where you want the file saved.
You can save the file to any location and then copy the file to a USB drive, or you can simply specify the location of the USB drive if it is connected to the core server. To use the setup.bin file for provisioning, the file must be saved to the root directory of the USB drive.
6. Click **Apply**.

Note: the IDs you generate are listed with other IDs you have generated on the **Generate Intel vPro IDs** page. The IDs will be shaded in the list to indicate that they are not available for provisioning other devices.

To use exported provisioning IDs on new Intel vPro devices

1. Export a batch of provisioning IDs as described above, and save the setup.bin file to the root directory of a USB drive.
2. At each new Intel vPro device, connect the USB drive to the device and reboot it.

As the device boots, it accesses the setup.bin file and takes an available provisioning ID pair (PID and PPS) for use in the provisioning process. It then marks the provisioning ID pair as used so it will not be used by another device. The next device you provision will then take the next available provisioning ID pair.

Note that for this process to work correctly, the default username and password for accessing the Intel AMT BIOS must not have been changed (the default is typically admin/admin). You should not have already entered provisioning IDs on the device.

Importing provisioning IDs from a key file to the core database

If a device manufacturer provides you with a set of provisioning IDs for the Intel vPro devices you have purchased, you can import those provisioning IDs into the core database so that the core server will recognize those devices as Intel vPro devices and discover them automatically. The manufacturer supplies these IDs in a setup.bin key file when you purchase the devices.

To import the IDs into the core database, you simply browse to the location of the setup.bin file that the manufacturer provided (this can be on a CD or DVD, or you can copy the file to any drive). After these IDs are saved to the database, when you start up the Intel vPro devices and they send a “hello” message, the core server recognizes them and discovers the devices.

To import provisioning IDs from a key file to the core database

1. Click **Configure | Intel vPro options | Import/Export**.
2. Select **Import from USB key file**.
3. Specify the location of the setup.bin file. Click **Browse** and select the drive and path of the file.
4. Click **Apply**.

The provisioning IDs are added to the core database and are listed on the **Generate Intel vPro IDs** page.

Using static IP addresses with Intel vPro devices

Because Intel vPro devices have two components that are assigned an IP address – the Intel vPro chip and the device’s operating system – you can potentially have two entries in your list of discovered devices for the same Intel vPro device. This happens only if you want to use a static IP address rather than using DHCP.

To use static IP addresses with Intel vPro devices, the Intel vPro firmware should be configured with its own MAC address. (For instructions on how to re-install the firmware and configure it properly, contact Intel.)

Once configured, the Intel vPro device will have a different MAC address, IP address, and host name than the device OS. To be able to manage Intel vPro devices correctly, you need to use the following settings for DHCP and static IP addresses:

- **DHCP:** Both the OS and Intel vPro use DHCP and the host names are the same.
- **Static IP:** Both the OS and Intel vPro are set to use static addresses and they are different from each other, the MAC addresses are different, and the host names are also different.

If an Intel vPro 2.x machine is provisioned in Enterprise mode, the only way to communicate with it is via the “hello” packet being sent to the setup and configuration server. After the machine is managed by LANDesk software, Intel vPro operations may be performed on it like normal. What you should not do is discover and manage the OS IP address; otherwise you will have two computer entries that represent the same computer. Because the only common identifier between the two devices is the AMT GUID, and because the AMT GUID can not be found remotely for the OS device, the two entries cannot be merged.

If you want to install the LANDesk agents, you cannot push the agents, because the only IP address in the database is the Intel vPro IP address, and the push utility needs access to the OS. Instead, the agents need to be pulled (from the managed Intel vPro device) by mapping a drive to LDLOGON on the core server and running ServerConfig.exe.

Before pulling the agents, we recommend changing a setting in the Configure Services utility. Click **Start | All Programs | LANDesk | LANDesk Configure Services**. On the **Inventory** tab, click **Device IDs** to manage duplicate records. In the **Attributes** List, expand **AMT Information**, scroll down and move the **AMT GUID** attribute to the **Identity Attributes** list. This will force the AMT GUID to be one of the attributes that can uniquely identify a computer.

After you change this setting, when the Inventory scan from the managed Intel vPro device is imported into the database, the Inventory service matches the Intel AMT GUID from the device that’s already in the database with the OS information in the scan file.

Remote configuration (zero-touch provisioning)

This section describes the process for remote configuration of devices with Intel vPro 2.2 or 3.0, or Centrino Pro 2.6.

Remote configuration lets you configure a device in a factory default state through the setup process and then add an Intel AMT profile to make the device ready for out of band management. When the device is first powered on and connected to a network, it begins sending "hello" messages to the Setup and Configuration Server (when you manage devices with LANDesk products, the core server acts as the Setup and Configuration Server). If the Setup and Configuration Server is running, it establishes a secure connection with the Intel vPro device and begins the configuration process.

When this process is successful, the device is added to the list of discovered devices and can then be managed from the core server. Limited management is available with only the Intel vPro functionality, or a management agent can be deployed to the device for full management features.

Remote configuration has two requirements:

- DHCP is required on the network, with a DNS entry identifying the core server as the "ProvisionServer"
- An Intel* Client Setup Certificate must be installed on the core server for the domain the core server is installed on (instructions are given below for purchasing and installing a certificate)

Delayed provisioning

If an Intel vPro device is powered on but does not receive a response from the Setup and Configuration Server after a certain period of time (typically 6 to 12 hours, depending on the manufacturer's settings), it stops sending hello packets and waits. At this point Intel vPro functionality is not enabled on the device.

To provision a device in this state, you can install the standard LANDesk management agent on the device. When the agent determines that the device has Intel vPro capabilities it enables Intel vPro functionality on the device and sends a call to the web service on the core server to receive the "hello" packet. The provisioning process is then initiated from the core server.

Bare metal provisioning

Intel vPro 3.0 devices support a bare-metal (or agentless) approach to remote configuration. With the Setup and Configuration Server correctly set up, a DNS entry, and the correct certificate installed on the core server, the configuration process is completed without the use of agents.

Notes

If an Intel vPro device is powered on but does not begin sending "hello" messages as described above, remote configuration may not be enabled on the device. This is dependent on the manufacturer enabling remote configuration by setting Manageability Mode to "AMT" on the device. If this appears to be the case, you can deploy a LANDesk management agent to the device to enable the Intel vPro functionality and begin provisioning the device as described under "Delayed provisioning" above.

Obtaining and installing an Intel* Client Setup Certificate

An Intel* Client Setup Certificate is required on every Setup and Configuration Server. The certificate is valid for one namespace on one domain, so if your core server is used on multiple namespaces within a domain you need to purchase a certificate for each namespace.

The certificate must be purchased from an approved certificate vendor and must be a support class. The following vendors are supported for LANDesk products on the following devices.

Before you purchase a certificate, verify in the vendor's documentation or support information which certificates are supported on your device.

Vendor/Certificate class	Intel devices	Acer devices	Lenovo devices
Go Daddy class 2 CA	X	X	X
VeriSign class 3 Primary CA-G3	X	X	X
VeriSign class 3 Primary CA-G1	X	X	X
Comodo AAA CA	X	X	
Starfield class 2 CA			X

When you purchase a certificate you need to provide a CSR (certificate signing request) file. This file is generated for your LANDesk product along with a private key file. After you receive the certificate files from the vendor, the private key file is saved in a directory with a shared public key file and the certificate file from the vendor. This procedure is described below.

To obtain an Intel* Client Setup Certificate

1. Select a vendor and log in to the vendor's web site.
2. To generate a CSR file and private key:
3. In the LDMAIN share on the core server, in the amtprov directory, run AMTProvMgr2.exe with the following arguments:
`AMTProvMgr2.exe -domainName name.domain.com -country US`
 Use a two-letter country code; if none is specified the default is US. The domain name you specify should include a namespace.
 This executable saves two files to the amtprov directory: certreq.csr (certificate signing request) and corecakey.pem (a private key file).
4. Open the certreq.csr file in a text editor and copy the contents.
5. At the vendor's web site, paste the contents of the certreq.csr file into the field provided, and complete the application for the certificate.
 After your certificate request is processed the vendor will send you two files: a root certificate file (a common or public file) and a certificate file for the domain you specified.
6. Copy the vendor's root certificate file and rename the copy `trusted_cert.pem`.
7. Copy the vendor's certificate file for your domain and rename the copy `corecacert.pem`.
8. Save the above two files, along with the `corecakey.pem` file (generated in step 3 above), to a folder in `LDMAIN\amtprov\certStore\cert_1`. You can store up to eight certificates in subfolders named `cert_1`, `cert_2`, and so on.

Discovering Intel AMT 1.0 devices

When you run a device discovery scan, Intel AMT version 1.0 devices are discovered and added to the Intel AMT folder in the **Unmanaged** devices list. The devices are recognized as Intel AMT devices if they have been configured with a secure password that replaces the default set by the manufacturer.

When you add a secure password at the Intel AMT Configuration Screen, you can also enter the IP address of the provisioning server and specify port 9971, as is done with Intel vPro 2.x devices. However, no PID/PPS pairs are used in provisioning Intel AMT 1.0 devices. If you specify a provisioning server IP address, the core server acts as a provisioning server and you can manage the device as an agentless device.

Note that Intel AMT version 1.0 does not use the same level of security as vPro version 2.x. Intel recommends that devices with version 1.0 be configured on an isolated, secure network. After configuration is complete they can be moved to a less secure network for management.

Changing the password for Intel* vPro devices

A secure password is required to communicate with and to provision new Intel* vPro devices. For devices that you will manage with Server Manager, the password you enter in the Intel AMT Configuration Screen (accessed in the device BIOS) should be the same as the password that you enter in the Server Manager Configure Services utility. The password in the Configure Services utility is saved in the database and applied globally for provisioning Intel vPro devices.

Intel vPro requires the use of a strong password to enable secure communications. Passwords should meet these requirements:

- At least 8 characters long
- Includes at least one number character (0-9)
- Includes at least one non-alphanumeric ASCII character (such as !, &, %)
- Contains both upper- and lowercase Latin characters, or non-ASCII characters (UTF+00800 and above)

After provisioning devices, you should regularly change passwords as part of your IT maintenance. You can use a different password for each Intel vPro device or apply a password to multiple devices. The new passwords you enter in the **Hardware configuration** page are stored in the database and used by Server Manager to communicate securely with managed Intel vPro devices.

To change the password for Intel vPro devices

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Change Password**.
2. Type the new password, then confirm the password.
3. Click **OK**.

To change the password when provisioning Intel vPro devices

The Configure Services utility lets you enter two passwords for Intel vPro devices. In the **Current Intel vPro Credentials** section you must enter the same password that you entered in the Intel AMT Configuration Screen. If you want to change the password as part of the provisioning process, enter a second password in the **Provision with new Intel vPro Credentials** section. This is recommended for added security. For example, if the person who sets up the devices is not the same as the person who will manage the devices, it is helpful to change the password as part of the provisioning process.

1. Click **Configure | Services**.
2. Click the **Intel vPro Configuration** tab.
3. Enter the password under **Current Intel vPro Credentials** (the same password that you entered in the device's Intel AMT Configuration Screen).
4. To change the password as part of the configuration, enter a password under **Provision with new Intel vPro Credentials**.

Configuring System Defense policies

Intel vPro* releases 2.x and 3.x include a System Defense feature, which enforces network security policies on managed devices. You can select and apply System Defense policies for managed devices using the **Hardware configuration** tool.

When a System Defense policy is applied on an Intel vPro 2.x/3.x device, the device filters incoming and outgoing network packets according to the defined policies. When network traffic matches the alert conditions defined in a filter, an alert is generated and the device's network access is blocked. The device is then isolated from the network until you complete the remediation steps for that policy.

Server Manager contains predefined System Defense policies that you can apply to your Intel vPro devices. Each policy contains a set of filters that define what kind of network traffic is not allowed and what the resulting actions are when traffic meets the criteria of the filter. The process for selecting and applying policies is as follows:

1. Target one or more managed devices
2. Select the System Defense policy to apply
3. Apply the policy to the targeted devices

When a System Defense policy is active on a managed device, the device monitors all incoming and outgoing network traffic. If a filter's conditions are detected, the following occurs:

1. The managed device sends an ASF alert to the core server and an entry is added to the alert log
2. The core server determines which policy has been violated and shuts down network access on the managed device
3. The device is listed in the System Defense remediation queue (in the **Hardware configuration** tool)
4. To restore network access on the device, the administrator follows the appropriate remediation steps and then removes the device from the remediation queue; this restores the original System Defense policy on the device

This process is described in more detail in the following sections.

Selecting and applying System Defense policies

Server Manager contains the following predefined System Defense policies that can be applied to Intel vPro 2.x and 3.x devices. Policies are defined with parameters such as port number, packet type, and number of packets within a specific amount of time. When you enable a policy, it is registered with Intel vPro on the devices you have selected. Policies are saved as XML files on the managed device, in the CircuitBreakerConfig folder.

- **BlockFTPSrvr:** This policy prevents traffic through an FTP port. When packets are sent or received on FTP port 21, the packets are dropped and network access is suspended.
- **LDCBKillNics:** This policy blocks traffic on all network ports except for the following management ports:

Port description	Number range	Traffic direction	Protocol
LANDesk management	9593-9595	Send/receive	TCP, UDP
Intel vPro management	16992-16993	Send/receive	TCP only
DNS	53	Send/receive	UDP only
DHCP	67-68	Send/receive	UDP only

When the core server shuts down network access on a managed device, it actually applies this policy to the device. Then, when the device is removed from the remediation queue, the original policy is re-applied to the device.

- **LDCBSYNFlood:** This policy detects a SYN flood denial-of-service attack: it allows no more than 10,000 TCP packets with the SYN flag turned on, in one minute. When that number is exceeded, network access is suspended.
- **UDPFloodPolicy:** This policy detects a UDP flood denial-of-service attack: it allows no more than 20,000 UDP packets per minute on ports numbered between 0 and 1023. When that number is exceeded, network access is suspended.
- **RemoveAllPolicy:** Select this to remove all policies, unregistering them with Intel vPro on the selected devices.

To select a System Defense policy

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro System Defense Policies**.
2. Select a policy from the list.
3. Click **Set Policy**.

Turning on Enhanced System Defense (Intel vPro 3.x devices)

For devices equipped with Intel vPro 3.0 or later, you can enable Enhanced System Defense. This feature prevents malicious software attacks by continuously inspecting network traffic and evaluating it with enhanced heuristic filtering rules. It identifies and blocks suspicious behavior such as repeated actions generated by worms.

When suspicious behavior is detected, the device causing the problem is isolated from further network communication except for a remediation port, through which Server Manager can reinstate the System Defense policy and restore a network connection after the problem has been resolved.

To turn on Enhanced System Defense

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Enhanced System Defense**.
2. Click **Turn on Enhanced System Defense**, then click **Set Configuration**.
3. To turn off Enhanced System Defense, click **Turn off Enhanced System Defense** and click **Set Configuration**.

Restoring network access to devices in the remediation queue

If a device's network access is suspended because of a System Defense policy, the device is listed in the remediation queue. It remains there until you remove it from the list, which reinstates the active policy on that device. Before you do that, you need to resolve the issue that placed the device in the queue. For example, if FTP traffic was detected, you need to verify that appropriate actions are taken to prevent further FTP traffic on the device.

To remove a device from the remediation queue

1. Click **Configure | Intel vPro options | System Defense Remediation**.
2. Select the devices that can have their original System Defense policy restored and click **Remediate**.

To remediate devices with Enhanced System Defense, click **Configure | Intel vPro options | Enhanced System Defense Remediation** in step 1 above.

Intel* vPro Agent Presence configuration

Intel* vPro release 2.x and 3.0 includes an Agent Presence tool that can monitor the presence of software agents on managed devices. You can enable Agent Presence monitoring to ensure that management agents on your devices are continually running, and be alerted when an agent stops even when other, software-based, agents can't detect the problem.

Server Manager uses Intel vPro Agent Presence to monitor two agents: the standard management agent and monitoring service. It is useful in situations where normal monitoring communications are not available. For example, a device's communication layer may not be functioning or the monitoring agent itself may have stopped running. By default, Agent Presence also monitors its own monitoring process so you are alerted if it has stopped running.

Agent Presence monitoring is done by configuring a timer that listens for "heartbeat" messages from management agents on the device, to verify that the agents are running. If a timer expires because it has not received a heartbeat message, Intel vPro sends an alert to the core server.

When you set up Agent Presence configuration, the agent on the device registers with Intel vPro to send the heartbeats directly to Intel vPro; if the heartbeats stop, Intel vPro can then alert the core server through out-of-band communication that the device agent is not responding. Intel vPro sends a platform event trap (PET) alert to the core server with a description of the changed state. By default, this alert is logged with device health. You can configure other alert actions to be initiated when this alert is received (for information about configuring alert actions, see [Configuring alert rulesets](#)).

When you configure Agent Presence monitoring, you can enable or disable monitoring for two agents and set the following values:

- **Heartbeat:** The maximum amount of time (in seconds) that can pass between heartbeat signals. If this time limit is exceeded without a new heartbeat being received, the agent is considered to be not responding. The default value is 120 seconds for the standard management agent and 180 seconds for the monitoring service; the minimum value for both is 30 seconds.
- **Startup time:** The maximum amount of time (in seconds) that can pass after the operating system starts before a heartbeat must be received from the agent. If this time limit is exceeded the agent is considered to be not responding. Agent Presence is configured on Intel vPro when the agent is installed, so this should allow for enough time for the agent to start running and send its first heartbeat. The default value is 360 seconds; the minimum value is 30 seconds.

To edit the Intel vPro Agent Presence configuration

1. Click **Configure | Intel vPro options | Agent Presence**.
2. To disable Agent Presence monitoring on Intel vPro 2.x/3.0 devices, clear the **Enable Agent Presence monitoring** checkbox.
3. To disable monitoring for a specific agent, clear the checkbox next to the agent name. (Even if both these checkboxes are cleared, Agent Presence will continue to monitor its own monitoring process as long as it is enabled).
4. Type a new value in the **Heartbeat** text box to change the maximum allowed time between heartbeats (minimum 30 seconds).
5. Type a new value in the **Startup** text box to change the maximum allowed time for the agent to send its first heartbeat after the operating system starts on the device (minimum 30 seconds; 120 seconds is recommended).

Intel* Centrino Pro wireless support

Intel* Centrino Pro notebooks with wireless capabilities can be managed out-of-band via a wireless LAN connection when they are powered on and the wireless interface is active. If a notebook is in sleep mode, it can be managed out-of-band only if it is connected to a wired LAN and to AC power.

When the notebook is powered up, the Intel Active Management Technology (Intel AMT) chip on the notebook communicates with the wireless LAN driver. If Intel AMT finds a matching profile, the driver will route traffic addressed to the Intel AMT device. Even if there is a problem with the driver, Intel AMT can receive out-of-band management traffic from the wireless network interface.

For wireless management, a Centrino Pro 2.5 notebook needs to have a wireless profile correctly configured by the network administrator so that Intel AMT communication with the notebook is secure. For Centrino Pro 2.6 notebooks, the wireless profile is not required for most management features, but is required to use serial-over-LAN (SOL) and IDE-redirection (IDE-R) functionality.

Important: for Intel AMT to work with a wireless LAN connection, it must share IP addresses with the notebook. To do this, Intel AMT must be configured to use DHCP and there must be a DHCP server available to allocate IP addresses. If Intel AMT is configured to use static IP addresses, wireless connectivity will be disabled.

Server Manager lets you define a wireless profile for Intel Centrino Pro notebooks so you can manage them out of band as described above. When you define a profile you can then deploy it to one or more devices.

To create and deploy an Intel vPro wireless profile

1. In the **All devices** list, right-click a managed Intel vPro device and select **Intel vPro Wireless Profiles**.
2. Click **Create Profile**.
3. Under **Profile configuration**, enter the following information:
 - Profile name:** a descriptive name for the profile.
 - SSID:** the network name of the wireless network.
 - Authentication:** select a method for managing wireless authentication, either Wi-Fi Protected Access (WPA-PSK) or Robust Secure Network (RSN-PSK).
 - Encryption:** select an encryption algorithm for wireless communication, either Temporal Key Integrity Protocol (TKIP) or Counter Mode CBC MAC Protocol (CCMP).
 - Passphrase:** enter and confirm a passphrase or 802.1x profile for authentication.
4. Click **OK**.
5. To edit or delete a profile, select the profile and click **Modify profile** or **Delete profile**.
6. To deploy the wireless profile to the device, select the profile in the list and click **Set profile**. To deploy the same profile to another Intel vPro device, right-click the device, select **Intel vPro Wireless Profiles**, select the profile from the list, and click **Set profile**.

When a notebook has been discovered and provisioned while connected to a wired network, it can be managed through the wired network immediately. However, when the notebook switches to a wireless connection there can be a delay before Intel vPro management is enabled for the notebook. This is due to a change in how the computer name is resolved in DNS on the network. The wireless IP address for the notebook is different than the IP address on the wired network, so there is a delay before the new IP address for the notebook matches the computer name.

Role-based administration

Role-based administration enhances LANDesk network security by enabling you to control user access to managed devices, console views, and specific features and tools. This chapter describes how role-based administration works and how you can implement it to effectively administer your LANDesk-managed network.

Read this chapter to learn about:

- "Role-based administration overview" on page 59
- "Managing LANDesk users" on page 61
- "Managing groups" on page 64
- "Understanding rights" on page 66
- "Creating scopes" on page 404
- "Assigning rights and scope to users" on page 75

Role-based administration overview

Role-based administration lets you manage who can access devices on your network and what tools or specific features they can use on those devices. LANDesk Administrators have full rights, which allows them to access all areas of the application and assign special rights to users (click **Tools | Administration | Users**). Groups and organizational units (OUs) from a directory service can also be assigned rights, which are propagated (or enumerated) to users belonging to the group or OU.

- **Rights:** Determine the tools and features a user can see and use (see "Understanding rights" on page 66).
- **Scopes:** Determine the range of devices a user can see and manage (see "Creating scopes" on page 404).

Note: Users who don't have the Administrator right won't see the Users tool.

You can create roles based on user responsibilities, the management tasks you want them to be able to perform, and the devices you want them to be able to see, access, and manage. Access to devices can be restricted to a geographic location like a country, region, state, city or even a single office or department. Or, access can be restricted to a particular device platform, processor type, or some other device hardware or software attribute. With role-based administration, it's completely up to you how many different roles you want to create, which users can act in those roles, and how large or small their device access scope should be. For example, you can have one or more users whose role is software distribution manager, another user who is responsible for remote control operations, a user who runs reports, and so on.

Example administrative roles

The table below lists some of the possible Management Suite administrative roles you might want to implement, the common tasks that user would perform, and the rights that user would need in order to function effectively in that role.

Role	Tasks	Required rights
Administrator	Configure core servers, install additional consoles, perform database rollup, manage users, configure alerts, integrate LANDesk System Manager, and so on. (Of course, administrators with full rights can perform any management tasks.)	LANDesk administrator (all rights implied)
Device inventory manager	Discover devices, configure devices, run the inventory scanner, create and distribute custom data forms, enable inventory history tracking, and so on.	Unmanaged device discovery, software distribution, software distribution configuration, and public query management
Helpdesk	Remotely control devices, chat, transfer files, execute software, shutdown, reboot, view agent and health status, and so on.	Remote control
Application manager	Distribute software packages, use Targeted Multicast and peer download, and so on.	Software distribution and software distribution configuration
Migration manager	Create images, deploy OS images, migrate user profiles, create and distribute user-initiated profile migration packages, deploy PXE representatives, assign PXE holding queues, configure the PXE boot menu, create boot floppy disks, and so on.	OS deployment
Reporting manager	Run predefined reports, create custom reports, print reports, publish reports, import and export reports, test user reports, and so on.	Reports (required for all reports)
Software license monitoring manager	Configure applications to monitor, add licenses, upgrade and downgrade licenses, verify reports, and so on.	Software license monitoring
Security manager	Download security content updates and patches, configure devices for security and antivirus scanning, create vulnerability scans and configure	Security and patch manager Security and patch

Role	Tasks	Required rights
	security scanner settings, create antivirus scans and configure antivirus settings, edit custom variables and configure custom variable override settings, and many more security-related tasks.	compliance Antivirus Edit Custom Variables

Note: Some of the example administrative roles would require the Basic Web console right in order to use the features in the Web console.

These are just example administrative roles. Role-based administration is flexible enough to let you create as many custom roles as you need. You can assign the same few rights to different users but restrict their access to a limited set of devices with a narrow scope. Even an administrator can be restricted by scope, essentially making them an administrator over a specific geographic region or type of managed device. How you take advantage of role-based administration depends on your network and staffing resources, as well as your particular needs.

To implement and enforce role-based administration, simply designate current NT users, or create and add new NT users as LANDesk users, and then assign the necessary rights (to features) and scopes (to managed devices).

Managing LANDesk users

LANDesk users can log in to the console and perform specific tasks for specific devices on the network. Users appear in the **All Users** group (click **Tools | Administration | Users | All users**) after they have been created and added to the Windows NT **LANDesk Management Suite** group on the core server (see "Adding LANDesk users" on page 62). The **All Users** group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

The user that is logged in to the server during LANDesk installation is automatically placed into the Windows NT **LANDesk Management Suite group**, added as a LANDesk user, and assigned rights as an administrator. This individual is responsible for adding additional users to the console and assigning rights and scopes. Once other administrators have been created, they can perform the same administrative tasks

All users added to the console after LANDesk has been installed assume the same rights and scope as the **Default Template User**. This user serves as a template of user properties (rights and scopes) that is used to configure new users. When users are added to the LANDesk Management Suite group in the Windows NT environment, the users automatically inherit the same rights and scopes currently defined in the Default Template User properties. You can change the property settings for the Default Template User by right-clicking it and then clicking **Properties**. Being able to configure the rights and scopes that users receive upon being added to the console greatly facilitates user management. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group.

Note: The Default Template User cannot be removed.

When you add a user to the console, their user name, scopes, and rights are displayed. Additionally, new user subgroups, named by the user's unique login ID, are created in the **User devices**, **User queries**, **User reports**, and **User scripts** groups (note that besides the actual user, ONLY an administrator can view user groups). To refresh the **All users** group to display any newly added users, right-click **All users** and click **Refresh**.

Creating LANDesk users

LANDesk users can be created from the console or from the native local accounts management system on the core server.

To create a LANDesk user from the console

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Users** and then click **Add**. Note that you can only manage local users here, not domain users.
4. In the **New User** dialog, enter a user name, a full name, and a description.
5. Enter a password, confirm the password, and specify the password settings.
6. Click **Save**.

Note: Remember to add the user to the LANDesk Management Suite group to have them appear in the All Users group in the console.

To create a LANDesk user from the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the **New User** dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The New User dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.

Note: Remember to add the user to the LANDesk Management Suite group to have them appear in the All Users group in the console.

Adding LANDesk users

LANDesk users need to be added to the LANDesk Management Suite group in order to be recognized as LANDesk users and appear in the console. Other domain groups can also be added to the LANDesk Management Suite group. If you add a domain group to the LANDesk Management Suite group, all users in the domain group are enumerated and added as console users. LANDesk only allows a single enumeration, so any additional domain groups under the top-tier domain group are ignored.

To add users to the LANDesk Management Suite group from the console

1. In the console, from the **Network View**, click **Devices | All devices**.

2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the **LANDesk Management Suite** group, and then click **Edit**.
5. In the **Edit group - LANDesk Management Suite** dialog, click **Add**.
6. In the **Select users** dialog, select the desired users and then click **Add>>**.
7. Click **OK**.
8. In the **Edit group - LANDesk Management Suite** dialog, click **OK**.

To add users to the LANDesk Management Suite group from the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Groups | Groups** utility.
2. Right-click the **LANDesk Management Suite** group, and then click **Add to group**.
3. In the **LANDesk Management Suite Properties** dialog, click **Add**.
4. In the **Select the users and groups** dialog, select the desired users (and groups) from the list and click **Add**.
5. Click **OK**.
6. In the **LANDesk Management Suite Properties** dialog, click **OK**.

Note: You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the Users list, clicking **Properties | Member Of**, and then clicking **Add** to select the group and add the user.

You can now assign your LANDesk users rights and scopes.

Removing LANDesk users

If you remove a user from the LANDesk Management Suite group from the console or the Windows NT users environment, the user still appears in the **All users** group, but has a red X through it, indicating it is no longer included as a member of that group, and cannot authenticate to any LANDesk console. The user's account still exists in the database and can be added back to the LANDesk Management Suite group at any time. Also, the user's subgroups under **User devices**, **User queries**, **User reports**, and **User scripts** are preserved so that you can restore the user without losing their data, and so that you can copy data to other users. You can also permanently delete a user from the database.

WARNING: When you delete a user from the database, all of the data owned by that user is permanently deleted, including scripts, tasks, queries, and so on.

To remove a user using the console

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to remove and then click **Delete**.
5. Click **Yes** to verify the procedure.

To remove a user using the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click the user you want to remove and then click **Delete**.
3. Click **Yes** to verify the procedure.

To permanently delete a user from the database

1. Make sure the user has been removed from the **LANDesk Management Suite** Windows NT group using the console or the Windows NT computer management dialog.
2. In the console, click **Tools | Administration | Users**.
3. Right-click the user (with a red X) and then click **Delete**. Remember, this action will result in permanent loss of the user data.
4. Click **Yes** to verify the procedure.

Managing groups

LANDesk interfaces with Microsoft Active Directory Services* (ADS) in order to assign rights to groups and organizational units (OUs). Any users, groups or OUs added to the group or OU will inherit the same rights.

You can categorize users by placing them into groups and OUs that have specific rights assigned to them. You only need to assign the group or OU the specific rights and then add the desired users, as opposed to configuring the rights for every single user, one user at a time. This simplifies user management and accelerates the appropriation of rights, as well as reduces the potential of misappropriating rights to users.

Using active directories

LANDesk enables you to utilize active directories to add groups and organizational units (OUs) to the console and assign them rights. You can authenticate to the server from the console. Once you have logged in to the active directory server, you can add groups and OUs to the console and assign rights to them. LANDesk supports using one LDAP directory at a time.

Managing active directories should be performed by an expert user with extensive experience working with directory services, specifically ADS. Tasks include adding and removing users and groups, maintaining the framework (forest, trees, domains, groups, OUs, etc.), and understanding LANDesk's interaction with the directory service. You should be aware of the following issues when managing active directories for use with LANDesk:

- Active directory is fully integrated with DNS and TCP/IP (DNS) is required, and to be fully functional, the DNS server must support SRV resource records or service records .
- Using active directory to add a user to a group being used in the console will not enable the user to log in to the console even though the user has LANDesk rights assigned. In order to log in to the console, a user must belong to the **LANDesk Management Suite** Windows NT group on the core server.

- In order for active directories to work properly with role-based administration, you need to configure the COM+ server credentials on the core server. This enables the core server to use an account in the **LANDesk Management Suite** Windows NT group that has the necessary rights to enumerate Windows domain members, such as the administrator account. For instructions on how to perform the configuration, see [Configuring COM+ server credentials](#).

For more information about LDAP, including LDAP queries, see "More about the Lightweight Directory Access Protocol (LDAP) " on page 112.

Logging in to the active directory

You need to log in to the active directory before you can add groups and organizational units to the console.

To login to the active directory

1. Click **Tools | Administration | Users**.
2. Click the **Login to Active Directory** button.
3. In the **Login to Active Directory** dialog, insert the path to the LDAP directory and provide the user name and password to authenticate to the server.
4. Click **OK**.

Adding groups and organizational units to the console

You need to add LDAP groups and organizational units (OUs) to the console before you can assign rights to them.

To add groups and OUs

1. Click **Tools | Administration | Users**.
2. Click **Active directory**.
3. Click the **Add a new group or OU** button.
4. In the **Available Active Directory groups and OUs** dialog, select the desired groups and OUs and click **OK**.

Assigning rights to a group or organizational unit

You can assign rights to groups and organizational units (OUs). Any user, group, or OU placed into the group or OU will inherit the rights you assign. This enables you to assign the same rights to multiple nodes at one time, rather than having to configure rights individually.



To assign rights to a group or OU

1. Click **Tools | Administration | Users**.
2. Click **Active Directories**.
3. Right-click the desired group or OU and click **Properties**.
4. Under the Rights tab, select the appropriate rights and click **OK**.

Understanding rights

Rights provide access to specific LANDesk tools and features. Users must have the necessary right (or rights) to perform corresponding tasks. For example, in order to remote control devices in their scope, a user must have the remote control right. A user, group, or organizational unit (OU) can be assigned rights, and they can also inherit rights by being added to a group or OU.

From the Users tool, you can see what rights are assigned or inherited:

-  This icon denotes an assigned right.
-  This icon denotes an inherited right.

Role-based administration includes the following rights:

- LANDesk Administrator
- Agent configuration
- Alerting
- Asset configuration
- Asset data entry
- Basic Web console
- Connection control manager
- OS deployment
- Provisioning - configuration
- Provisioning - scheduling
- Public query management
- Remote control
- Reports
- Security and Patch Manager
 - Patch manager
 - Patch compliance
 - Antivirus
 - Edit patch custom variables
- Host intrusion prevention system
- Software distribution
 - Software distribution configuration (private only)
 - Software distribution configuration (public/private)
- Software license monitoring
- Unmanaged device discovery

See the descriptions below to learn more about each right and how rights can be used to create administrative roles.

Scope controls access to devices

Keep in mind that when using the features allowed by these rights, users will always be limited by their scope (the devices they can see and manipulate).

LANDesk Administrator

The LANDesk Administrator (Admin) right provides full access to all of the application tools (however, use of these tools is still limited to the devices included in the administrator's scope).

This is the default right for a newly-added user, unless you've modified the settings for the Default Template User.

The LANDesk Administrator right provides users the ability to:

- See and access the **Users** tool in the **Tools** menu and **Toolbox**
- See and manage **User device** groups in the **Network view**
- See and manage **User query** groups in the **Network view**
- See and manage **User scripts** groups in the **Manage scripts** window
- See and manage **User reports** groups in the **Reports** window
- See and configure product licensing in the **Configure** menu
- See and manage the **Executive dashboard** (only administrators are provided with a link in the Web console to access the executive dashboard)
- **Important:** Perform ALL of the Management Suite tasks allowed by the other rights

Basic rules about rights and tools

The LANDesk Administrator right is exclusively associated with the **Users** tool. In other words, if a user doesn't have the LANDesk Administrator right, the **Users** tool won't appear in the console.

All users, regardless of their assigned rights, can see and use the following universal features: inventory options, alert history, queries, and alert settings.

All of the other tools in the Management Suite console are associated with a corresponding right (as described below).

Agent configuration

The agent configuration right provides users the ability to open the agent configuration tool and schedule an agent configuration task.

Alerting

The alerting configuration right provides users the ability to open the alerting tool and configure alerts.

Asset configuration

The asset configuration right is specific to the Asset Manager add-on product. When an add-on product isn't installed, its corresponding rights still appear in LDMS in the list (checked in LDMS but are dimmed). The respective add-on product's tools and features aren't available, of course. After an add-on product is installed, its respective rights are activated in this list, and can be checked to allow access to the add-on's features or cleared to deny access. For more information, see [Using the Asset Manager add-on](#).

The Asset Configuration is an administration-level right that provides users the ability to:

- See and access all the Asset Management links in the Web console: Assets, Contracts, Invoices, Projects, Global Lists, Detail Templates, and Reports. (And the new Asset Access link.)
- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset data entry

The asset data entry right is specific to the Asset Manager add-on product. When an add-on product isn't installed, its corresponding rights still appear in LDMS in the list (checked but are dimmed). The respective add-on product's tools and features aren't available, of course. After an add-on product is installed, its respective rights are activated in this list, and can be checked to allow access to the add-on's features or cleared to deny access. For more information, see [Using the Asset Manager add-on](#).

The asset data entry right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global Lists links in the Web console.
- Browse types and details (can't add, edit, or delete them)
- Add items to the database by completing in data entry forms
- Edit items that have been added to the database

Basic Web console

The basic Web console right applies to the Web console. The right provides users the ability to:

- See and use **My devices** (the right doesn't allow for the updating of public groups or deleting devices under the Actions tab)
- Change preferences (but not custom attributes)
- Use the dashboard
- Use software distribution on the Web console
- Use the executive dashboard (URL must be provided by an administrator)

Connection control manager

The connection control manager right provides users the ability to:

- See and access the connection control configuration tool in the **Tools** menu and **Toolbox**
- Control the access to external devices to control and configure them

OS deployment

The OS deployment right provides users the ability to:

- See and access the **Manage Scripts** tool in the **Tools** menu and **Toolbox**
- Create and run OS deployment and profile migration scripts
- Schedule OS deployment and profile migration tasks
- Configure PXE representatives with the Deploy PXE Representative script
- Designate PXE holding queues
- Configure the PXE boot menu
- Create and deploy customer data forms

Provisioning-configuration

The provisioning-configuration right lets users create and modify provisioning templates.

Provisioning-scheduling

The provisioning-scheduling right lets users schedule existing provisioning templates for execution on targeted devices.

Public query management

The public query management right provides users the ability to:

- Create, modify, copy, delete, and move queries in the **Public queries** group in the **Network view**. (Without this right, the devices in the **Public query** group are view-only.)

Remote control tools

The remote control tools right provides users the ability to:

- Use the remote control options on a device's shortcut menu (otherwise, they are dimmed)
- Remote control devices that have the remote control agent loaded
- Wake up, shut down, and reboot devices
- Chat with devices
- Execute device programs remotely
- Transfer files to and from devices
- View only

Click the **Remote Control Settings** button at the bottom of the dialog to configure specific remote control rights and time constraints.

Reports

In order to use the reports tool, you must be a member of the Windows NT **LANDesk Reports** group and be given the reports right. The reports right provides users the ability to:

- See and access the **Reports** tool in the **Tools** menu and **Toolbox**
- Run predefined reports
- View reports that have been run
- Create and run custom asset reports
- Publish reports in order to make them available to users with access credentials

Security and Patch Manager

The security and Patch Manager right provides users the ability to:

- See and access the **Security and Patch Manager** tool in the **Tools** menu and **Toolbox**
- Configure managed devices for security assessment and remediation scanning
- Configure devices for real-time spyware and blocked application scanning
- Configure devices for high frequency scanning for critical security risks
- Download security updates (definitions and detection rules and associated patches) for the security types that you have a Security Suite content subscription for
- Create scheduled tasks that automatically download definitions and/or patch updates
- Create custom vulnerability definitions and custom detection rules
- Import, export, and delete custom definitions
- View downloaded security and patch content by type (including: all types, blocked applications, custom definitions, LANDesk updates, security threats, spyware, vulnerabilities, driver updates, and software updates)
- Customize selected security threats with custom variables
- Configure and run security scans on managed devices as a scheduled task or as a policy
- Divide a scheduled task scan into a staging phase and a deployment phase
- Create and configure scan and repair settings that determine the scan options, such as: content type to be scanned for, scanner information and progress display, device reboot behavior, and the amount of end user interaction. Then, apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks
- View detailed scan results (detected security data) by: detected group, specific definition, individual device, or a group of selected devices
- Perform remediation as a scheduled task or as a policy
- Use Auto Fix to automatically remediate the following security types if they are detected: vulnerabilities, spyware, LANDesk software updates, and custom definitions (must be a LANDesk Administrator)
- Track and verify the status of patch deployment and installation (repair) history on scanned devices
- Purge unused security type definitions (must be a LANDesk Administrator)
- Uninstall patches from scanned devices
- Remove patches from the core database
- Configure vulnerability alerts
- Generate a variety of security related reports (also requires the Reports right)

Security and patch compliance

The security and patch compliance right is a subordinate right to the Security and Patch Manager right. It extends the users ability to:

- Add and remove security definitions from the **Compliance** group

- Change the status of definitions contained in the Compliance group
- **Note:** Even with this right a user can't configure LANDesk NAC services, such as adding posture servers or remediation servers, or configure and publish compliance rules. A user must be a LANDesk Administrator in order to configure LANDesk NAC.

Antivirus

The antivirus right is a subordinate right to the Security and Patch Manager right. It extends the users ability to:

- Deploy agent configurations with LANDesk Antivirus to target devices
- Download virus definition file updates
- Create scheduled virus definition file updates
- Create scheduled antivirus scan tasks
- Create and edit antivirus settings
- Enable real-time file and email protection
- Configure antivirus scans to scan for certain file types
- Exclude certain files, folders, and file types (by extension) from antivirus scans
- View antivirus scan activity and status information for scanned devices
- Enable antivirus alerts
- Generate antivirus reports

Edit custom variables

The edit custom variables right is a subordinate right to the security and Patch Manager right. It extends the users ability to:

- Edit custom variable values (for security content types with custom variables, such as security threats)
- Enable a custom variable's override option in order to ignore the modified value and scan for the original value
- Create and deploy a change settings task that includes custom variable override settings

Software distribution

The software distribution right provides users the ability to:

- See and access the **Manage Scripts** tool in the **Tools** menu and **Toolbox**. Users can create custom scripts, local scheduler scripts, and file transfer scripts.
- See and access the **Scheduled Tasks** tool in the **Tools** menu and **Toolbox**. Users can schedule custom scripts, local scheduler scripts, and file transfer scripts.
- See and access the **Delivery Methods** and **Distribution Packages** tools in the **Tools** menu and **Toolbox** (can only select items)
- Run software distribution scripts. User's can create and schedule custom scripts, Local Scheduler Scripts, and File Transfer scripts.
- Run device agent configurations (can't create, edit, or delete)
- Schedule other script-based tasks (with the exception of OS deployment and profile migration scripts)

- Deploy custom data forms. Users can create, edit, and delete custom forms, including forms created by other users.
- View LDAP directories

Note: Users require the basic Web console right to use software distribution on the Web console.

Configuration-private only

The configuration-private only right is a subordinate right to the software distribution right. It extends the users ability to perform the following tasks for themselves only, not other (public) users:

- Create, modify, and delete delivery methods and distribution packages
- Create and run software distribution scripts
- Create and run device agent configurations
- Schedule other script-based tasks (with the exception of OS deployment and profile migration scripts)
- Create and deploy custom data forms
- Create and distribute software packages through application policies

Configuration-public and private

The configuration-public and private right is a subordinate right to the Configuration - private only right and the software distribution right. It extends the users ability to perform all software distribution tasks given in the configuration-private only right for other users, in addition to themselves.

Software license monitoring

The software license monitoring right provides users the ability to:

- See and access the **Software license monitoring** tool in the **Tools** menu and **Toolbox**
- Configure applications to monitor, add licenses, upgrade and downgrade licenses, and verify reports

Unmanaged device discovery

The unmanaged device discovery right provides users the ability to:

- See and access the **Unmanaged device discovery** tool in the **Tools** menu and **Toolbox**
- Create scanner configurations and run different types of discovery scans (LANDesk agent, NT Domain, etc.)
- Create and run the different types of discovery scan tasks

Creating scopes

A scope defines the devices that can be viewed and managed by a Management Suite user.

A scope can be as large or small as you want, encompassing all of the managed devices scanned into a core database, or possibly just a single device. This flexibility, combined with modularized tool access, is what makes role-based administration such a versatile management feature.

Default scopes

Management Suite's role-based administration includes one default scope. This predefined scope can be useful when configuring the user properties of the Default Template User.

- **Default all machines scope:** Includes all managed devices in the database.

You can't edit or remove the default scope.

Custom scopes

There are three types of custom scopes you can create and assign to users:

- **LDMS query:** Controls access to only those devices that match a custom query search. You can select an existing query or create new queries from the Scope properties dialog to define a scope. Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group. For more information on creating queries, see "Creating database queries" on page 105.
- **LDAP:** Controls access to only those devices gathered by the inventory scanner that are located in an LDAP-compliant directory structure. Select directory locations from the **Select visible devices** dialog to define a scope. This directory-based scope type also supports custom directory locations (if you've entered custom directory paths as part of an agent configuration). Available custom directory paths appear in the **Select visible devices** dialog. Use custom directories to define a scope if you don't have an LDAP-compliant structure, or if you want to be able to restrict access to devices by a specific organizational detail such as geographic location or department.
- **Device group:** Controls access to only those devices that belong to a specific device group in the network view.

A Management Suite user can be assigned one or more scopes at a time. Additionally, a scope can be associated with multiple users.

How multiple scopes work

You can assign more than one scope to any of your Management Suite users. When multiple scopes are assigned to a user, the cumulative effective scope (the complete range of devices that can be accessed and managed) as a result of the combination of assigned scopes is a simple composite.

You can customize a user's effective scope by adding and removing scopes at any time. All three types of scopes can be used together.

Creating scopes

To create a scope

1. Click **Tools | Administration | Users**.
2. Right-click **Scopes** and select **New Scope**.
3. In the **Scope Properties** dialog, enter a name for the new scope.
4. Specify the type of scope you want to create (LDMS query, LDAP or custom directory, or device group) by clicking the desired scope type from the drop-down list, and then clicking **New**.
5. If you're creating an LDMS query-based scope, define the query in the **New scope query** dialog, and then click **OK**.
6. If you're creating an directory-based scope, select locations (LDAP directory and/or custom directory) from the **Select visible devices** list, and then click **OK**.

Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.

LDAP directory locations are determined by a device's directory service location. For more information, see "Using active directories" on page 64. Custom directory locations are determined by a device's computer location attribute in the inventory database. This attribute is defined during device agent configuration.

7. If you're creating a device group-based scope, select a group from the available device group list, and then click **OK**.
8. Click **OK** again to save the scope and close the dialog.

About the Scope Properties dialog

Use this dialog to create or edit a scope. You can access this dialog by selecting a scope and clicking the **Edit scope** toolbar button or by right-clicking the scope and then clicking **Properties**.

- **Scope name:** Identifies the scope.
- **Select a scope type:**
 - **LDMS query:** Creates a scope whose device range is determined by a custom query. Clicking **New** with this scope type selected opens the **New query** dialog where you can define and save a query. This is the same query dialog you use when creating a database query from the network view. (Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group.)
 - **LDAP:** Creates a scope whose device range is determined by the device location (LDAP directory and/or custom directory). Clicking **New** with this scope type selected opens the **Select visible devices** dialog where you can select locations. Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.

- **Device group:** Creates a scope whose device range is determined by an existing group of devices contained under the Devices object in the network view. Clicking **New** with this scope type selected opens the **Query filter** dialog where you can select a device group.
- **Current scope definition:** Displays the query statements for a query-based scope, the location paths for a directory-based scope, or the group name for a device group-based scope.
- **Edit:** Opens the scope's appropriate dialog where you can change query parameters and statements.
- **OK:** Saves the scope and closes the dialog.
- **Cancel:** Closes the dialog without saving any of your changes.

Assigning rights and scope to users

Once you've added LANDesk users, learned about rights and how they control access to features and tools, and created device scopes to allow or restrict access to managed devices, the next step in establishing role-based administration is to assign the appropriate rights and scopes to each user.

A user's role is completely configurable. They can have any combination of rights. Additionally, they can be assigned one or more scopes (see "How multiple scopes work" on page 73).

You can modify a user's rights and scopes at any time.

If you modify a user's rights or scopes, those changes will only take affect the next time that user logs into the core server.

To assign rights and scope to a user

1. Click **Tools | Administration | Users**.
2. Select the **All users** group to view all of the users that are currently a member of the LANDesk Management Suite group in the core server's Windows NT environment.

The right-side pane displays a list of users, including their user name, current scope, and assigned rights (an x character indicates the right is enabled or active).

You can refresh this list by right-clicking **All users** and clicking **Refresh**.

3. Right-click a user, and then click **Properties**.
4. In the **User properties** dialog, click the **Rights** tab, and then check or clear rights as desired (see "Understanding rights" on page 66).
5. Click the **Scopes** tab, and then define a composite scope for the selected user by adding and removing scopes. For more information, see "How multiple scopes work" on page 73.
6. Click **OK**.

The new rights and scope display next to the user's name in the list and will take affect the next time the user connects to the core server.

Note: If the user has more than one assigned scope, the **Scope** column says "Multiple".

Configuring services

Many of the most integral and fundamental functions provided by LANDesk components, such as the inventory server and the scheduler service, can and should be configured in order to optimize performance in your particular network environment. Do this by using the **LANDesk Configure services** applet that you can launch from the **LANDesk Start** menu program group.

Configuring services is restricted to only LANDesk Administrators

Only a user with the LANDesk Administrator right can modify service settings. Also, the **Configure services** option is available only from the main console, not from any additional consoles you may have set up.

Read this chapter to learn about:

- "Selecting a core server and database with General settings" on page 76
- "Configuring the Inventory service" on page 77
- "Resolving duplicate device records in the database" on page 78
- "Configuring the scheduler service" on page 80
- "Configuring preferred server credentials" on page 82
- "Configuring the custom jobs service" on page 82
- "Configuring the Multicast service" on page 84
- "Configuring the OS deployment service" on page 84
- [Managing Intel* vPro devices](#)

Selecting a core server and database with General settings

Before configuring a service, use the **General** tab to specify the core server and database you want to configure the service for.

Note: Any service configuration changes you make for a core server and database will not take affect until you restart the service on that core server.

About the Configure Management Suite services dialog: General tab

Use this dialog to select the core server and database you want to configure a specific service for. Then, select the desired service tab and specify the settings for that service.

- **Server name:** Displays the name of the core server you're currently connected to.
- **Server:** Lets you enter the name of a different core server and its database directory.
- **Database:** Lets you enter the name of the core database.
- **User name:** Identifies a user with authentication credentials to the core database (specified during setup).
- **Password:** Identifies the user's password required to access the core database (specified during setup).

- **This is an Oracle database:** Indicates that the core database specified above is an Oracle database.
- **Refresh settings:** Restores the settings that were present when you opened the dialog.

When specifying usernames and passwords to a database, the username and the password may not contain an apostrophe ('), a semicolon (;) or an equals sign (=).

Configuring the Inventory service

Use the **Inventory** tab to configure the Inventory service for the core server and database you selected using the General tab.

About the Configure Management Suite services dialog: Inventory tab

Use this tab to specify the following inventory options:

- **Server name:** Displays the name of the core server you're currently connected to.
- **Log statistics:** Keeps a log of core database actions and statistics. You can view the log data in the Windows **Event Viewer's Application** log.
- **Encrypted data transport:** Enables the inventory scanner to send device inventory data from the scanned device back to the core server as encrypted data through SSL.
- **Scan server at:** Specifies the time to scan the core server.
- **Perform maintenance at:** Specifies the time to perform standard core database maintenance.
- **Days to keep inventory scans:** Sets the number of days before the inventory scan record is deleted.
- **Primary owner logins:** Sets the number of times the inventory scanner tracks logins to determine the primary owner of a device. The primary owner is the user who has logged in the most times within this specified number of logins. The default value is 5 and the minimum and maximum values are 1 and 16, respectively. If all of the logins are unique, the last user to log in is considered the primary owner. A device can have only one primary owner associated with it at a time. Primary user login data includes the user's fully qualified name in either ADS, NDS, domain name, or local name format (in that order), as well as the date of the last login.
- **Advanced:** Displays the **Advanced settings** dialog. You can change inventory-related advanced settings here. As you click each item, help text appears at the bottom of the dialog explaining each option. The default values should be fine for most installations. To change a setting, click it, change the **Value**, then click **Set**. Restart the inventory service when you're done.
- **Software:** Displays the **Software scan settings** dialog. Configure when the software scans run and how long to save the inventory history.
- **Manage duplicates: Devices:** Opens the **Duplicate devices** dialog, where you can configure how duplicate devices are handled.
- **Manage duplicates: Device IDs:** Opens the **Duplicate device ID** dialog, where you can select attributes that uniquely identify devices. You can use this option to avoid having duplicate device IDs scanned into the core database (see "Resolving duplicate device records in the database" on page 78).

- **Inventory service status:** Indicates whether the service is started or stopped on the core server.
- **Start:** Starts the service on the core server.
- **Stop:** Stops the service on the core server.
- **Restart:** Restarts the service on the core server.

About the Software scan settings dialog

Use this dialog (**Configure | Services | Inventory** tab | **Software** button) to configure the frequency of software scans. A device's hardware is scanned each time the inventory scanner is run on the device, but the device's software is scanned only at the interval you specify here.

- **Every login:** Scans all of the software installed on the device every time the user logs on.
- **Once every (days) :** Scans the device's software only on the specified daily interval, as an automatic scan.
- **Save history (days) :** Specifies how long the device's inventory history is saved.

Configuring what inventory scan attributes get stored in the database

The inventory scanner looks for hundreds of inventory items. If you don't need all of this scan information in your database, you can speed up scan insertion time and reduce your database size by limiting the number of scan attributes that get stored in the database. When you do this, managed devices still submit complete inventory scans, but the core server's inventory service only stores the attributes you specify in the database.

By default, the inventory service inserts all scan attributes into the database. Any attribute filtering changes you make won't affect data that is already in the database. To limit what data gets stored, follow the steps below.

To set up inventory scan data filtering

1. Click **Configure | Services | Inventory** tab | **Attributes** button.
2. Attributes in the **Selected attributes** column on the right get inserted into the database. Move the attributes you don't want in the database to the **Available attributes** column on the left.
3. Restart the inventory service by clicking **Restart** on the Inventory tab.
4. Click **OK**.

Resolving duplicate device records in the database

In some environments OS imaging is used regularly and frequently to set up devices. Because of this, the possibility of duplicate device IDs among devices is increased. You can avoid this problem by specifying other device attributes that, combined with the device ID, create a unique identifier for your devices. Examples of these other attributes include device name, domain name, BIOS, bus, coprocessor, and so on.

The duplicate ID feature lets you select device attributes that can be used to uniquely identify the device. You specify what these attributes are and how many of them must be missed before the device is designated as a duplicate of another device. If the inventory scanner detects a duplicate device, it writes an event in the applications event log to indicate the device ID of the duplicate device.

In addition to duplicate device IDs, you may also have duplicate device names or MAC addresses that have accumulated in the database. If you're experiencing persistent duplicate device problems (and as a precaution against duplicate device records being scanned into your database by the inventory scanner in the future), you can also specify that any duplicate device names currently residing in the database are removed. This supplementary duplicate device handling feature is included as part of the procedure below.

To set up duplicate device handling

1. Click **Configure | Services | Inventory | Device IDs**.
2. Select attributes from the Attributes list that you want to use to uniquely identify a device, and then click the right-arrow button to add the attribute to the Identity Attributes list. You can add as many attributes as you like.
3. Select the number of identity attributes (and hardware attributes) that a device must fail to match before it's designated as a duplicate of another device.
4. If you want the inventory scanner to reject duplicate device IDs, check the **Reject duplicate identities** option.
5. Click **OK** to save your settings and return to the **Configure Inventory** dialog.
6. (Optional) If you also want to resolve duplicate devices by name and/or address, click **Devices** to open the **Duplicate Devices** dialog where you can specify the conditions when duplicate devices are removed, such as when device names match, MAC addresses match, or both match.

About the Duplicate Device ID dialog

Use this dialog (click **Configure | Services | Inventory** tab | **Device IDs** button) to set up duplicate device ID handling.

- **Attributes list:** Lists all of the attributes you can choose from to uniquely identify a device.
- **Identity attributes:** Displays the attributes you've selected to uniquely identify a device.
- **Duplicate device ID triggers:**
 - **Log as a duplicate device ID when:** Identifies the number of attributes that a device must fail to match before it's designated as a duplicate of another device.
 - **Reject duplicate identities:** Causes the inventory scanner to record the device ID of the duplicate device and reject any subsequent attempts to scan that device ID. Then, the inventory scanner generates a new device ID.

About the Duplicate Devices dialog

Use this dialog (click **Configure | Services | Inventory** tab | **Devices** button) to specify the name and/or address conditions when duplicate devices are removed from the database. When you have one of the remove duplicate options checked, duplicates are allowed in the database, but they are removed the next time database maintenance happens.

- **Remove duplicate when:**
 - **Device names match:** Removes the older record when two or more device names in the database match.
 - **MAC addresses match:** Removes the older record when two or more MAC addresses in the database match.
 - **Both device names and MAC addresses match:** Removes the older record ONLY when two or more device names and MAC addresses (for the same record) match.
- **Restore old device IDs:** Restores the original device ID from the older record of a scanned device, IF two records for that device exist in the database and at least one of the remove options above is selected and its criteria met, The original device ID is restored when the next inventory maintenance scan runs. This option has no affect unless one of the remove options above is selected.

Configuring the scheduler service

Use the **Scheduler** tab to configure the scheduler service (**Tools | Distribution | Scheduled tasks**) for the core server and database you selected using the **General** tab.

You must have the appropriate rights to perform these tasks, including full administrator privileges to the Windows NT/XP/2000/2003 devices on the network, allowing them to receive package distributions from the core server. You can specify multiple login credentials to use on devices by clicking **Change login**.

One additional setting you can configure manually is the **Scheduled task** window's refresh rate. By default, every two minutes the **Scheduled tasks** window checks the core database to determine if any of the visible items have been updated. If you want to change the refresh rate, navigate to this key in the registry:

- HKEY_CURRENT_USER\Software\LANDesk\ManagementSuite\WinConsole

Set " TaskRefreshIntervalSeconds" to the number of seconds between refreshes for an active task. Set " TaskAutoRefreshIntervalSeconds" to the refresh interval for the whole **Scheduled task** window.

About the Configure Management Suite services dialog: Scheduler tab

Use this tab to see the name of the core server and the database that you selected earlier, and to specify the following scheduled task options:

- **User name:** The username under which the scheduled tasks service will be run. This can be changed by clicking the **Change login** button.
- **Number of seconds between retries:** When a scheduled task is configured with multiple retries, this setting controls the number of seconds the scheduler will wait before retrying the task.
- **Number of seconds to attempt wake up:** When a scheduled task is configured to use Wake On LAN, this setting controls the number of seconds that the scheduled tasks service will wait for a device to wake up.

- **Interval between query evaluations:** A number that indicates the amount of time between query evaluations, and a unit of measure for the number (minutes, hours, days, or weeks).
- **Wake on LAN settings:** The IP port that will be used by the Wake On LAN packet set by the scheduled tasks to wake up devices.
- **Schedule service status:** Indicates whether the service is started or stopped on the core server.
- **Start:** Starts the service on the core server.
- **Stop:** Stops the service on the core server.
- **Restart:** Restarts the service on the core server.
- **Advanced:** Displays the **Advanced scheduler settings** dialog. You can change scheduler-related advanced settings here. As you click each item, help text appears at the bottom of the dialog explaining each option. The default values should be fine for most installations. To change a setting, click it, click **Edit**, enter a new value, then click **OK**. Restart the scheduler service when you're done.

About the Configure Management Suite services dialog: Change login dialog

Use the **Change login** dialog (click **Change login** on the **Scheduler** tab) to change the default scheduler login. You can also specify alternate credentials the scheduler service should try when it needs to execute a task on unmanaged devices.

To install LANDesk agents on unmanaged devices, the scheduler service needs to be able to connect to devices with an administrative account. The default account the scheduler service uses is LocalSystem. The LocalSystem credentials generally work for devices that aren't in a domain. If devices are in a domain, you must specify a domain administrator account.

If you want to change the scheduler service login credentials, you can specify a different domain-level administrative account to use on devices. If you're managing devices across multiple domains, you can add additional credentials the scheduler service can try. If you want to use an account other than LocalSystem for the scheduler service, or if you want to provide alternate credentials, you must specify a primary scheduler service login that has core server administrative rights. Alternate credentials don't require core server administrative rights, but they must have administrative rights on devices.

The scheduler service will try the default credentials and then use each credential you've specified in the **Alternate credentials** list until it's successful or runs out of credentials to try. Credentials you specify are securely encrypted and stored in the core server's registry.

You can set these options for the default scheduler credentials:

- **Username:** Enter the default domain\username or username you want the scheduler to use.
- **Password:** Enter the password for the credentials you specified.
- **Confirm password:** Retype the password to confirm it.

You can set these options for additional scheduler credentials:

- **Add:** Click to add the username and password you specified to the alternate credentials list.
- **Remove:** Click to remove the selected credentials from the list.

- **Modify:** Click to change the selected credentials.

When adding alternate credentials, specify the following:

- **Username:** Enter the username you want the scheduler to use.
- **Domain:** Enter the domain for the username you specified.
- **Password:** Enter the password for the credentials you specified.
- **Confirm password:** Retype the password to confirm it.

Configuring preferred server credentials

There is a **Credentials** button at the bottom of the **Configure LANDesk Software services** dialog. This button launches the **Server credentials** dialog, where you can specify the preferred servers that devices will check for software distribution packages. These preferred servers offload demand on the core server and help you distribute network traffic in low-speed WAN environments where you don't want devices downloading packages from off-site servers. Preferred servers work for every delivery method except multicast. UNC package shares work with all packages. HTTP package shares only work with MSI and SWD packages.

The **User name and password** dialog (click **Add** in the **Server credentials** dialog) has the following options:

- **Description:** A description for this preferred server. The description appears in the **Server credentials** dialog.
- **Server name:** The name of the server that will host packages.
- **User name:** The user name devices will use to log into the server. This user name should allow only read access for security reasons.
- **Password and Confirm password:** The password for the user name you specified.
- **Limit preferred server usage by these IP address ranges:** If you only want devices within a specified IP range to use this preferred server, you can specify the **Starting IP address** and **Ending IP address**, and click **Add**.
- **Test credentials:** Click this button to make sure the server name and credentials you entered work correctly.

When controlling preferred server access through IP address ranges, note that devices within the same multicast domain share their configuration files and may use the same servers, even if some of those devices aren't in a particular preferred server's IP address range.

Configuring the custom jobs service

Use the **Custom jobs** tab to configure the custom jobs service for the core server and database you selected using the General tab. Examples of custom jobs include inventory scans, device deployments, or software distributions.

When you disable TCP remote execute as the remote execute protocol, custom jobs uses the standard LANDesk agent protocol by default, whether it's marked disabled or not. Also, if both TCP remote execute and standard LANDesk agent are enabled, custom jobs tries to use TCP remote execute first, and if it's not present, uses standard LANDesk agent remote execute.

The **Custom jobs** tab also enables you to choose options for device discovery. Before the custom jobs service can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

About the Configure Management Suite services dialog: Custom jobs tab

Use this tab to set the following custom jobs options:

Remote execute options

- **Disable TCP execute:** Disables TCP as the remote execute protocol, and thereby uses the standard LANDesk agent protocol by default.
- **Disable CBA execute / file transfer:** Disables standard LANDesk agent as the remote execute protocol. If standard LANDesk agent is disabled and TCP remote execute protocol is not found on the device, the remote execution will fail.
- **Enable remote execute timeout:** Enables a remote execute timeout and specifies the number of seconds after which the timeout will occur. Remote execute timeouts trigger when the device is sending heartbeats, but the job on the device is hung or in a loop. This setting applies to both protocols (TCP or standard LANDesk agent). This value can be between 300 seconds (5 minutes) and 86400 seconds (1 day).
- **Enable client timeout:** Enables a device timeout and specifies the number of seconds after which the timeout will occur. By default, TCP remote execute sends a heartbeat from device to server in intervals of 45 seconds until the remote execute completes or times out. Device timeouts trigger when the device doesn't send a heartbeat to the server.
- **Remote execute port (Default is 12174):** The port over which the TCP remote execute occurs. If this port is changed, it must also be changed in the device configuration.

Distribution options

- **Distribute to <nn> computers simultaneously:** The maximum number of devices to which the custom job will be distributed simultaneously.

Discovery options

- **UDP:** Selecting UDP uses a LANDesk agent ping via UDP. Most LANDesk device components depend on standard LANDesk agent, so your managed devices should have standard LANDesk agent on them. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping **Retries** and **Timeout**.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

Configuring the Multicast service

Use the **Multicast** tab to configure the multicast domain representative discovery options for the core server and database you selected using the **General** tab.

About the Configure Management Suite services dialog: Multicast tab

Use this tab to set the following multicast options:

- **Use multicast domain representative:** Uses the list of multicast domain representatives stored in the network view's **Configuration | Multicast domain representatives** group.
- **Use cached file:** Queries each multicast domain to find out who might already have the file, therefore not needing to download the file to a representative.
- **Use cached file before preferred domain representative:** Changes the order of discovery to make **Use cached file** the first option attempted.
- **Use broadcast:** Sends a subnet-directed broadcast to find any device in that subnet that could be a multicast domain representative.
- **Log discard period (days):** Specifies the number of days that entries in the log will be retained before being deleted.

Configuring the OS deployment service

Use the **OS deployment** tab to designate PXE representatives as PXE holding queues, and to configure basic PXE boot options for the core server and database you selected using the **General** tab.

PXE holding queues are one method of deploying OS images to PXE-enabled devices. You designate existing PXE representatives (located in the **Configuration** group in the network view) as PXE holding queues. For more information, see "PXE-based deployment" on page 237.

Select and move PXE representatives from the **Available proxies** list to the **Holding queue proxies** list.

About the Configure Management Suite Services dialog: OS Deployment tab

Use this tab to assign PXE holding queue proxies (representatives), and to specify the PXE boot options.

- **Available proxies:** Lists all available PXE proxies on your network, identified by device name. This list is generated when the inventory scanner detects PXE software (PXE and MFTFTP protocols) running on the device.

- **Holding queue proxies:** Lists the PXE proxies that have been moved from the **Available proxies** list, thereby designating the proxy as a PXE holding queue. PXE-enabled devices on the same subnet as the PXE holding queue proxy will be automatically added to the **PXE holding queue** group in the console's network view when they PXE boot. The devices can then be scheduled for an image deployment job.
- **Reset:** Forces all of the PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the **PXE holding queue** group in the console's network view. The devices can then be scheduled for an imaging job. (The Reset button is enabled when you select a PXE proxy in the Holding queue proxies list).

Note: Changes you make here to the PXE boot options will not take effect on any of your PXE representatives until you run the PXE Representative Deployment script on that representative.

- **Timeout:** Indicates how long the boot prompt displays before timing out and resuming the default boot process. The maximum number of seconds you can enter is 60 seconds.
- **Message:** Specifies the PXE boot prompt message that appears on the device. You can type any message you like in the text box, up to 75 characters in length.

Configuring the BMC password

Use the **BMC password** tab to create a password for the IPMI Baseboard Management Controller (BMC). This tab only appears on core servers that include LANDesk Server Manager or LANDesk System Manager.

- In the **BMC password** tab, type a password in the **Password** text box, retype the password in the **Confirm password** text box, then click **OK**.

The password cannot be longer than 15 characters, each of which must be numbers 0-9 or upper/lower case letters a-z.

Configuring device agents

Devices need the Management Suite agents on them to be fully manageable. Read this chapter to learn about:

- "Working with agent configurations" on page 86
- "Creating an agent configuration" on page 87
- "Using the advance agent" on page 88
- "Updating agent preferences on devices" on page 89
- "Creating standalone agent configuration packages" on page 90
- "Agent security and trusted certificates" on page 90
- "Uninstalling device agents" on page 93

The **Agent configuration** window lets you create new agent configurations for Windows, Linux, and Macintosh devices. The agent configurations you create can then be pushed to clients using the console's **Scheduled tasks** window.

Deploying agents to Windows 95/98/NT devices

Management Suite no longer ships with agents that support Windows 95, Windows 98, or Windows NT devices. You can contact LANDesk Customer Care if you need the legacy agent that works with these devices.

Creating device configurations for Windows 2000/2003/XP devices not enabled for management

If you have Windows 2000/2003/XP devices that are part of a Windows 2000/2003/XP domain, you can push a configuration to those devices even if the standard LANDesk agent and the remote control agents aren't present. For more information, see the *Installation and Deployment Guide*.

Working with agent configurations

Management Suite uses agent configurations that you create to deploy agents and agent preferences to managed devices. Once devices have the Management Suite agents on them, you can easily update agent configurations. For more information on initial agent deployment, see the "Deploying the primary agents to clients" chapter in the *Installation and Deployment Guide*.

Read the following sections for more information on:

- Agent configuration changes in Management Suite 8.5
- Creating an agent configuration
- Updating agent preferences on devices
- Creating standalone agent configuration packages

Agent configuration changes in Management Suite 8.5+

Users of Management Suite prior to version 8.5 will notice several agent configuration changes from past releases.

- The standard LANDesk agent is the new name for CBA and it now includes the inventory scanner, local scheduler, security and patch scanner, software monitoring, and bandwidth detection. These components aren't individually selectable and are installed by default. You can also set reboot options in the standard LANDesk agent.
- Application policy management is now called policy-based delivery and it's configured under software distribution.
- Targeted Multicast is supported by software distribution. You don't need to separately enable it or configure it.
- The security and patch scanner agent is installed by default with the standard LANDesk agent. You can configure security scans to determine how and when the security scanner runs on managed devices and whether to show progress and interactive options to the end user. (The security scanner allows you to check for LANDesk software updates on devices and core servers even if you don't have a LANDesk Security Suite content subscription. With a Security Suite subscription you can take full advantage of the security scanner's capability to scan for and remediate known vulnerabilities, spyware, unauthorized applications, viruses, and other potential security risks.)

Creating an agent configuration

Use the **Agent configuration** window to create and update device and server agent configurations (such as what agents are installed on devices and what network protocols the agents use).

You can create different configurations for groups' specific needs. For example, you could create configurations for the devices in your accounting department or for devices using a particular operating system.

To push a configuration to devices, you need to:

- **Create the agent configuration:** Set up specific configurations for your devices.
- **Schedule the agent configuration:** Push the configuration to devices that have the standard LANDesk agent installed. For more information, see "Scripts and tasks" on page 136. Users with administrative rights can also install the default agent configuration by running WSCFG32.EXE or IPSETUP.BAT from the core server's LDLogon share.

To create an agent configuration

1. In the console, click **Tools | Configuration | Agent configuration**.
2. Click the **New** toolbar button.
3. Enter a **Configuration name**.
4. In the **Agent configuration** window's **Start** page, select the agents you want to deploy.
5. Use the tree to navigate the dialogs relating to the options you selected. Customize the options you selected as necessary. Click **Help** for more information if you have questions about a page.
6. Click **Save & Close**.
7. If you want the configuration to be the default (the configuration LDLOGON\WSCFG32.EXE or LDLOGON\IPSETUP.BAT will install), from the configuration's shortcut menu, click **Default configuration**.

For more information on device setup options, see "Managed device help" on page 673 and the *Installation and Deployment Guide*.

Using the advance agent

The advance agent reduces the amount of network bandwidth used for Windows-based agent configuration. The advance agent works well most devices, including laptops with intermittent or slow network connections. The advance agent doesn't support PDAs and other handheld devices.

The advance agent is a small 500 KB .MSI package. When this package runs on a managed device, it downloads an associated full agent configuration package, which may be up to 15 MB in size, depending on the agents you select. In the **Advance agent configuration** dialog, you can configure what bandwidth-friendly distribution options the .MSI will use for the full agent configuration download.

The advance agent works independently from the core server once it starts downloading the full agent configuration. If a device disconnects from the network before the agent configuration finishes downloading, the advance agent will automatically resume the download once the device is back on the network.

When you create an advance agent configuration, it takes a few seconds for the console to create the full agent configuration package. The console places the advance agent package (<configuration name>.msi) and the newly-created full agent configuration package (<configuration name>.exe) in the core server's LDLogon\AdvanceAgent folder. The file names are based on the agent configuration name.

Once you've created an agent configuration package, you need to run the .MSI portion on devices by using one of the following methods:

- Schedule the small .MSI portion for push distribution.
- Run the .MSI manually on each device.
- Manually configure the .MSI to run via a login script.

Once you deploy the advance agent to devices, the advance agent starts downloading the associated agent configuration. The agent runs silently on the managed device, without showing any dialogs or status updates. The advance agent uses the bandwidth preferences you specified in the **Advance agent configuration** dialog, such as Peer Download and dynamic bandwidth throttling.

Once the .MSI installs and successfully configures agents on a device, it removes the full agent configuration package. The .MSI portion stays on the device and if the same .MSI runs again it won't reinstall the agents.

To create an advance agent configuration

1. Create a Windows-based agent configuration (**Tools | Configuration | Agent configuration**).
2. From that configuration's shortcut menu, click **Advance agent**.
3. Select the options you want.

4. If you select **Peer download**, you must make sure that the advance agent .msi file and the full agent configuration .EXE package are in the software distribution cache of a device in the broadcast domain. If you select **Peer download** and don't do this before deploying the advance agent configuration, the deployment will fail because no cache or peer in the broadcast domain has the necessary files.
5. If you'll be relocating the associated agent configuration package (the .EXE file), change the path for the agent configuration package to match the new location.
6. Click **OK**.
7. If necessary, copy the associated .EXE file from the LDLogon\AdvanceAgent folder to your distribution server. Make sure the path to the agent configuration executable matches the path you specified in the **Advance agent configuration** dialog. You should leave the MSI package on the core server in the default location. Otherwise, the package won't be visible for the advance agent push distribution task below.

To set up an advance agent push distribution

1. In the Agent configuration window (**Tools | Configuration | Agent configuration**), click the **Schedule a push of an advance agent configuration** button.
2. The **Advance agent configurations** dialog lists the agent configurations in the LDLogon\AdvanceAgent folder. Click the configuration you want to distribute and click **OK**.
3. The **Scheduled tasks** window opens with the advance agent task you created selected. The task name is "Advance agent <your configuration name>".
4. Add target devices to the task by dragging them from the **Network view** and dropping them on the task in the **Scheduled tasks** window.
5. From the task's shortcut menu, click **Properties** and schedule the task. You can see the .MSI portion distribution progress in the **Scheduled tasks** window. There are no status updates on the full agent configuration once the .MSI distribution completes.

Updating agent preferences on devices

If you want to update agent preferences on devices, such as requiring permission for remote control, you don't have to redeploy the entire agent configuration. You can make the changes you want in the **Agent configuration** window, and from that configuration's shortcut menu click **Schedule update**. This opens the **Scheduled tasks** window and creates an update task and package for the configuration you scheduled the update from. This package is only a few hundred kilobytes in size.

Note that updating preferences won't install or remove agents on a device. If the update contains preferences for agents that aren't on a device, the preferences that don't apply will be ignored.

To update agent preferences on devices

1. Click **Tools | Configuration | Agent configuration**.
2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Schedule update**. This opens the **Scheduled tasks** window.
4. Target the devices you want to update and schedule the task.

Creating standalone agent configuration packages

Normally the client configuration utility, WSCFG32.EXE, configures clients. If you want, you can have the **Agent configuration** window create a self-extracting single-file executable that installs an agent configuration on the device it's run on. This is helpful if you want to install agents from a CD or portable USB drive, or if you want to multicast an agent configuration.

To create a standalone agent configuration package

1. Click **Tools | Configuration | Agent configuration**.
2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Create self-contained client installation package**.
4. Select the path where you want the package stored.
5. Wait for Management Suite to create the package. It may take a few minutes.

Agent security and trusted certificates

With Management Suite 8, the certificate-based authentication model has been simplified. Device agents still authenticate to authorized core servers, preventing unauthorized cores from accessing clients. However, Management Suite 8 doesn't require a separate certificate authority to manage certificates for the core, console, and each client. Instead, each core server has a unique certificate and private key that Management Suite Setup creates when you first install the core or rollup core server.

These are the private key and certificate files:

- **<keyname>.key**: The .KEY file is the private key for the core server, and it only resides on the core server. If this key is compromised, the core server and device communications won't be secure. Keep this key secure. For example, don't use e-mail to move it around.
- **<keyname>.crt**: The .CRT file contains the public key for the core server. The .CRT file is a viewer-friendly version of the public key that you can view to see more information about the key.
- **<hash>.0**: The .0 file is a trusted certificate file and has content identical to the .CRT file. However, it's named in a manner that lets the computer quickly find the certificate file in a directory that contains many different certificates. The name is a hash (checksum) of the certificates subject information. To determine the hash filename for a particular certificate, view the <keyname>.CRT file. There is a .INI file section [LDMS] in the file. The hash=value pair indicates the <hash> value.

An alternate method for getting the hash is to use the openssl application, which is stored in the \Program Files\LANDesk\Shared Files\Keys directory. It will display the hash associated with a certificate using the following command line:

```
openssl.exe x509 -in <keyname>.crt -hash -noout
```

All keys are stored on the core server in \Program Files\LANDesk\Shared Files\Keys. The <hash>.0 public key is also in the LDLOGON directory and needs to be there by default. <keyname> is the certificate name you provided during Management Suite Setup. During Setup, it's helpful to provide a descriptive key name, such as the core server's name (or even its fully qualified name) as the key name (example: ldcare or ldcare.org.com). This will make it easier to identify the certificate/private key files in a multi-core environment.

You should back up the contents of your core server's Keys directory in a safe, secure place. If for some reason you need to reinstall or replace your core server, you won't be able to manage that core server's devices until you add the original core's certificates to the new core, as described below.

Sharing keys among core servers

Devices will only communicate with core and rollup core servers for which they have a matching trusted certificate file. For example, let's say you have three core servers, managing 5,000 devices each. You also have a rollup core managing all 15,000 devices. Each core server will have its own certificate and private keys, and by default, the device agents you deploy from each core server will only talk to the core server from which the device software is deployed.

There are two main ways of sharing keys among core and rollup core servers:

1. Distributing each core server trusted certificate (the <hash>.0 file) to devices and their respective core servers. This is the most secure way.
2. Copying the private key and certificates to each core server. This doesn't require you to do anything to devices, but since you have to copy the private key, it exposes more risk.

In our example, if you want the rollup core and Web console to be able to manage devices from all three cores, you need to distribute the rollup core's trusted certificate (the <hash>.0) file to all devices, in addition to copying the same file to each core server's LDLOGON directory. For more information, see "Distributing trusted certificates to devices" on page 91. Alternatively, you can copy the certificate/private key files from each of the three core servers to the rollup core. This way, each device can find the matching private key for its core server on the rollup core server. For more information, see "Copying certificate/private key files among core servers" on page 92.

If you want one core to be able to manage devices from another core, you can follow the same process, either distributing the trusted certificate to devices or copying the certificate/public key files among cores.

If you are copying certificates between standalone cores (not to a rollup core), there is an additional issue. A core won't be able to manage another core's devices unless it first has an inventory scan from those devices. One way of getting inventory scans to another core is to schedule an inventory scan job with a custom command line that forwards the scan to the new core. In a multiple core scenario, using a rollup core and the Web console is a simpler way to manage devices across cores. Rollup cores automatically get inventory scan data from all devices on the cores that get rolled up to it.

Distributing trusted certificates to devices

There are two ways you can deploy trusted certificates to devices:

1. Deploy a device setup configuration that includes the core server trusted certificates you want.
2. Use a software distribution job to directly copy the trusted certificate files you want to each device.

Each additional core server trusted certificate (<hash>.0) that you want devices to use must be copied to the core server's LDLOGON directory. Once the trusted certificate is in this directory, you can select it within the device setup dialog's **Common base agent** page. Device setup copies keys to this directory on devices:

- Windows devices: \Program Files\LANDesk\Shared Files\cbaroot\certs
- Mac OS X devices: /usr/LANDesk/common/cbaroot/certs

If you want to add a core server's certificate to a device, and you don't want to redeploy device agents through device setup, create a software distribution job that copies < hash>.0 to the directory specified above on the device. You can then use the **Scheduled tasks** window to deploy the certificate distribution script you created.

The following is an example of a custom script that can be used to copy a trusted certificate from the LDLOGON directory of the core server to a device. To use this, replace d960e680 with the hash value for the trusted certificate you want to deploy.

```
; Copy a trusted certificate from the ldlogon directory of the core server
; into the trusted certificate directory of the client
[MACHINES]
REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Copying certificate/private key files among core servers

An alternative to deploying certificates (<hash>.0) to devices is to copy certificate/private key sets among cores. Cores can contain multiple certificate/private key files. As long as a device can authenticate with one of the keys on a core, it can communicate with that core.

When using certificate-based remote control, target devices must be in the core database

If you're using certificate-based remote control security with devices, you can only remote control devices that have an inventory record in the core database that you're connected to. Before contacting a node to launch remote control, the core looks in the database to ensure the requesting party has the right to view the device. If the device isn't in the database, the core denied the request.

To copy a certificate/private key set from once core server to another

1. At the source core server, go to the \Program Files\LANDesk\Shared Files\Keys folder.
2. Copy the source server's <keyname>.key, <keyname>.crt, and <hash>.0 files to a floppy disk or other secure place.
3. At the destination core server, copy the files from the source core server to the same folder (\Program Files\LANDesk\Shared Files\Keys). The keys take effect immediately.

Care should be taken to make sure that the private key <keyname>.key is not compromised. The core server uses this file to authenticate devices, and any computer with the <keyname>.key file can perform remote executions and file transfer to a Management Suite device.

Uninstalling device agents

Prior to Management Suite 8.5, anyone could uninstall Management Suite agents by running WSCFG32 with the /u parameter. Since WSCFG32 was in the LDLogon share, which managed devices could access, it was relatively easy for users to uninstall Management Suite agents.

With Management Suite 8.5 and later, the /u parameter has been removed from WSCFG32. There's a new utility called UninstallWinClient.exe in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Server Manager agents on any device it runs on. You can move it to any folder you want or add it to a login script. It's a Windows application that runs silently without displaying an interface.

Running this program won't remove a device from the core database. If you redeploy agents to a device that ran this program, it will be stored in the database as a new device.

Using LANDesk Server Manager and LANDesk System Manager with LANDesk Management Suite

Server Manager and System Manager are available separately from LANDesk Software and integrate with Management Suite. Management Suite includes one server license and as many device licenses as you purchased. If you install Management Suite agents on a server operating system, Management Suite requires an additional server license for each server. Server Manager adds Management Suite server licenses, in addition to Server Manager-specific features for managed servers.

System Manager helps you manage devices on your network and troubleshoot common computer problems before they become serious. If you have devices on your network that you're already managing with System Manager, you can use Management Suite's System Manager integration to manage these computers from the Management Suite console.

You can use LANDesk Management Suite to manage supported Linux/UNIX distributions.

Read this chapter to learn about:

- "Supported Linux/UNIX distributions" on page 94
- "Installing Linux agents" on page 95
- "Installing UNIX agents" on page 98
- "Using the inventory scanner with Linux/UNIX" on page 101

Supported Linux/UNIX distributions

SUSE Linux, Red Hat Linux 7.3, 8, 9, and Red Hat Enterprise Linux support these Management Suite features:

- Agent deployment
- Standard LANDesk agent
- Inventory scanning for hardware and software
- Software distribution, including policy support
- Vulnerability scanning and remediation

Sun Solaris (Intel architecture) supports these Management Suite features:

- Inventory scanning for hardware and software

Sun Solaris (SPARC architecture) supports these Management Suite features:

- Inventory scanning for hardware and software
- Vulnerability scanner (manual launch)

Supported Linux and UNIX distributions:

- Red Hat Linux 7.3, 8.0, 9
- Red Hat Enterprise Linux v3 (ES) 32-bit - U8
- Red Hat Enterprise Linux v3 (ES) EM64t - U8
- Red Hat Enterprise Linux v3 (WS) 32-bit - U8
- Red Hat Enterprise Linux v3 WS EM64t - U8
- Red Hat Enterprise Linux v3 (AS) 32-bit - U8
- Red Hat Enterprise Linux v3 (AS) EM64t - U8
- Red Hat Enterprise Linux v4 (ES) 32-bit - U5
- Red Hat Enterprise Linux v4 (ES) EM64t - U5
- Red Hat Enterprise Linux v4 (AS) 32-bit - U5
- Red Hat Enterprise Linux v4 (AS) EM64t - U5
- Red Hat Enterprise Linux v4 (WS) 32-bit - U5
- Red Hat Enterprise Linux v4 (WS) EM64t - U5
- Red Hat Enterprise Linux v5
- SUSE Linux Enterprise Server 9
- SUSE* Linux Server 9 ES 32-bit SP3
- SUSE Linux Server 9 EM64t SP3
- SUSE Linux Server 10 ES 32-bit
- SUSE Linux Server 10 EM64t
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- Mandriva Linux 10.1
- IBM AIX* 5.1, 5.2, or 5.3
- Intel Architecture Solaris 8 (only supports inventory)
- Sun Sparc Solaris 8
- Sun Sparc Solaris 9
- UNIX Hewlett Packard (HP-UX 11.1)

- UNIX Sun Sparc (Solaris 8)

Linux runs on a variety of architectures, but the Linux inventory scanner will only run on Intel architecture.

Installing Linux agents

You can remotely deploy and install Linux agents and RPMs on Linux servers. Your Linux server must be configured correctly for this to work. To install an agent on a Linux server, you must have root privileges.

The default Red Hat Enterprise Linux AS and ES install includes the RPMs that the Linux standard agent requires. For the complete list of RPMs that the product requires, see the list later in this chapter.

For an initial Linux agent configuration, the core server uses an SSH connection to target Linux servers. You must have a working SSH connection with username/password authentication. This product doesn't support public key/private key authentication. Any firewalls between the core and Linux servers need to allow the SSH port. Consider testing your SSH connection from the core server with a 3rd-party SSH application.

The Linux agent installation package consists of a shell script, agent tarballs, .INI agent configuration, and agent authentication certificates. These files are stored in the core server's LDLogon share. The shell script extracts files from the tarballs, installs the RPMs, and configures the server to load the agents and run the inventory scanner periodically at the interval you specified in the agent configuration. Files are placed under /usr/LANDesk.

Use the Configure Services (**Tools | Configure Services**) dialog to enter the SSH credentials you want the scheduler service to use as alternate credentials. The scheduler service uses these credentials to install the agents on your servers. You should be prompted to restart the scheduler service. If you aren't, click **Stop** and then **Start** on the **Scheduler** tab to restart the service. This activates your changes.

Deploying the Linux agents

After you've configured your Linux servers and added Linux credentials to the core server, you must create a Linux agent configuration, and then use unmanaged device discovery to discover your Linux servers. You can then add the discovered servers to the **My devices** list so you can deploy the Linux agents. Before you can deploy to a server, you must add it to the **My devices** list. Do this by discovering your Linux server with unmanaged device discovery.

To create a Linux agent configuration

1. In **Tools | Configuration | Agent configuration**, click the **New Linux** button.
2. Enter a **Configuration name**.
3. On the **Start** page, the Standard LANDesk agent, remote control, and software distribution agents are installed by default. If you want to install the **LANDesk vulnerability scanner**, check that box.

4. On the **Standard LANDesk agent** page, select the **Trusted certificates for agent authentication** that you want installed. For more information, see "Agent security and trusted certificates" on page 90.
5. Click **Save**.

To discover your Linux servers and deploy a configuration to them

1. In **Tools | Configuration | Unmanaged Device discovery**, create a discovery job for each Linux server. Use a standard network scan and enter the Linux server's IP address for the starting and ending IP ranges. If you have many Linux servers, enter a range of IP addresses. Click **Scan now** once you've added your discovery IP ranges.
2. When the task finishes, verify that unmanaged device discovery found the Linux servers you want to manage.
3. In the **Unmanaged device discovery** window, drag the Linux servers onto the Linux configuration that you want in the **Agent configuration** window.
4. Finish scheduling the task in the **Scheduled tasks** window.

To manually pull a Linux agent configuration

1. Create a new Linux configuration using the console or you can use the Default Linux configuration.
2. Create a directory on your Linux device (for example, /mnt/core) .
3. Mount to LDLOGON. You can use the following command to do this:

```
mount -t smbfs -o username=administrator,workgroup=<yourworkgroup>  
//<corename>/ldlogon /mnt/core
```

4. Change the directory to /mnt/core.
5. Enter `./linuxpull.sh <configuration name.ini>` (where this is the name of the configuration you created).

To uninstall a Linux agent configuration

1. On the Linux device you want to uninstall the agent from, mount <corename>\LDMAIN.
2. From the LDMAIN share, copy linuxuninstall.tar.gz to the Linux device.
3. Extract linuxuninstall.tar.gz.
4. In the extracted folder, run the following command: `./linuxuninstall.sh -f ALL`

Required RPMs for Red Hat and SUSE (version # or later)

It is recommended that you store all RPMs in the `...ManagementSuite\ldlogon\RPMS` directory. You can browse to this folder through `http://core name/RPMS`.

Red Hat Enterprise

python

RPM Version:2.2.3-5 (RH3), 2.3.4-14 (RH4)
Binary Version:2.2.3

pygtk2

RPM Version:1.99.16-8 (RH3), 2.4.0-1 (RH4)
Binary Version:

sudo

RPM Version:1.6.7p5-1, Binary Version:1.6.7.p5

bash

RPM Version:2.05b-29 (RH3), 3.0-19.2 (RH4)
Binary Version:2.05b.0(1)-release

xinetd

RPM Version:2.3.12-2.3E, (RH3) 2.3.13-4 (RH4)
Binary Version:2.3.12

mozilla

RPM Version: 1.7.3-18.EL4 (RH4)
Binary Version:1.5

openssl

RPM Version:0.9.7a-22.1 (RH3), 0.9.7a-43.1 (RH4)
Binary Version:0.9.7a

sysstat

RPM Version:4.0.7-4, Binary Version:4.0.7

lm_sensors

RPM Version: 2.6 (this version may not be sufficient to display sensors on newer ASIC machines. Please see the lm_sensors documentation or the web site (<http://www2.lm-sensors.nu/~lm78>) for more detailed information.

SUSE Linux (SUSE 64)

bash

RPM Version: 2.05b-305.6

mozilla

RPM Version: 1.6-74.14

net-snmp

RPM Version: 5.1-80.9

openssl

RPM Version: 0.9.7d-15.13

python-gtk

RPM Version: 2.0.0-215.1 [note: package name change]

python

RPM Version: 2.3.3-88.1

sudo

RPM Version: 1.6.7p5-117.1

sysstat

RPM Version: 5.0.1-35.1

xinetd

RPM Version: 2.3.13-39.3

lm_sensors

RPM Version: NA (note: this has been incorporated into the kernel for the 2.6 version)

Installing UNIX agents

You have to manually install the UNIX agents. Follow the steps below for your UNIX distribution.

To install the agents on AIX

1. From LDLogon\unix\common, copy ldiscnux.conf and ldappl.conf to /etc. Copy ldiscnux.8 to /usr/man/man8. Give ldiscnux.conf read/write access for users. Give ldappl.conf read access for users. Use the UNIX chmod command to assign rights to the files.
2. Edit ldappl.conf to customize the software scanning if desired. See the sample entries in ldappl.conf for more information.
3. From the LDLogon\unix\aix, navigate to the folder that matches your AIX version. Copy ldiscnux and vulscan to a directory that is accessible by the individuals who will be running the application. Usually this is /usr/sbin.
4. If needed, make ldiscnux and vulscan executable using the chmod command.

To install the agents on HPUX

1. From LDLogon\unix\hpux, extract baseclient.tar.gz and vulscan.tar.gz.
2. Follow the directions in the README file that is in each archive to finish the installation.

To install the agents on Solaris (Intel architecture)

1. From LDLogon\unix\common, copy ldiscnux.conf and ldappl.conf to /etc. Copy ldiscnux.8 to /usr/man/man8. Give ldiscnux.conf read/write access for users. Give ldappl.conf read access for users. Use the UNIX chmod command to assign rights to the files.
2. Edit ldappl.conf to customize the software scanning if desired. See the sample entries in ldappl.conf for more information.
3. From LDLogon\unix\common\solia, copy ldiscnux to a directory that is accessible by the individuals who will be running the application. Usually this is /usr/sbin.
4. If needed, make ldiscnux executable using the chmod command.

To install the agents on Solaris 8 and 9 (SPARC architecture)

- From LDLogon\solsparc, follow the directions in installation.txt.

Required AIX libraries

Inventory scanner libraries:

- libstdc++-3.3.2-5
- libgcc-3.3.2-5
- The latest version of the rpm libraries that matches your operating system version

Vulnerability scanner libraries:

- The inventory scanner libraries above.
- The latest version of the expat libraries that matches your operating system version

These files are available from <ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPM/ppc>. For the libstdc++ and libgcc libraries mentioned above, they must be those exact versions because they are the versions that the shipping binaries are linked against.

Required HPUX libraries

Inventory scanner libraries:

- libdl.2
- libc.2
- libcl.2
- libsamstub.1
- libm.2
- libCsup.2
- libstream.2
- libstd.2

- libnsl.1
- libxti.2

Inventory scanner filesets:

- OS-Core.CORE-SHLIBS
- PHSS_32573.CORE-SHLIBS (Patch to OS-Core.CORE-SHLIBS)
- NFS.NFS-SHLIBS
- Streams.STREAMS-MIN

Vulnerability scanner libraries:

- libdld.2
- libc.2
- libcl.2
- libisamstub.1
- libm.2
- libCsup_v2.2
- libstd_v2.2
- libexpat.sl

Vulnerability scanner filesets:

- OS-Core.CORE-SHLIBS
- PHSS_32573.CORE-SHLIBS (Patch to OS-Core.CORE-SHLIBS)
- expat.expat-RUN

Required Solaris libraries

Solaris 8 libraries:

- libstdc++.so.5.0.4 (<ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/libgcc-3.3-sol8-sparc-local.gz>)
- libexpat.so (<ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/expat-1.95.5-sol8-sparc-local.gz>)

Solaris 9 libraries:

- libstdc++.so.5.0.5 (<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/libgcc-3.3-sol9-sparc-local.gz>)
- libexpat.so (<ftp://ftp.sunfreeware.com/pub/freeware/sparc/9/expat-1.95.5-sol9-sparc-local.gz>)

Using the inventory scanner with Linux/UNIX

Inventory scanner command-line parameters

The inventory scanner, `ldiscnux`, has several command-line parameters that specify how it should run. See "`ldiscnux -h`" or "`man ldiscnux`" for a detailed description of each. Each option can be preceded by either `'-'` or `'/'`.

Parameter	Description
<code>-d=Dir</code>	Starts the software scan in the <code>Dir</code> directory instead of the root. By default, the scan starts in the root directory.
<code>-f</code>	Forces a software scan. If you don't specify <code>-f</code> , the scanner does software scans on the day interval (every day by default) specified in the console under Configure Services Inventory Scanner Settings .
<code>-f-</code>	Disables the software scan.
<code>-i=ConfName</code>	Specifies the configuration filename. Default is <code>/etc/ldappl.conf</code> .
<code>-ntt=address:port</code>	Host name or IP address of core server. Port is optional.
<code>-o=File</code>	Writes inventory information to the specified output file.
<code>-s=Server</code>	Specifies the core server. This command is optional, and only exists for backward compatibility.
<code>-stdout</code>	Writes inventory information to the standard output.

Parameter	Description
-v	Enables verbose status messages during the scan.
-h or -?	Displays the help screen.

Examples

To output data to a text file, type:

```
ldiscnux -o=data.out -v
```

To send data to the core server, type:

```
ldiscnux -ntt=ServerIPName -v
```

UNIX inventory scanner files

File	Description
ldiscnux	<p>The executable that is run with command-line parameters to indicate the action to take. All users that will run the scanner need sufficient rights to execute the file.</p> <p>There is a different version of this file for each platform supported above.</p>
/etc/ldiscnux.conf	<p>This file always resides in /etc and contains the following information:</p> <ul style="list-style-type: none">• Inventory assigned unique ID• Last hardware scan• Last software scan <p>All users who run the scanner need read and write attributes for this file. The unique ID in /etc/ldiscnux.conf is a unique number assigned to a computer the first time the inventory scanner runs. This number is used to identify the computer. If it ever changes, the core server will treat it as a different computer, which could result in a duplicate entry in the database.</p> <p>Warning: Do not change the unique ID number or remove the ldiscnux.conf file after it has been created.</p>

File	Description
/etc/ldappl.conf	This file is where you customize the list of executables that the inventory scanner will report when running a software scan. The file includes some examples, and you'll need to add entries for software packages that you use. The search criteria are based on filename and file size. Though this file will typically reside in /etc, the scanner can use an alternative file by using the <code>-i=</code> command-line parameter.
ldiscnux.8	Man page for ldiscnux.

Console integration

Once a Linux/UNIX computer is scanned into the core database, you can:

- Query on any of the attributes returned by the Linux inventory scanner to the core database.
- Use the reporting features to generate reports that include information that the Linux scanner gathers. For example, Linux will appear as an OS type in the Operating Systems Summary Report.
- View inventory information for Linux computers.
- Distribute software on distributions that support this.

Queries on "System Uptime" sort alphabetically, returning unexpected results

If you want to do a query to find out how many computers have been running longer than a certain number of days (for example, 10 days), query on "System Start" rather than "System Uptime." Queries on System Uptime may return unexpected results, because the system uptime is simply a string formatted as "x days, y hours, z minutes, and j seconds." Sorting is done alphabetically and not on time intervals.

Path to config files referenced in ldappl.conf doesn't appear in the console

ConfFile entries in ldappl.conf file need to include a path.

Database queries

Queries are customized searches for managed devices. LANDesk Management Suite provides a method for you to query devices that have been scanned into your core database via database queries, as well as a method for you to query for devices located in other directories via LDAP queries. You view, create and organize database queries with the Queries groups in the console's network view. You create LDAP queries with the Directory Manager tool.

For more information on creating and using LDAP directory queries with Directory Manager, see "LDAP queries" on page 108.

Read this chapter to learn about:

- "Queries overview" on page 104
- "Query groups" on page 104
- "Creating database queries" on page 105
- "Running database queries" on page 107
- "Importing and exporting queries" on page 107

Queries overview

Queries help you manage your network by allowing you to search for and organize network devices that are in the core database, based on specific system or user criteria.

For example, you can create and run a query that captures only devices with a processor clock speed of less than 166 MHz, or with less than 64 MB of RAM, or a hard drive of less than 2 GB. Create one or more query statements that represent those conditions and relate statements to each other using standard logical operators. When the queries are run, you can print the results of the query, and access and manage the matching devices.

Query groups

Queries can be organized into groups in the network view. Create new queries (and new query groups) by right-clicking either the **My queries** group and selecting **New query** or **New group**, respectively.

A Management Suite administrator (user with LANDesk Administrator rights) can view the contents of all of the query groups, including: **My queries**, **Public queries**, **All queries**, and **User queries**.

When other Management Suite users log in to the console, they can see queries in the **My queries**, **Public queries**, and **All queries** groups, based on their device scope. A user will not see the **User queries** group.

When you move a query to a group (by right-clicking and selecting **Add to new group** or **Add to existing group**), or by dragging and dropping the query, you're actually creating a copy of the query. You can remove the copy in any query group and the master copy of the query (in the **All queries** group) isn't affected. If you want to delete the master copy, you can do it from the **All Queries** group.

For more information on how query groups and queries display in the network view, and what you can do with them, see "Understanding the network view" on page 23.

Creating database queries

Use the **New query** dialog to build a query by selecting from attributes, relational operators, and the attribute's values. Build a query statement by choosing an inventory attribute and relating it to an acceptable value. Logically relate the query statements to each other to ensure they're evaluated as a group before relating them to other statements or groups.

To create a database query

1. In the console's network view, right-click the **My queries** group (or **Public queries**), if you have the public query management right, and then click **New query**.
2. Enter a unique name for the query.
3. Select a **component** from the inventory attributes list.
4. **Select a relational operator.**
5. Select a **value** from the values list. You can edit a value.
6. Click **Insert** to add the statement to the query list.
7. If you want to query for more than one component, click a **logical operator (AND, OR)** and repeat steps 2-5.
8. (Optional) To group query statements so they're evaluated as a group, select two or more **query statements** and click **Group()**.
9. When you're finished adding statements, click **Save**.

About the New query dialog

Use this dialog to create a new query with the following functions:

- **Name:** Identifies the query in query groups.
- **Machine components:** Lists inventory components and attributes the query can scan for.
- **Relational operators:** Lists relational operators. These operators determine which description values for a certain component will satisfy the query.

The Like operator is a new relational operator. If a user doesn't specify any wild cards (*) in their query, the Like operator adds wildcards to both ends of the string. Here are three examples of using the Like operator:

Computer.Display Name LIKE "Bob's Machine" queries for: Computer.Display Name LIKE "%Bob's Machine%"

Computer.Display Name LIKE "Bob's Machine*" queries for: Computer.Display Name LIKE "Bob's Machine%"

Computer.Display Name LIKE "*"Bob's Machine" queries for: Computer.Display Name LIKE "%Bob's Machine"

- **Display scanned values:** Lists acceptable values for the chosen inventory attribute. You can also manually enter an appropriate value, or edit a selected value, with the Edit values field. If the selected relational operator is Exists or Does Not Exist, no description values are possible.
- **Logical operator:** Determines how query statements logically relate to each other:
 - **AND:** Both the previous query statement AND the statement to be inserted must be true to satisfy the query.
 - **OR:** Either the previous query statement OR the statement to be inserted must be true to satisfy the query.
- **Insert:** Inserts the new statement into the query list and logically relates it to the other statements according to the listed logical operator. You can't choose this button until you've built an acceptable query statement.
- **Edit:** Lets you edit the selected query statement. When you're finished making changes, click the **Update** button.
- **Delete:** Deletes the selected statement from the query list.
- **Clear all:** Deletes all statements from the query list.
- **Query list:** Lists each statement inserted into the query and its logical relationship to the other listed statements. Grouped statements are surrounded by parentheses.
- **Group ():** Groups the selected statements together so they're evaluated against each other before being evaluated against other statements.
- **Ungroup:** Ungroups the selected grouped statements.
- **Filters:** Opens the Query Filter dialog that displays device groups. By selecting device groups, you limit the query to only those devices contained in the selected groups. If you don't select any groups, the query ignores group membership.
- **Select columns:** Lets you add and remove columns that appear in the query results list for this query. Select a component, and then click the right-arrow button to add it to the column list. You can manually edit the Alias and Sort Order text, and your changes will appear in the query results list.
- **Qualifier:** The qualifier button is used to limit the results of one-to-many relationships in the database; without it, you will get the same machine listed numerous times in your result set. For example, if you want to see which version of Microsoft Word is installed on every machine in your organization, you would insert `Computer.Software.Package.Name = 'Microsoft Word'` in the query box and select `Computer.Software.Package.Version` in the Select Columns list. However, simply listing the software version will list every version of every piece of software installed on each machine; precisely what you don't want. To solution is to limit (or qualify) the version to only Microsoft Word. Click on the Qualify button and you will be able to insert `Computer.Software.Package.Name = "Microsoft Word"`. This will return only the versions of Microsoft Word.
- **Save:** Saves the current query. When you save a query before running it, the query is stored in the core database and remains there until you explicitly delete it.

Query statements are executed in the order shown

If no groupings are made, the query statements listed in this dialog are executed in order from the bottom up. Be sure to group related query items so they're evaluated as a group; otherwise, the results of your query may be different than you expect.

Running database queries

To run a query

1. In the network view, expand the query groups to locate the query you want to run.
2. Double-click the query. Or, right-click and select **Run**.
3. The results (matching devices) display in the right-hand pane of the network view.

Importing and exporting queries

You can use import and export to transfer queries from one core database to another. You can import:

- Management Suite 8 exported queries
- Web console exported .XML queries
- Management Suite 6.52, 6.62, and 7.0 exported .QRY queries

To import a query

1. Right-click the query group where you want to place the imported query.
2. Select **Import** from the shortcut menu.
3. Navigate to the query you want to import and select it.
4. Click **Open** to add the query to the selected query group in the network view.

To export a query

1. Right-click the query you want to export.
2. Select **Export** from the shortcut menu.
3. Navigate to the location where you want to save the query (as an .XML file).
4. Type a name for the query.
5. Click **Save** to export the query.

LDAP queries

In addition to the ability to query the core database with database queries, Management Suite also provides the Directory Manager tool that lets you locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).

You can query devices based on specific attributes such as processor type or OS. You can also query based on specific user attributes such as employee ID or department.

For information about creating and running database queries from the Queries groups in the network view, see "Database queries" on page 104.

Read this chapter to learn about:

- "Configure LDAP Directories" on page 108
- "About the Directory manager window" on page 109
- "Creating LDAP directory queries" on page 110
- "More about the Lightweight Directory Access Protocol (LDAP) " on page 112

Configure LDAP Directories

Use the Directory Manager configuration tool to manage the LDAP directories you use with LANDesk Management Suite. The LDAP server, username and password you enter are saved and used when you browse or execute queries to the directory. If you change the password of the configured user in the LDAP directory, you must also change the password in here.

NOTE: The account you configure here must be able to read the users, computers and groups that you use for management with LDMS.

To access the Directory Manager configuration tool

To access the Directory Manager configuration tool, select **Configure | Manage Directories**.

To configure a new directory

1. Right-click anywhere in the **Manage Directories** list view and select **Manage New Directory**
2. Enter the DNS name of the directory server in the LDAP:// field
3. Enter the user name and password

NOTE: If you are using Active Directory, enter the name as <domain-name>\<nt-user-name>

NOTE: If you are using another directory service, enter the distinguished name of the user

4. Click **Apply** or **OK** to save the information. The information you enter is verified against the directory before the dialog closes

To modify an existing directory configuration

1. Double-click the directory entry you want to modify or right-click and select **Properties...**
2. Change the server, username, password as desired
3. Click **Apply** or **OK** to save the information. The information is verified against the directory before the dialog closes

To delete and existing directory configuration

1. Right-click the directory entry you want to delete
2. Select **Remove Managed Directory**

NOTE: All LDAP queries using this directory will be deleted when the directory is removed.

About the Directory manager window

Use directory manager to accomplish the following tasks:

- **Manage directory:** Opens the **Directory properties** dialog where you identify and log in to an LDAP directory.
- **Remove directory:** Removes the selected directory from the preview pane and stops managing it.
- **Refresh view:** Reloads the list of managed directories and targeted users.
- **New query:** Opens the **LDAP query** dialog where you can create and save an LDAP query.
- **Delete query:** Deletes the selected query.
- **Run query:** Generates the results of the selected query.
- **Object properties:** See the properties for the selected object.

Using directory manager, you can drag LDAP groups and saved LDAP queries onto scheduled tasks, making them task targets.

The directory manager window consists of two panes: a directory pane on the left and a preview pane on the right.

Directory pane

The directory pane displays all registered directories and users. As an administrator, you can specify the name of a registered directory and see a list of queries that are associated with the directory. You can create and then save new queries for a registered directory with a right mouse click or by using drop-down menus. After creating a query, you can drag and drop it to the **Scheduled tasks** window so that the task is applied to users who match the query.

Preview pane

When you select a saved query in directory manager's directory pane on the left side of the dialog, the policies targeted to that query appear in the preview pane on the right side. Likewise, when an individual LDAP user is selected in the directory pane, the policies targeted to that user appear in the preview pane.

- **Registered directory:** Query groups item and Browse item.
- **Query groups:** Queries associated with the directory.
- **Query:** Provides details about the query.
- **Browse and directory items:** Sub-items in the directory.

Creating LDAP directory queries

To create and save a directory query

The task of creating a query for a directory and saving that query is divided into two procedures:

To select an object in the LDAP directory and initiate a new query

1. Click **Tools | Distribution | Directory Manager**.
2. Browse the **Directory Manager** directory pane, and select an object in the LDAP directory. You'll create an LDAP query that returns results from this point in the directory tree down.
3. From directory manager, click the **New query** toolbar button. Note that this icon only appears when you select the root organization (o) of the directory tree (o=my company) or an organizational unit (ou=engineering) within the root organization. Otherwise, it's dimmed.
4. The **Basic LDAP query** dialog appears.

To create, test, and save the query

1. From the **Basic LDAP query** dialog, click an attribute that will be a criterion for the query from the list of directory attributes (example = department).
2. Click a comparison operator for the query (=, <=, >=) .
3. Enter a value for the attribute (example department = engineering).
4. To create a complex query that combines multiple attributes, select a combination operator (AND or OR) and repeat steps 1 through 3 as many times as you want.
5. When you finish creating the query, click **Insert**.
6. To test the completed query, click **Test query**.
7. To save the query, click **Save**. The saved query will appear by name under **Saved queries** in the directory pane of directory manager.

About the Basic LDAP query dialog

- **LDAP query root:** Select a root object in the directory for this query (LDAP://ldap.xyzcompany.com/ou = America.o = xyzcompany). The query that you're creating will return results from this point in the tree down.
- **LDAP attributes:** Select attributes for user-type objects.
- **Operator:** Select the type of operation to perform relating to an LDAP object, its attributes, and attribute values including equal to (=), less than or equal to (<=), and greater than or equal to (>=).
- **Value:** Specify the value assigned to the attribute of an LDAP object.
- **AND/OR/NOT:** Boolean operators that you can select for your query conditions.
- **Test query:** Execute a test of the query you've created.
- **Save:** Save the created query by name.

- **Advanced:** Create a query using the elements of a basic LDAP query but in a freeform manner.
- **Insert:** Insert a line of query criteria.
- **Delete:** Delete a selected line of criteria.
- **Clear all:** Clear all lines of query criteria.

About the Save LDAP query dialog

From the **Basic LDAP query** dialog, click **Save** to open the **Save LDAP query** dialog, which displays the following:

- **Choose a name for this query:** Enables you to choose a name for the query you've created.
- **Query Details LDAP Root:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Query Details LDAP Query:** Displays query examples you can use as a guide when creating your own query in freeform.
- **Save:** Enables you to save the created query by name. The query is saved under the **Saved queries** item under the LDAP directory entry in the directory manager directory pane.

About the Directory properties dialog

From the directory manager toolbar, click the **Manage directory** toolbar button to open the **Directory properties** dialog. This dialog enables you to start managing a new directory, or to view properties of a currently managed directory. This dialog also shows the URL to the LDAP server and the authentication information required to connect to the LDAP directory:

- **Directory URL:** Enables you to specify the LDAP directory to be managed. An example of an LDAP directory and the correct syntax is `ldap.<companyname>.com`. For example, you might type `ldap.xyzcompany.com`.
- **Authentication:** Enables you to log in as the following user (that is, you specify a user path and name and the user password).

About the Advanced LDAP query dialog

From the **Basic LDAP query** dialog, click **Advanced** to open the **Advanced LDAP query** dialog, which displays the following:

- **LDAP query root:** Enables you to select a root object in the directory for this query. The query that you're creating will return results from this point in the tree down.
- **LDAP query:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Examples:** Displays query examples you can use as a guide when creating your own query in freeform.
- **Test query:** Enables you execute a test of the query you have created.

The **Advanced LDAP query** dialog appears when you select to edit a query that has already been created. Also, if you select an LDAP group in directory manager and then choose to create a query from that point, the **Advanced LDAP query** dialog appears with a default query that returns the users who are members of that group. You can't change the syntax of this default query, only save the query.

More about the Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for accessing and viewing information about users and devices. LDAP enables you to organize and store this information into a directory. An LDAP directory is dynamic in that it can be updated as necessary, and it is distributed, protecting it from a single point of failure. Common LDAP directories include Novell Directory Services* (NDS) and Microsoft Active Directory Services* (ADS).

The following examples show LDAP queries that can be used to search the directory:

- Get all entries: (objectClass=*)
- Get entries containing 'bob' somewhere in the common name: (cn=*bob*)
- Get entries with a common name greater than or equal to 'bob': (cn>='bob')
- Get all users with an e-mail attribute: (&(objectClass=user)(email=*))
- Get all user entries with an e-mail attribute and a surname equal to 'smith': (&(sn=smith)(objectClass=user)(email=*))
- Get all user entries with a common name that starts with 'andy', 'steve', or 'margaret': (&(objectClass=User)(| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Get all entries without an e-mail attribute: (!(email=*))

The formal definition of the search filter is as follows (from RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*
- <substring> ::= <attr> '= <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*'
- <starval> ::= NULL | <value> '*'
- <final> ::= NULL | <value>

The token <attr> is a string representing an AttributeType. The token <value> is a string representing an AttributeValue whose format is defined by the underlying directory service.

If a <value> must contain one of the characters * or (or), precede the character with the slash (\) escape character.

Managing inventory

LANDesk uses an inventory scanning utility to add devices to the core database and to collect device hardware and software data. You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

Read this chapter to learn about:

Inventory

- "Inventory scanning overview" on page 114
- "Viewing inventory data" on page 116
- "Tracking inventory changes" on page 117
- "Creating custom data forms" on page 119
- "Using an off-core inventory server" on page 121

Note: For more information about running the inventory scanner, and inventory scanner troubleshooting tips, see "Appendix A: Additional inventory operations and troubleshooting" on page 595

Inventory scanning overview

The inventory scanner collects hardware and software data and enters it into the core database. When you configure a device with the Agent configuration tool, the inventory scanner is one of the components of the standard LANDesk agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database. The scanner executable is named LDISCN32.EXE and supports Macintosh, Linux, and Windows 95/98/NT/2000/2003/XP devices.

There are two types of inventory scans:

- **Hardware scan:** Hardware scans inventory hardware on managed devices. Hardware scans run quickly. You can configure the hardware scan interval in an agent configuration (**Tools | Configuration | Agent Configuration**) that you can deploy to managed devices. By default, hardware scans run each time the device boots.
- **Software scan:** Software scans inventory software on managed devices. These scans take longer to run than hardware scans. Software scans can take a few minutes to complete, depending on the number of files on the managed device. By default, the software scan runs once a day, regardless of how often the inventory scanner runs on the device. You can configure the software scan interval in the **Configure | Services | Inventory** tab.

You can scan a device on demand by finding it in the network view, and from its shortcut menu, and clicking **Inventory scan**.

Note: A device added to the core database using the discovery feature has not yet scanned its inventory data into the core database. You must run an inventory scan on each device for full inventory data to appear for that device.

You can view inventory data and use it to:

- Customize the network view columns to display specific inventory attributes
- Query the core database for devices with specific inventory attributes
- Group devices together to expedite management tasks, such as software distribution
- Generate specialized reports based on inventory attributes

You can also use inventory scans to keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur. For more information, see "Tracking inventory changes" on page 117.

Read the sections below to learn more about how the inventory scanner works.

Delta scanning

After the initial full scan is run on a device, the inventory scanner only captures delta changes and sends them to the core database. By sending only changed data, network traffic and data processing times are minimized.

Forcing a full scan

If you want to force a full scan of the device's hardware and software data, you can delete the existing delta scan file and change a setting in the **Configure LANDesk Software Services** applet.

1. Delete the **invdelta.dat** file from the server. A copy of the latest inventory scan is stored locally as a hidden file named **invdelta.dat**. The **LDMS_LOCAL_DIR** environment variable sets the location for this file. By default it is in **C:\Program Files\LANDesk\LDClient\Data**.
2. Add the **/sync** option to the inventory scanner utility's command line. To edit the command line, click **Start | All Programs | LANDesk Management**, right-click the **Inventory Scan** shortcut icon, select **Properties | Shortcut**, then edit the **Target** path.
3. At the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**.
4. Click the **Inventory** tab, then click **Advanced settings**.
5. Click the **Do Delta** setting. In the **Value** box type **0**.
6. Click **OK** twice, then click **Yes** at the prompt to restart the service.

Scan compression

Inventory scans performed by the Windows inventory scanner (**LDISCAN32.EXE**) are compressed by default. The scanner compresses full scans and delta scans with approximately an 8:1 compression ratio. Scans are first built completely in memory, then compressed and sent to the core server using a larger packet size. Scan compression requires fewer packets and reduces bandwidth usage.

Scan encryption

Inventory scans are encrypted (TCP/IP scans only). You can disable inventory scan encryption by changing a setting in the LANDesk Configure Services applet.

1. At the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**.
2. Click the **Inventory** tab, then click **Advanced settings**.
3. Click the **Disable Encryption** setting. In the **Value** box type **1**.
4. Click **Set**, then click **OK**.
5. Click **OK**, then click **Yes** at the prompt to restart the service.

Encrypted data transport

In **Configure | Services | Inventory** tab, there is an **Encrypted data transport** option. This option causes device scans to be sent to the core using SSL. Since the files are sent through the Web service and not the inventory service front end, a NAT address won't be appended to the scan file, even if that option is enabled in the registry.

Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the console.

Device inventories are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use the inventory to help manage and configure devices, and to quickly identify system problems.

You can view inventory data in the following ways:

- "Viewing a summary inventory" on page 116
- "Viewing a full inventory" on page 117

You can also view inventory data in reports that you generate. For more information, see "Reports" on page 123.

Viewing a summary inventory

Summary inventory is found on the device's properties page and provides a quick look at the device's basic OS configuration and system information. The summary also shows the date and time of the last inventory scan so you know how current the data is.

Note: If you added a device to the core database using the discovery tool, its inventory data isn't yet scanned into the core database. You must run an inventory scan on the device for the summary inventory feature to complete successfully.

To view summary inventory

1. In the console's network view, right-click a device.
2. Click **Properties | Inventory** tab.

Inventory summary data is different for Windows NT/2000/2003/XP and Windows 95/98 devices.

Viewing a full inventory

A full inventory provides a complete listing of a device's detailed hardware and software components. The listing contains objects and object attributes.

To view a full inventory

1. In the console's network view, right-click a **device**.
2. Click **Inventory**.

For detailed information, see "Inventory help" on page 666.

Viewing attribute properties

You can view attribute properties for a device's inventory objects from the inventory listing. Attribute properties tell you the characteristics and values for an inventory object. You can also create new custom attributes and edit user-defined attributes.

To view an attribute's properties, double-click the attribute.

For more information, see "About the Inventory attribute properties dialog" on page 667.

Tracking inventory changes

LANDesk can detect and record changes about the device hardware and software. Tracking inventory changes can help you control your network assets. Inventory change settings let you select which types of changes you want to save and with what severity level. The selected changes can be saved in an inventory history log, the core server's Windows event log, or sent as an AMS alert.

You can view and print a device's history of inventory changes. Additionally, you can export the inventory changes to a .CSV formatted file for analysis using your own reporting tools.

To track and use inventory changes, you must first configure the inventory change settings. You will be able to perform the other inventory changes history tasks:

- "Configuring inventory change settings" on page 118
- "Viewing, printing, or exporting inventory changes" on page 118

Configuring inventory change settings

Note: You must first configure these settings if you want to view, print, or export inventory changes for any devices on your network.

To configure inventory change settings

1. Click **Configure | Inventory history**.
2. In the **Inventory change settings** dialog, expand the **Computer** object in the **Current inventory** list, and select the system component you want to track.
3. In the **Log event in** list, select the component's attribute you want to track.
4. Check the appropriate box to specify where to record a change in that attribute. Inventory changes can be recorded in the inventory changes history log, Windows NT event viewer log, or as an AMS alert.
5. Select a severity level from the **Log/Alert severity** drop-down list. Severity levels include: None, Information, Warning, and Critical.
6. Click **OK**.

For more information, see "About the Inventory change settings dialog" on page 667.

Viewing, printing, or exporting inventory changes

To view, print, or export inventory changes

1. In the console's network view, right-click a device (or devices).
2. Click **Inventory history**.
3. Click **Print** to print the inventory changes history.
4. Click **Export** to save the inventory changes history as a .CSV file.

For more information, see "About the Inventory changes history dialog" on page 668.

Using custom data forms

LANDesk includes a custom data forms tool (**Tools | Custom data forms**) that you can use to create and manage forms. Custom data forms provide a way for you to collect information from users and add it to the core database.

Custom data forms are not supported in LANDesk Security Suite

Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite license in order to use the custom data forms feature.

The inventory scanner can't gather certain types of personalized user-specific information, such as:

- Where is a user's desk?
- What is a user's asset number?
- What is the user's phone number?

The best way to get this information is directly from your users with custom data forms.

Custom data forms have two main components: the form designer which is used by you to create forms for users to fill out, and the form viewer which is used by users to fill out forms.

Forms can be stored centrally or locally. If they're stored centrally, all users automatically have access to the latest forms because everyone views the same form from the same place. If forms are stored locally, you must ensure that users receive the latest forms.

After a user completes a form, the form viewer stores the results locally in C:\Program Files\LANdesk\LDCClient\LDCSTM.DAT. This file contains the results from all of the forms the user has responded to. If the user ever needs to fill out the same form again (for example, if the original form was revised), the form viewer fills in the form with the previously entered data.

The inventory scanner takes the information from each device's LDCSTM.DAT file and adds it to the core database.

Oracle databases are case-sensitive

When creating custom fields with custom data forms (or using any other feature) on an Oracle database, make sure you consistently capitalize field names. For example, data associated with "Cube location" is stored in a different place in the database than data associated with "Cube Location."

Also, make sure custom fields have names that are unique regardless of capitalization. The correct inventory data may not be retrieved if two custom fields have the same name but different capitalization.

For more information about custom data forms, see the following procedures:

- "Creating custom data forms" on page 119
- "Creating a group of forms" on page 120
- "Configuring devices to receive custom data forms" on page 120
- "Filling out forms on the device" on page 121

Creating custom data forms

Follow these steps to create a custom data form.

To create a custom data form

1. Click **Tools | Configuration | Custom data forms**.
2. In the Custom Data Forms window, double-click **Add new form**.
3. Enter a name for the **form**.
4. Enter a description for the form.
5. Click **Add** to open the **Add question** dialog.
6. In the Add Question dialog, type in the **Question text**, **Inventory name**, and **Description**.
7. **Select the Control type**.
8. **Select** whether you want the field to be required.
9. If you selected the **Edit** control type, click **Finish** to close the **Add question** dialog. The Edit control type lets users type in their own answers to questions in an editable text box. You can add more questions or proceed to step 12.

10. If you selected either of the **Combo box** control types, click **Next** to open the **Add items** dialog. The Combo box control type lets users select their answers from a drop-down list of pre-defined items.
11. In the Add Items dialog, enter an item name and click **Insert** to place the item in the Items list. These items appear in a drop-down list for that question on the form. You can add as many items as you like, then click **Finish**.
12. When you're done adding questions, click **Close** to save the form.

You can right-click on a form to schedule it for distribution to devices.

Creating a group of forms

If you have more than one form that you want to send to devices, you can organize them into a group. Then you can simply schedule the group of forms for distribution. Of course, this is not a required procedure.

When you schedule a group of forms for distribution, the local scheduler reads the contents of the group when it's time to distribute it. In other words, you can still change the contents of the group even after it has been scheduled (as long as the scheduled job hasn't yet occurred).

Note: If a form that is part of a group is later modified or deleted, the group automatically reflects those changes.

To create a group of forms

1. In the **Custom data forms** window, click the **Multiple forms toolbar button**.
2. Enter a name for the new group.
3. Select the forms you want to add to the group from the list of available forms.
4. Click **OK**.

You can right-click on a group of forms to schedule it for distribution to devices.

Configuring devices to receive custom data forms

When you set up devices, you can configure them to receive custom data forms. You must select to install the custom data forms component, and specify custom data form options on the agent configuration dialog. For more information, see "Deploying custom data forms" on page 679.

In the agent configuration dialog, you need to specify how you want to update forms on the device:

- **Automatic update:** If all of the forms are stored centrally (automatic updates), users check a single location for new forms. That way, when a new form is available, all devices looking there have immediate access to it. The disadvantage is that users may see forms that aren't relevant to them.
- **Manual update:** If forms are stored locally (manual updates), you'll need to distribute the forms to the users that need to fill them out. There is less network overhead because each device has its own copy of the form. The benefit of local forms is that you can limit the forms users see to only those that are relevant to them. You copy forms to devices during device setup or with the Scheduled Tasks tool.

You also need to specify when forms will be shown on the device:

- **On startup:** The device's form viewer checks for any new or modified forms each time the device boots. The form viewer launches after the operating system loads. The next time the inventory scanner runs, it sends completed forms to the core database.
- **When the inventory scanner runs:** The inventory scanner starts the form viewer, which checks for any new or modified forms. As soon as users finish filling out the form and close the form viewer, the scan finishes and the data is entered in the core database.
- **Only in LANDesk program folder:** The form viewer can be launched manually from the LANDesk Management Suite program group. The next time the inventory scanner runs, it sends completed forms to the core database.

You can also use the **Scheduled tasks** window to launch the form viewer on devices at a predefined time. In this scenario, use the **Scheduled tasks** window to first distribute the forms to devices. Make sure to allow enough time to distribute the forms before you use the scheduled task scriptable jobs feature to run the form viewer.

Filling out forms on the device

When the form viewer launches on the device, a list of forms and each form's status displays:

- **New:** Indicates the form has never been filled out by this user.
- **Completed:** Indicates the user has opened this form and filled out, at a minimum, the required fields.
- **Do again:** Indicates the user has completed this form before, but the form has since changed. The user needs to look at the form again and make any necessary changes. Once this is done, the form's status changes to completed.

Once users select a form to fill out and click Open, a simple Form wizard appears. It contains a list of questions and fields for answers. If there are more questions than fit on a page, there are Back/Next buttons. Users can click Help (or press F1) while the cursor is in a field to display a help message generated by the **Description** field in the form designer.

Users must answer any required questions before continuing to the next page or exiting a form. Required questions have a red dot beside them.

The last page of the form wizard has a **Finish** button that users click when they're done. Clicking this button returns users to the **Form selection** dialog where the status message beside the form name is updated.

Using an off-core inventory server

Normally, the core server processes inventory scans from managed devices. If you're concerned about the demand this scan processing is placing on your core server, you can install an off-core inventory server. This off-core inventory server contains a special version of the LANDesk Inventory Server service that will accept inventory scans and insert scan data into the database. Once you've configured an off-core inventory server, when the inventory scanner on a Windows-based device pings the core server, the core server replies telling the scanner to send its scan file to the off-core server.

The off-core inventory server only processes scans from Windows-based devices. The core server still processes scans from these devices:

- Macintosh
- Linux
- Unix
- Devices behind a Management Gateway
- Devices running pre-8.7 versions of the inventory scanner

The off-core inventory server has these system requirements:

- Microsoft Windows 2000 Server SP4, Microsoft Windows 2000 Advanced Server SP4, Microsoft Windows 2003 Standard Server, Microsoft Windows 2003 Enterprise Server, Windows XP Professional SP1
- .NET Framework 1.1
- ASP.NET 1.1
- MDAC 2.8 or higher
- Administrator privileges
- Can't install on a core server or rollup core server
- If the device is firewalled, you need to open port 5007

WARNING: Don't use the inventory Encrypted Data Transport option with off-core inventory servers

The **Configure LANDesk Software Services** dialog's **Inventory** tab has an **Encrypted Data Transport** option. Encrypted transport isn't compatible with off-core inventory servers. If you're using an off-core inventory server, make sure this option is disabled.

To install an off-core inventory server

1. From the device you want to make an off-core inventory server, map a drive to the core server's LDMAIN share and run \Install\Off-Core Inventory Server\Setup. This installs the off-core inventory server. When setup finishes, it will prompt you to reboot. Reboot to finish the installation.
2. From the core server, click **Start | Programs | LANDesk | LANDesk Configure Services**.
3. On the **Inventory** tab, click **Advanced settings**.
4. Click the **Off-core inventory server** option.
5. In the **Value** box, enter the off-core inventory server's computer name and click **Set**.
6. Click **OK**, and on the **Inventory** tab click **Restart** to restart the inventory service.
7. Go to the off-core inventory server, and from the **Services** Control Panel applet, restart the **LANDesk Inventory Server** service.
8. Windows-based device scans will now go to the off-core inventory server.

Note: Any time you make changes on the **Configure LANDesk Software Services** dialog's **Inventory** tab, you need to restart the **LANDesk Inventory Server** service on both the core server and the off-core server. Restarting the off-core service allows it to load the configuration changes you made.

Reports

The reporting tool can be used to generate a wide variety of specialized reports that provide critical information about the devices on your network.

Read this chapter to learn about:

- "Reports overview" on page 123
- "Understanding reports and report groups" on page 123
- "Running and viewing reports" on page 125
- "Publishing reports" on page 126
- "Creating custom reports" on page 129
- "Using the report designer" on page 130
- "Importing and exporting reports" on page 134
- "Creating .CSV files" on page 134

Reports overview

The reporting tool takes advantage of the robust inventory scanning utility, which collects and organizes hardware and software data, in order to produce useful, informative, and up-to-date reports. You can use the standard (predefined service and inventory reports, or create your own custom reports (see "Creating custom reports" on page 129). The predefined reports are provided by default with the application. The custom reports enable you to define a unique set of information with which to generate a report. The predefined or custom parameters are run and a report is generated containing the relevant data, which can be viewed from the console. Additionally, you can schedule reports to be published and saved to disk or to a secure file share location on your network where anyone with proper login credentials can access and view the reports. You can schedule the published reports to be e-mailed to designated recipients according to their rights and scope.

Understanding reports and report groups

Reports are organized in groups in the Reports window (**Tools | Reporting/Monitoring | Reports**). Administrators can view the contents of all of the report groups. Users with the Reports right can also see and run reports, as well as publish reports, but only on the devices included in their scope.

The left-hand pane of the **Reports** window shows a hierarchical view of the following report groups:

My reports

Lists the reports (and reports groups) you have added to your **My reports** group. These are typically reports that you run on a regular basis and have organized for your own use. They can be predefined or custom reports. Reports are run against the currently logged-in user's scope. An administrator has access to each user's reports groups and can add and remove reports (see "User reports" on page 125).

All custom reports

Lists all of the custom reports on your core server, including those created or imported by yourself or another user. For more information, see "Creating custom reports" on page 129.

Standard reports

Lists the predefined reports that are provided with the application. The reports are preformatted, have query properties and chart types assigned, and are ready to be used.

Management Suite log files

Lists the log files for scheduled tasks that are run on your system. These log files provide status information about various services, tasks, actions, or events that are executed on devices on your network. The log files include delivery method statuses, multicast client and subnet representative statuses, OS deployment success rates, scheduled task statuses, and so on.

Note: Log files are typically stored in the \LANDesk\ManagementSuite\log directory. You can specify a different directory location during installation by changing the path.

Inventory reports

Lists all of the predefined inventory reports. Inventory reports provide information about devices on the network, including which devices are assigned to users, the software being run on devices, how devices are used, the type of hardware, memory utilization, load capacities, specifications, and so on.

Software licensing monitoring reports

Lists all of the predefined software license monitoring reports. The reports provide information about the type of software being used, the frequency of usage, volume rates, and denial instances in order to monitor usage and ensure compliance with software license agreements.

Note: Software License Monitoring reports are not constrained by the user's scope.

Remote control reports

Lists all of the predefined remote control reports. The reports maintain a history of remote control usage based on client, console, computer, duration, and so on.

Unmanaged devices reports

Lists all of the predefined unmanaged device discovery reports. The reports provide information about unmanaged devices, including device types, network locations, applied agents, and so on.

Security and Patch Manager reports

Lists all of the security and patch manager reports. The reports provide information about vulnerabilities, spyware, security threats, blocked applications, LANDesk updates, custom definitions, and so on. The reports can be produced based on device types, dates, locations, and other criteria.

User reports

Lists all reports for individual users, which are organized into subgroups by user. User subgroups are named with their login IDs, such as `computername\user account` or `domain\user account`. Each user group contains the reports that appear in that user's My Reports group.

As with the **User devices** and **User queries** groups, the **User reports** group can be seen ONLY by a user with the LANDesk Administrator right. Administrators can access a user's reports group to run reports against that user's scope, as if they were that user. In this way, an administrator can preview exactly what a user will see when they run a report.

Running and viewing reports

You run the reports from the **Reports** tool window by double-clicking the report, or right-clicking the report and selecting **Run**. If prompted, select the relevant report criteria, and then click **OK**. The report data displays in the report viewer (see "Report viewer" on page 125). You can also run inventory reports directly from a device in the network view. From the network view, right-click the device you want to run a report for, click **Run inventory report**, and then double-click the report you want to run. If prompted, select the relevant report criteria, and then click **OK**. The report data displays in the **Report** viewer.

Note: Some reports are limited to a single device selection and will not run if more than one has been selected in the network view. A message box will notify you if the report cannot be run against multiple devices.

Report viewer

Once a report runs, the report viewer launches and displays the generated report with the specified information. This report viewer provides controls that enable you to display the report according to your viewing preferences. You can also export a report from the report viewer. The report viewer toolbar consist of the following:

- **Table of Contents:** Displays a table of contents for the report, if available. Click on a node in the tree to take you to that location within the report.
- **Print:** Opens your standard default printer dialog.
- **Copy:** Copies the contents of the report for the selected page.
- **Find:** Searches for a specific text string anywhere in the report data.
- **Single page view:** Displays the report as a single page.
- **Multiple page view:** Displays the report with multiple pages, which you can determine.
- **Zoom in:** Increases the size of the report.
- **Zoom out:** Decreases the size of the report.
- **Zoom percentage:** Selects the specific size of the report.

- **Previous page:** Takes you to the previous page in sequential order (compare with Backward).
- **Next page:** Takes you to the next page in sequential order (compare with Forward).
- **Page box:** Inserts a specific page number, which takes you directly to that page.
- **Backward:** Takes you to the previous page regardless of the numeric order.
- **Forward:** Takes you to the next page regardless of the numeric order.
- **Graph:** Determines whether to use a graph (none, bar, or pie), if available.
- **Sort:** Changes the sort order of the details of the report based on the selected column.
- **Export:** Enables you to export the report in HTML, PDF, XLS, DOC, and RTF formats.

Publishing reports

Publishing a report enables you to provide critical and timely information about your network devices to a controlled audience. When you publish a report, it is saved to a shared location on the network. The reports can be made accessible for viewing (see "Sharing published reports" on page 127), or sent to designated recipients (see "E-mailing reports" on page 128), even if they don't have access to the application. This enables the report to be shared with non-LANDesk users and reviewed at the reader's convenience. You can schedule reports to automatically be published at designated times, as well as configure them to reoccur on a regular basis (see "Scheduling to publish a report" on page 127).

Note: Reports don't have to be run before they are published. The report generation is performed during publishing. This can reduce bandwidth usage when you publish a large report that gathers and formats an extensive amount of data from across your network.

Defining a default user in the LANDesk reports user group

During the installation of LANDesk, you are prompted to create and define a user account in a user group called LANDesk Reports. This group controls access to the share where the published reports are stored. The default user group name is LANDesk Reports. You can change the name during installation. The LANDesk Reports user group shouldn't be changed after the application is installed.

You define a default user for this group by specifying a user name and password during installation. You can choose to clear this option during installation, but if you want to be able to provide access to published reports from a file share on a network, you should define the default user account. Send the default user's login information to the non-LANDesk users to give access to published reports. Existing LANDesk users can be added to the LANDesk Reports user group and use their own authentication, or be provided with the default user information as well. LANDesk users can be added to the LANDesk Reports group via the Windows NT users environment on the core server or by using local accounts (see "Managing local accounts" on page 285).

Publishing a report

When publishing a report, you can save the report file in any of the following formats: .HTML, .PDF, .XLS, .DOC, and .RTF.

To publish a report

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Locate the report you want to publish, right-click the report, and then click **Publish**.

Note: You do NOT have to run a report before publishing it.

3. If prompted, select the requested report criteria, and then click **OK**.
4. In the **Publish report** dialog, verify the name of the report (you can change this name if you like, verify the location where the report file is saved, specify the file format, and then click **Save**.

Note: The default storage location for published reports is in the **ldmain\reports** folder on your core server. This is the secured file share that only the LANDesk Reports user group has access to.

5. (Optional) In the **Report published** dialog, you can click **Preview** to verify the report's contents and formatting before sending the network path of the file share to recipients. You can also click **Copy path to clipboard** if you want to paste the full path and file name into another application for future reference, or directly into the body of an e-mail message to send to anyone you want to review the report.
6. Click **Close**.

Sharing published reports

Once a report is published to the shared folder on your core server, it can be accessed by an external audience if they have been given a valid user name and password to authenticate to the file share. Distribute the published report by sending your intended recipients the network path to the published report. The network path must contain the full path and filename. When the recipient accessed the file share, they are prompted to enter a valid user name and password for a user that is a member of the LANDesk Reports group before they can open and view the report. The default user for the LANDesk Reports user group is defined when you install the application (see "Defining a default user in the LANDesk reports user group" on page 126). If you've added other users to the LANDesk Reports group, they can use their own user name and password to access the published report.

Scheduling to publish a report

Automating the publishing process ensures the scheduled report is made available promptly at the time you designate. With the report scheduling feature, you don't have to be physically present to initiate the publishing. Configuring the publishing of the report to reoccur on a regular basis free up valuable resources to perform other important tasks. This provides continual and reliable reporting. The ability to schedule when to publish a report is paramount to making critical information available at the required time.

Note: Scheduling a report to publish is limited to certain types of reports.

To schedule the publishing of a report

1. Click **Tools | Reporting/Monitoring | Reports**.

2. Right-click on the report you want to schedule to be published.
3. Select **Schedule Publish**. A task with the report name is created under **Scheduled Tasks** and is highlighted.
4. From the **Scheduled Tasks** tool, right-click on the task and select **Properties**.
5. Under **Schedule task**, enter the desired scheduling information.
6. Under **Recipients**, select where to deliver the report.
7. Click **Save**.

E-mailing reports

In order to e-mail a report, create a scheduled task of the report to be published and designate the intended recipients. The reports you configure to be e-mailed are automatically sent to the recipients every time a scheduled report is run. The content of the reports are based on the users scope. E-mailed reports are delivered in .PDF format. You have to provide an e-mail address for the intended recipients under their individual user properties (see "About the user properties dialog" on page 714). Supplying an e-mail address will only make the users eligible to receive the report. You still need to select them as recipients from the scheduled task you create when you schedule the publishing of a report (see "Scheduling to publish a report" on page 127).

The following tasks must be completed before a report can be e-mailed to the intended recipients:

- "Scheduling to publish a report" on page 127
- "Assigning e-mail addresses to users" on page 128
- "Selecting the recipients of a report" on page 128
- "Configuring SMTP for e-mailing a report" on page 129

Assigning e-mail addresses to users

You must assign users e-mail addresses to make them eligible to receive reports. Once assigned, their user names will be available for selection as recipients when the schedule publishing task is created. For more information, see "About the Scheduled task - properties dialog" on page 712.

To assign e-mail addresses to users

1. Click **Tools | Administration | Users**.
2. Right-click on the user and click **Properties**.
3. On the **User** tab, enter an e-mail address for the intended recipient of the report.
4. Click **OK**.

Selecting the recipients of a report

You can select the recipients of the report. The file share location on your core server is the default destination. Select the users you want to have the report e-mailed to. To add recipients to the list, see "Assigning e-mail addresses to users" on page 128. For more information, see "About the Scheduled task - properties dialog" on page 712.

To select the recipients of a report

1. Click **Tools | Distribution | Scheduled tasks**.
2. Locate the scheduled task for the report you want to have e-mailed. Remember, the report must have been previously scheduled for publishing (see "Scheduling to publish a report" on page 127).
3. Right-click on the task of the report and select **Properties**.
4. Under **Recipients**, select the users you want to receive the report.
5. Click **Save**.

Configuring SMTP for e-mailing a report

Your outgoing mail server and the port number are required in order for reports to be e-mailed when a schedule publish task occurs. You can test your SMTP configuration to validate that it's set up correctly by sending a test e-mail to a designated address. For more information, see "About the Scheduled task - properties dialog" on page 712.

To configure SMTP for e-mailing a report

1. Click **Tools | Distribution | Scheduled tasks**.
2. Locate the scheduled task for the report you want to have e-mailed. Remember, the report must have been previously scheduled for publishing (see "Scheduling to publish a report" on page 127).
3. Right-click on the report and select **Properties**.
4. Under **SMTP configuration**, make sure the outgoing mail server (SMTP), the port number, the login information, and the test e-mail address are specified.
5. Click **Save**.

Creating custom reports

When creating custom reports, you specify what information will be displayed and how it will be displayed once the report is run. Each report consists of a query (custom or predefined), a layout (custom or predefined), and a graph selection (if applicable). The specified query will cause the appropriate data to be extracted from the database and populate the report at run time. The report is formatted according to the specified layout. The default report layout is used unless you choose otherwise. You can design a custom format using the report designer (see "Using the report designer" on page 130). For reports with graphing data, you can select a default grouping column and a graph type (pie, bar, or none) to have in the report.

Note: If you want a customer report with the same query data as a predefined report but in your own format, you will need to create a custom report that utilizes the same query parameters and then apply your formatting using the report designer.

You can create custom reports by right-clicking **My reports** from the Reports tool and then selecting **New custom report**. Administrators can also create custom reports by selecting a user from the **User reports** group by right-clicking a user and then selecting **New custom report**. Another method for creating custom reports is done directly from existing queries by right-clicking on a query and selecting **New custom report**. The New custom report icon can also be used to create a custom report. When you create a custom report, it's automatically added to the All Custom Reports group.

To create a custom report

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click on **My reports** and select **New custom report**.
3. From the **Reports properties** dialog, enter a title for the report, which also serves as the actual title of the report once it's generated.
4. Provide a description for the report, which also will be the formal description under the title in the final report.
5. Click **Select** or **Create** to specify a query.
6. If you want to alter the layout and formatting of the report, click **Design** to launch the report designer.
7. If applicable, choose the type of graph you want in your report.
8. Click **OK**.

Using the report designer

The report designer enables you to customize the layout and formatting of the reports you create in order to have the look and feel you require, whether it's to meet corporate style guides or produce a unique report. The layout and formatting capabilities of the report designer are similar to a desktop publishing application. You also have the additional functionality of having relational data fields within the report, which dynamically populate the report with data extracted from the database (see "Data fields" on page 132). The report designer is accessed from the Report Properties dialog when you create or modify a custom report (see "Creating custom reports" on page 129).

Note: Changing the title or description of the report from the report designer doesn't change the title and description in the **Report properties** dialog. You must change each one individually. Once you've made changes to the report layout, save the report and then make the corresponding changes in the dialog.

For information about the report designer, see the following sections:

- "About the report designer" on page 130
- "Using report templates" on page 133

About the report designer

Design Surface

The design surface acts as the canvas for the report. The report is segmented into specific content areas in a hierarchical order. The ReportHeader is always the top-tier node, and Details should always be the lowest-tier node. If you insert an additional GroupHeader (by right-clicking in the design surface), you may need to reorder the groups (also by right-clicking in the design surface). These report segments are collapsible and aid in the design process by keeping your surface area manageable. The grid, which can be turned on and off, is used to assist you with placing content on the design surface.

Toolbox

The toolbox consists of components (objects) that serve as the building blocks of the reports. They are placed onto the design surface in order to develop the structure and layout of your report. By inserting toolbox components, you begin to develop the foundation of your custom report. The toolbox is made up of the following components:

- **Pointer:** Selects components in the report. Just click a component on the design surface. Once a component is selected, you will be able to apply additional formatting, like resizing the component or applying different styles.
- **Label:** Inserts a label. Click and drag the box to define the boundaries of the label. The text of the label is added in the properties section while the label is selected.
- **Text box:** Inserts a textbox. Click and drag the box to define the boundaries of the text box. The text of the text box is added in the properties section while the text box is selected. Text boxes can be bound to a database field.
- **Checkbox:** Inserts a checkbox. Click and drag the box to define the width and height of the checkbox. Checkboxes can be bound to a database field.
- **Picture:** Inserts an image loaded from a file. Click and drag the box to define the width and height of the image. A dialog will prompt you to select an image for the picture component.
- **Shape:** Inserts a rectangle, circle, or square shape. Click and drag the shape to define its width and height.
- **Line:** Inserts a line. Click and then drag the line to the location you want the line to go.
- **Rich text box:** Inserts a rich text box. Click and drag the box to define the boundaries of the rich text box. When you release the button, a dialog will appear that enables you to select an RTF file. The content of the RTF file is placed in the rich text box. Clicking inside the rich text box will place a cursor in the box, which enables you to apply formatting to specific words. Rich text boxes can be bound to a database field.
- **Page break:** Inserts a page break.
- **Bar code:** Inserts a bar code. Click and drag the bar code to define the boundaries of the component. Bar codes can be bound to a database field.

Toolbars

The toolbars consist of standard formatting options, including text styles, fonts, font sizes, bold, italics, underline, justification, bullets, indentation, layering, and so on. Once the components have been placed onto the design surface, formatting can be applied to the components to achieve the desired appearance. Additional formatting is available from the Properties section. There are a few unique tools found on the toolbar:

- **OK:** Saves all changes and closes the report designer dialog.
- **Cancel:** Closes the report designer dialog without saving any changes.
- **New report:** Clears the report and provides a blank design surface in order to build a new report, however, you're still restricted to the same query fields you defined before entering the report designer.
- **Auto-generate report based on query:** Returns the report design to the original format before any changes were made. This enables you to restore the report to its original format according to the default settings.
- **Report settings:** Enables you to configure the report settings. The report settings consist of the following:
 - **Page Setup:** Defines the margins of the report.

- **Printer Settings:** Defines the paper size, print orientation, and other print properties.
- **Styles:** Enables you to create and edit font styles within the report
- **Global Settings:** Provides grid controls and defines the unit of measurement.

Data fields

The data field values are aliases of the query parameters that you defined before opening the report designer. The data fields are proxies or placeholders that are linked to a data source. When you run the report, the data field is replaced with the information extracted from the data source. Initially, the data fields are automatically placed in the report. If you've deleted them or you're starting a new report, you can drag and drop the data fields back onto the design surface. You cannot create data fields from within the report designer. You must specify the data fields in the query before launching the designer (from the **Report query** dialog, click **Select Columns>>**).

Data fields should be used primarily in the Details section of the design surface, but can also be placed in a GroupHeader section. When you use data fields in the GroupHeader section, you must also apply a data field to the GroupHeader itself in order for it to propagate down and create instances for all the queried data. This is needed to properly group the data. For example, using a data field to serve as a heading, like "device name," will insert the device name of every device in the database as the heading when the report is run. Each device name heading will be followed by the content designated in the details section (the next tier), which would be the rest of the data fields of the report. In the GroupHeader section of the design surface, the desired data field would be inserted first. Then the GroupHeader tag would be selected and have the data field in the Contents section changed to the same data field that was inserted into the data field.

Note: If you enter a data field value that doesn't exist according to the query, a missing data field box will appear above the data field box. Clicking the value provided in the missing data field box will select the erroneous data field on the design surface, so you will know which one to fix.

Contents

The Contents section contains a tree structure of the design surface. The main report is divided into the individual sections of the report. Any component placed onto the design surface in any given section is also represented in the tree under the corresponding report section. Clicking a node from the tree will select that item in the design surface, as well as display its properties directly underneath.

Properties

Each item, including report sections and components placed onto the design surface, has a unique set of properties. These properties are used to further configure your report and are more advanced than the standard formatting and layout tools. Not all properties are available for each node. Only the properties applicable to the selected item are given. The properties consist of the following:

- **Appearance:** Affects the look and feel of the selected item. All of the standard formatting tools are included.
- **Behavior:** Affects how the selected item will act.

- **Data:** Contains the actual content of the selected item, like textual information or a data field.
- **Design:** Provides a description of the selected item, which doesn't appear on the design surface.
- **Layout:** Provides the size and orientation of the selected item, like the location in terms of X and Y coordinates, or the size in terms of width and height.
- **Misc:** Contains any additional functionality for the selected item that is not included under the other property types.
- **Summary:** Enables you to create summations within the report. These total fields will automatically perform the mathematical equations at run time and display the computed value in the designated location.

Using report templates

You can create report templates to replace the default layout of a report. This makes it easier to create custom reports since a large portion of the customization will have already been performed. You only need to apply the report template to implement your custom look and feel. Once your template is loaded, you can further customize your new report as needed.

Note: Report templates only can be applied to custom reports.

Creating a report template

A report template is created from the report designer. You can alter the default template or another template and then save it as a template.

To create a report template

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **My reports** and then click **New custom report**.
3. Provide a title, description, query, and chart type and click **Design**.
4. From the report designer, build your new template by making all design, layout, and format modifications.
5. Click **File | Save as Template**.
6. Provide a title and description and click **OK**.

Applying a report template

Once a template has been created, it can be applied to any custom report.

Note: Apply the template before making any changes to the report. Any changes made in the report before the template is applied will be lost. This cannot be undone.

To apply a report template

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **My reports** and then click **New custom report**.
3. Provide a title, description, query, and chart type and click **Design**.
4. From the report designer, click **Tools | Templates**.

5. Select the template you want to apply and click **Load**.

Importing and exporting reports

The **Reports** tool supports both importing and exporting reports. You can transfer reports from one core database to another. The query is automatically imported and exported with the report since it is required by the report to display properly. Imported reports are placed into the **My reports**, **All custom reports**, and **User reports** groups.

Note: Changing the embedded query (XML) in the report will not produce a separate report. It will cause an error. If you want to make a change to the report, it must be done from the Reports tool in LDMS.

To import a report

1. Right-click the reports group where you want to place the imported report.
2. Select **Import** from the shortcut menu (or from the toolbar).
3. Navigate to the report file (.XML) you want to import and select it.
4. Click **Open** to add the report to the selected group in the network view.

You can export individual reports as well as entire reports groups and their contents.

To export a report

1. Right-click the report (or reports group) you want to export.
2. Select **Export** from the shortcut menu (or from the toolbar).
3. Navigate to the location where you want to save the report.
4. Type a name for the report.
5. Click **Save** to export the report.

Creating .CSV files

You can create comma-delimited files in plain text that are easily integrated into databases, spreadsheets, word processors, and so on. The file is created according to the inventory data that displays in the network view. These files are saved as generic .CSV files.

To create a .CSV file

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **Reports** and select **New CSV report**.
3. In the **New .CSV report** dialog, enter a name for the report.
4. Select whether to report on all devices or only selected devices.
5. Select whether you will use the current column configuration in the network view, or if you will select a different column configuration.
6. Click **OK** to save the .CSV file with a name and directory location you specify.

Note: You can also export a .CSV asset report for use with other reporting tools. You can export a .CSV report in one of the following formats: HTML, RTF, or TXT.

Anti-virus report

New anti-virus application data (name, version, and size) can be added to the Anti-VirusSummary.ini file, so the inventory scanner can collect the data and make it available for reporting purposes. Once you have manually added the application information to the file, use the software license monitoring tool to add the file to the scan list. Follow the directions given in "Adding files to LDAPPL3" on page 212 to add the updated Anti-VirusSummary.ini file.

Implementing localized messages

In order to implement localized messages, you must install the .Net Framework language pack for the language you are expecting the message to be in. These can be downloaded from Microsoft: <http://www.microsoft.com/downloads/details.aspx?familyid=04DBAF2E-61ED-43F4-8D2A-CCB2BAB7B8EB&displaylang=en>

Scripts and tasks

LANDesk Management Suite includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. Management Suite consoles and Web consoles can add tasks to the scheduler.

A task consists of a distribution package, delivery method, targeted devices, and a scheduled time. Non-distribution tasks consist of a script, targeted devices, and scheduled time.

Here are some of the tasks you can schedule:

- Device configurations
- Various custom scripts
- Custom data form deployments
- Unmanaged device discoveries
- Vulnerability scans
- Software execution on managed devices

Completing the script creation dialogs for these tasks generates an ASCII text file in the Windows INI format with an .INI extension. These scripts are stored on the core server in the \Program Files\LANDesk\ManagementSuite\Scripts folder. The script filename becomes the script name in the console. Software distribution scripts are an exception. They don't create an INI file and are instead stored in the database. The scripts only contain information about the task being completed, not which devices the script will run on. The scripts use a custom scripting language unique to Management Suite. For more information on scripts, see "Processing custom scripts" on page 630.

Read this chapter to learn about:

- "Managing scripts" on page 136
- "Scheduling tasks" on page 137
- "Using the Scheduled tasks window" on page 138
- "Assigning targets to a task" on page 140
- "What you see when tasks run" on page 141
- "Monitoring task status" on page 142
- "Viewing task logs" on page 142
- "Using the default scripts" on page 142
- "Using the rollup core to globally schedule tasks" on page 143

Managing scripts

LANDesk Management Suite uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools | Distribution | Manage scripts**) for these tasks:

- "Creating file deployment scripts" on page 768
- Custom scripts that you create

- "Using the local scheduler" on page 144

The Manage scripts window divides scripts into three categories:

- **My scripts:** Scripts that you created.
- **All scripts:** All scripts on the core server.
- **User scripts** (only visible to Management Suite administrators): Scripts created by all Management Suite users. These are sorted by the creator's username.

You can create groups under the **My scripts** item to further categorize your scripts. To create a new script, right-click the **My scripts** item or a group you've created and click the script type you want to create.

Once you've created a script, you can click Schedule on the script's shortcut menu. This launches the **Scheduled tasks** window (**Tools | Distribution | Scheduled tasks**) where you can specify devices the task should run on and when the task should run. See the next section for more information on scheduling tasks.

Due to specific capabilities supported by the Windows console, scripts created in the Windows console shouldn't be edited in the Web console.

Changes to script and task ownership for users of previous Management Suite versions

With Management Suite versions prior to 8.5, all scripts were global and all users could see them. In Management Suite 8.5, scripts are only visible to the script creator and Management Suite administrators.

The **Manage scripts** window (**Tools | Distribution | Manage scripts**) now has a **State** column. The **State** column shows **Public** if all users can see the script, or **Private** if only the user that created the script or administrators can see it. Users can right-click scripts they have created and toggle the **Public script** option on and off. Administrators can change the status of any script.

Scheduling tasks

The **Scheduled tasks** window shows scheduled task status and whether tasks completed successfully or not. The scheduler service has two ways of communicating with devices:

- Through the standard LANDesk agent (must already be installed on devices).
- Through a domain-level system account. The account you choose must have the log in as a service privilege. For more information on configuring the scheduler account, see "Configuring the scheduler service" on page 80.

The console includes scripts that you can schedule to perform routine maintenance tasks such as running inventory scans on selected devices. You can schedule these scripts from **Tools | Distribution | Manage scripts | All other scripts**.

Using the Scheduled tasks window

Use the **Scheduled tasks** window to configure and schedule scripts you've created. Schedule items for single delivery, or schedule a recurring task, such as a script task to regularly search for unmanaged devices.

The **Scheduled tasks** window is divided into two halves. The left half shows task tree and tasks, and the right half shows information specific to what you've selected in the tree.

Left pane

The left pane shows these task groups:

- **My tasks:** Tasks that you have scheduled. Only you and Management Suite administrative users can see these tasks.
- **Common tasks:** Tasks that users have marked common. Anyone who schedules a task from this category will become the owner of that task. The task remains in the **Common tasks** folder and will also be visible in the **User tasks** group for that user.
- **All tasks:** Both your tasks and tasks marked common.
- **All policies:** Any task that is active as a policy. These tasks also appear in the other task groups. This group provides a convenient way of seeing active policies.
- **User tasks** (Management Suite administrative users only): All tasks users have created.

You can drag scripts onto the **Scheduled tasks** window's left pane. Once a script is in the left pane, you can configure targets for it by dragging devices, queries, or groups to the right pane.

When you click **My tasks**, **Common tasks**, or **All tasks**, the right pane shows this information:

- **Task:** The task names.
- **Start On:** When the task is scheduled to run. Double-click a task name to edit the start time or to reschedule it.
- **Status:** The overall task status. View the right pane **Status** and **Result** columns for more details.
- **Owner:** The name of the person who originally created the script this task is using.

When you click a scheduled task, the right pane shows this summary information:

- **Name:** The task state name.
- **Quantity:** The number of devices in each task state.
- **Percentage:** The percentage of devices in each task state.

When you click a task status category under a task, the right pane shows this information:

- **Name:** The device name.
- **Status:** The task status on that device (for example, "Waiting").
- **Result:** Whether the task ran successfully on the device.
- **LDAP object name:** If the device was targeted through LDAP, the LDAP object name.
- **Query name:** If the device was targeted through a query, the query name.
- **Message:** Custom messages from the device. These are used with tasks that run a DOS batch file. Include a command that launches sdclient.exe with a /msg="<Message you want to send>" command-line parameter.

- **Log file:** If a device failed to complete the task, the path to the task log file for that device is here.

Before you can schedule tasks for a device, it must have the standard LANDesk agent and be in the inventory database.

To schedule a task

1. In the **Manage scripts** window, click **Scripts | My scripts** or **All other scripts**, and the script you want to distribute.
2. Click the **Schedule** button. This displays the **Scheduled tasks** window and adds the script to it, where it becomes a task.
3. In the **Network view**, select the devices you want to be task targets and drag them onto the task in the **Scheduled tasks** window.
4. In the **Scheduled tasks** window, click **Properties** from the task's shortcut menu.
5. On the **Schedule task** page, set the task start time and click **Save**.

You can add more devices to the task by dragging them from the network view and dropping them on the task you want in the **Scheduled tasks** window.

Canceling a task

You can cancel waiting or active tasks. The way to cancel a task depends on the task type, as described below.

- **Software distribution tasks:** Use the cancel button on the toolbar. This toolbar button is only available for software distribution tasks.
- **Custom scripts:** From the shortcut menu of the script you want to cancel, click **Current status**. The **Task status** dialog has **Discontinue task** and **Cancel task** buttons. Click the button you want.
- **Waiting tasks:** From the shortcut menu of the task you want to cancel, click **Properties**. On the **Schedule task** page, click **Leave unscheduled**.

Understanding the Common tasks folder

The **Common tasks** group provides a convenient way for multiple users to access the same task. Tasks marked common appear in the **Common tasks** group as well as in the **User tasks** group for the user that last modified the task. Having the task in both places allows multiple users who share similar responsibilities to access and modify the task.

A user can mark any task that is visible to them as common. Once a user clears the common option, the task is only visible in their **User tasks** group.

To mark a task common

1. From the shortcut menu of the task you want to make common, click **Properties**.
2. On the **Overview** tab, check **Show in common tasks**.

Alternatively, you can use the mouse to drag tasks from the **My tasks** group to the **Common tasks** group.

Assigning targets to a task

Once you've added a script to the **Scheduled tasks** window, you can assign targets to it. Drag targets from the network view onto the task that you want in the **Scheduled tasks** window. Targets can include individual devices, device groups, LDAP objects, LDAP queries, and inventory queries. Queries and groups are powerful options that let you have a dynamic list of devices that can change for recurring tasks. For example, as the device target list from a query changes, any tasks using that query will automatically target the new devices.

If a device is targeted more than once, such as when two target queries have overlapping results, the core server detects the duplication and won't run the task multiple times for the same device.

When using queries for task targets, the query won't run until the task is started. The **Scheduled task properties** dialog won't show the target devices until after the task is launched.

Applying scope to tasks

For scheduled tasks, multiple Management Suite users can add targets to a task. However, in the **Scheduled tasks** window, each Management Suite user will only see targets within their scope. If two Management Suite users with scopes that don't overlap each add 20 targets to a task, each Management Suite user will see only the 20 targets they added, but the task will run on all 40 targets.

Selecting targets for your task

Each task you create needs a set of targets that the task will run on. Tasks can have two types of targets, static and dynamic.

- **Static targets:** A list of specific devices or users that doesn't change unless you manually change it. Static targets can be LDAP users or devices from Directory Manager or devices from the console's network view.
- **Dynamic targets:** A dynamic list of devices that allows policy-based distribution tasks to periodically check the target list for any changes. Dynamic targets include query results and LDAP groups/containers or network view groups.

Dynamic policy targets are unique, in that Management Suite updates the results of these queries periodically. As new devices meet the query criteria, recurring tasks using those queries get applied to the new devices.

You can specify static policy targets in these ways:

- **Network view devices :**A static set of devices from the core database.
- **LDAP users or devices:** A static set of user and/or device objects.

You can specify dynamic policy targets in these ways:

- **Network view group:** A dynamic set of devices from the core database.

- **LDAP group/container:** A dynamic set of user, machine, or group objects.
- **Database query:** A set of devices generated by a query against the core database.
- **User group:** A group of users selected from an LDAP-compliant directory.
- **LDAP query:** A set of users, devices, or both, generated by a query on an LDAP-compliant directory.

Targeting devices through a directory

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct device software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager.

Windows 95/98 devices need to be configured to log into the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management. As of this printing, more information on installing Active Directory device support was available here:

<http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utils/dsclient.msp>

For each Windows NT/2000/2003/XP device, there must be a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged into the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows NT domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools | Distribution | Directory manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "LDAP queries" on page 108.

What you see when tasks run

The **Scheduled tasks** window always shows job status. If you're scheduling device configurations or OS deployments, you'll also see the **Client setup utility** dialog. As the scheduler service proceeds through the target list, you'll see the devices to be configured, devices being configured, and devices completed lists. For more information, see "About the Client Setup Utility dialog" on page 694.

If you're scheduling Targeted Multicast distributions, you'll see the **Multicast software distribution status** window. This window shows multicast status. For more information, see "About the Multicast software distribution status window" on page 767.

If you're scheduling custom scripts, you'll see the **Custom job processing** window showing scheduled, working, and completed targeted devices, in addition to a line-by-line script status as it executes.

Monitoring task status

When a task starts processing, targeted devices move through various task states. You can monitor the task state for targeted devices by clicking an active task in the Scheduled tasks window. Devices will be in one of these categories:

- **All devices:** All targets for the task.
- **Active:** Targets that are currently being processed.
- **Pending:** Targets that haven't been processed yet.
- **Successful:** Targets that completed the task successfully.
- **Failed:** Targets that failed the task.

These are the states the device can be in, and the category they are visible in:

- **Waiting:** Ready to process a task. (**Pending**) category
- **Active:** Processing the current task. (**Active**) category
- **Done:** Task processed successfully. (**Successful**) category
- **Busy:** Device is already processing a different task and couldn't process the current task. (**Failed**) category
- **Failed:** Didn't complete processing the task for some reason. (**Failed**) category
- **Off:** Device was off or unreachable. (**Failed**) category
- **Canceled:** The user cancelled the task. (**Failed**) category

Viewing task logs

If a device fails to process a task, the **Scheduled tasks** window stores the task log. Available logs appear in the **Log file** column next to a device. In the log file you can see the task command that failed.

Using the default scripts

Management Suite ships with a default set of scripts that are listed below. You can use them to help you complete some Management Suite tasks. These scripts are available under the **All other scripts** tree in the **Manage scripts** window (**Tools | Distribution | Manage scripts**):

- **am_verifyall:** Verifies all packages installed via policies on clients
- **Generic sample dir command:** Uses an OS deployment script to demonstrate rebooting a device with a virtual disk and running a dir command.
- **inventoryscanner:** Runs the inventory scanner on the selected devices.
- **multicast_domain_discovery:** Does a Targeted Multicast domain representative discovery. For more information, see "Using Targeted Multicast with software distribution" on page 178.
- **multicast_info:** Runs a troubleshooting script that shows what information the Scheduled Tasks window will pass to Targeted Multicast, including target device IP addresses and subnet information. Creates a file called C:\MCINFO.TXT.
- **MSI service deployment:** Deploys the MSI service required for a PXE representative.
- **PXE representative deployment:** Deploys or updates a PXE representative.
- **PXE representative removal:** Removes the PXE service software from a PXE representative.

- **Restore client records:** Runs the inventory scanner on selected devices, but the scanner reports to the core the device was configured from. If you have to reset the database, this task helps you add devices back to the proper core database in a multi-core environment.
- **Uninstall metering client:** Removes the software metering agent on target devices. This agent was used in Management Suite prior to version 8.

Understanding bandwidth options

When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute.

You can select these bandwidth options:

- **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
- **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
- **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools | Configuration | Agent | Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.

Using the rollup core to globally schedule tasks

If you have a rollup core in your LANDesk environment, tasks you create on it are globally scheduled and can have targets from multiple child cores. When you create a task on the rollup core and schedule it, the rollup core checks the target list to see which targets belong to which child core server. The rollup core then sends each child core server the task and its unique portion of the overall target list. Each child core server runs the task in the background and reports task status to the rollup core.

If a child core server has targets but doesn't have a rollup core certificate, which is necessary for a child core to process globally scheduled tasks, the rollup core runs the task on those targets instead.

Globally scheduled tasks and task status doesn't appear in the child core's **Scheduled tasks** window. The easiest way to view this information is from the task details on the rollup core. If you want to see delegated task status on a child core that is processing the task, you can use the Delegated Tasks report.

To view delegated task status on a child core

1. On the child core, click **Tools | Reporting / Monitoring | Reports**.
2. In the reports window, click **Standard Reports | Management Suite Delegated Task Status**.
3. Double-click the **Delegated Tasks** report, and enter the date range you want.
4. Click **OK** to see the report.

To reduce network traffic, task status on delegated tasks isn't reported in real-time to the rollup core. Instead, task status is updated every two minutes by default. Do the following to change this interval.

To change the task status check interval

1. On the rollup core, click **Start | Programs | LANDesk | LANDesk Configure Services**.
2. On the **Scheduler** tab, click **Advanced**.
3. Click **Delegate task status check**, and click **Edit**.
4. Enter the number of seconds you want the scheduler to wait between task status checks, and click **OK**.
5. From the **Scheduler** tab, **Restart** the scheduler service on the rollup core.

Using the local scheduler

The local scheduler is a service that runs on devices. It's part of the common base agent and you can install it through device setup. Usually the local scheduler handles Management Suite tasks, such as running the inventory scanner periodically. Other tasks that you schedule, such as software or OS deployments, are handled by the core server rather than the local scheduler. You can use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script, you can deploy it to devices by using the **Scheduled tasks** window.

The local scheduler assigns each task an ID number. Local scheduler scripts have an ID range that is different from the default local scheduler scripts that Management Suite uses. By default, you can only have one custom scheduler script active on each device. If you create a new script and deploy it to devices, it will replace the old script (any script in the custom local scheduler ID range) without affecting the default local scheduler scripts, such as the local inventory scan schedule.

When selecting schedule options, don't be so restrictive that the task criteria are infrequently met, unless that's your intention. For example, while configuring a task, if you select Monday as the day of the week and 17 as the day of the month, the task will only execute on a Monday that's also the 17th of the month, which happens very infrequently.

To configure a local scheduler command

1. In the **Managed scripts** window (**Tools | Distribution | Manage Scripts**), from the My scripts shortcut menu, click **New local scheduler script**.
2. Enter a **Script name**.
3. Click **Add** to define the script options.
4. Configure the local scheduler options as described earlier.

5. Click **Save** to save your script.
6. Use the **Scheduled tasks** window to deploy the script you created to devices.

Installing the local scheduler service on an unmanaged Device

LANDesk's Local Scheduler service can be installed on an unmanaged device. Only two files are required for local scheduler functionality:

- LocalSch.exe
- LTapi.dll

To install the LANDesk Local Scheduler service on an unmanaged server or workstation, follow the steps below.

1. Create the following folder.

%ProgramFiles%\LANDesk\LDClient
2. Copy LocalSch.exe and LTapi.dll to this folder.
3. Click **Start | Run** and type the following command.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /i
```

Uninstalling the Local Scheduler service

To uninstall the LANDesk Local Scheduler service, follow the steps below.

1. Click **Start | Run** and type the following command.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /r
```

2. Delete the files and folders.

LocalSch.exe command-line parameters

In addition to monitoring and running local tasks, LocalSch.exe can be used to install or remove the service, add new tasks, and list all of the currently configured tasks.

The following are the command line options supported by the local scheduler application.

```
LocalSch.exe [/i] [/r] [/d] [/tasks] [/isinstalled] [/del] [/removetasks]
[/exe=<executable>] [/cmd=<command line>] [/start="<date/time>"]
[/freq=xxx]
[/user] [/bw=xxx|<server>] [/tod=<begin>|<end>] [/dow=<begin>|<end>]
[/dom=<begin>|<end>] [/ipaddr] [/taskid=<id>] [/range=<min>|<max>]
```

/i – Install service

Installs the local scheduler service on the device. After being installed the local scheduler will still need to be started.

/r – Remove service

Removes the local scheduler service from the machine. The local scheduler service should be stopped before removing the service.

/d – Run in debug mode

Runs the local scheduler in a debug mode. When run in debug mode, the local scheduler runs as a normal Windows process rather than as a service or pseudo service. This mode does not result in any additional debug output.

/isinstalled – Is installed check

Checks to see if the local scheduler service is installed on the local computer. This method will return S_OK, or zero, if the local scheduler is installed. If the local scheduler is not installed a non-zero value will be returned.

/tasks – List tasks

This command will output the currently configured tasks to stdout but can only be seen in a command prompt if piped to more.

```
LocalSch.exe /tasks | more
```

The output can be redirected to a text file, tasks.txt for example, using the following command line:

```
LocalSch.exe /tasks > tasks.txt
```

Adding a task with LocalSch.exe

The rest of the command-line parameters are used for adding a local task. When adding a local task, you must specify the executable using the /exe parameter. If the user or process executing the command line doesn't have administrator rights, the task won't be scheduled. If the current user doesn't have administrator privileges, the task won't be created.

In addition to the command line options outlined below, the /taskid option may be used to specify the task.

/exe=<executable> - Scheduled application

Specifies the application that is to be launched when the scheduled time arrives. If this parameter isn't provided, the local task won't be created.

/cmd=<command line> - Application command line

Specifies the command line to be used when the scheduled application is launched. If this parameter is not specified, the scheduled application will be launched without command line parameters.

/start="<date/time>" – Start time

Specifies the start time for the application. If this parameter isn't specified, the application will be launched as soon as possible. If any filters are specified they must be satisfied before the application is launched. The start time is specified in local system time of the computer and has the following format:

```
/start="06 Nov 2001 17:39:47" /bw=WAN|myserver.domain.com
```

This format is a shortened version of the format used by HTTP. The month is always specified using a three-letter ASCII abbreviation: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec. If the format of the date is specified incorrectly, the task won't be added.

/freq=xxx – Frequency

Specifies a periodic frequency. Frequency is the number of seconds before the task will be run again. If this parameter isn't specified or is zero, the task will only be run once.

/user – User filter

Specifies that a user filter should be created for the task. A user filter will prevent the task from being run until a user is logged onto the system.

/bw=xxx|<network host> - Bandwidth filter

Specifies the bandwidth needed to a specific network host. The bandwidth can be specified as LAN, WAN, or RAS. If another bandwidth value is used the local scheduler will default to RAS bandwidth. The task won't be run until the local scheduler detects that the specified type of bandwidth is available between the device and the specified network host.

For example, the following filter would specify not running the task until at least WAN connectivity is available to the myserver.domain.com computer.

```
/bw=WAN|myserver.domain.com
```

/tod=<begin>|<end> - Time of day filter

Specifies a time of day filter. The task won't be run unless the time of day is between the specified begin and end hours. Time of day values are specified as the hour 0 through 23. For example, the following filter would specify running a task between 7 p.m. and 10 p.m.

```
/tod=19|22
```

/dow=<begin>|<end> - Day of the week filter

Specifies a day of the week filter. The task won't be run unless the weekday is between the specified begin and end days. Day of week values are specified as an integer with 0 being Sunday. For example, the following filter would specify running a task between Sunday and Thursday.

```
/dow=0|4
```

/dom=<begin>|<end> - Day of month filter

Specifies a day of the month filter. The task won't be run unless the day of the month is between the specified begin and end days. The day of month filter is specified using numeric value between 1 and 31. For example, the following filter would specify running the task between the 16th and 28th of the month.

```
/dom=16|28
```

/ipaddr - IP address change filter

Specifies that the task should be run whenever the IP address of the machine changes. This functionality requires the IP Helper libraries and is not available on Windows 95 systems and on Windows 98/NT systems without Internet Explorer 4 or later installed.

Deleting a task with LocalSch.exe

The local scheduler provides the ability to delete one or more tasks. The following parameters are used when deleting tasks.

/del – Delete task or tasks

Deletes the task specified by the /taskid parameter or deletes all tasks within the /range max and min values inclusive. The task IDs can be determined by either looking at the tasks using /tasks command line option or by using a constant /taskid when adding a task.

/removetasks – Remove all tasks

Removes all currently scheduled local tasks.

/taskid – Specifying the task ID

Specifies the ID of the task that is being deleted. Task IDs can be determined by looking at the tasks currently scheduled (see /tasks above). The ID is specified as an integer value.

/range=<min>|<max> – Range of task IDs

Specifies a minimum and maximum value of a range of task IDs. It can be used with the /del command to remove all tasks with task IDs within the given range.

Normally when generating a task an ID is randomly assigned, using the current time (time_t) value as the task ID. A randomly assigned ID will never be less than 100000. This command line parameter can be used to specify the ID for the task. Task ID values 0 -1000 are reserved for internal LANDesk Software use. Task ID values 1001-2000 are reserved for use by the management console's local scheduler interface.

Character parsing and the command line

The local scheduler uses standard white space-delimited parsing for the command line. This means that if any of the parameters contain white space they need to be enclosed in quotation marks. Certain parameters, such as /start, always contain white space and hence always need to be quoted. Other parameters, such as /exe and /cmd, may or may contain white space and may or may not need to be quoted.

The following example shows a command line that does not need quotation marks.

```
LocalSch.exe /exe=c:\windows\system32\cmd.exe
```

The following example shows a command line that does need quotation marks.

```
LocalSch.exe /exe="%ProgramFiles%\LANDesk\amclient.exe" /cmd="/apm /s /ro"
```

Quoting already quoted parameters

If the parameters that are to be passed to /cmd= are already quoted, then three quotes are required. One set to quote the entire string. Another to quote the quoted values, and the quoted values.

For example, the following command line shows an example of parameters that need to be surrounded by three quotation marks.

```
LocalSch.exe /exe="%ProgramFiles%\LANDesk\File  
Replicator\LANDeskFileReplicatorNoUI.exe "  
/cmd=" " "%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml" "  
" "%ProgramFiles%\LANDesk\File Replicator\replicator.log" " "
```

In the above command, the two parameter are paths to files. Because both paths are in the "Program Files" directory, they paths have spaces and must be quoted in order to be proper parameters for LANDeskFileReplicatorNoUI.exe. So each quoted parameter is surrounded by a second set of quotes, and then the entire string is surrounded by quotes.

Quoting redirection operators

Quotes must also surround any switches that contain a redirection operator. Redirection operators include the following symbols: <, >, |. The /bw switch uses a | character called a pipe or bar. It is important to remember that the | character is used in the command prompt to pipe the output to another application. To prevent this character from being parsed by the command line, it must be surrounded with quotes.

For example, the following command uses a /bw parameter with a | character and needs to be quoted.

```
LocalSch.exe /exe=C:\ldclient\amclient.exe /cmd="/apm /s /ro"  
/bw="LAN|server"
```

Remote control

Use LANdesk Management Suite's remote control feature to easily resolve device problems from one location. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users, you and the end user. You can do anything at the remote device that the user sitting at it can do. All of your actions are in real-time on that device.

Management Suite enables you to remote control these device types:

- Windows NT/2000/2003/XP/Vista devices
- Windows 95/98 devices
- NetWare servers
- Mac OS 9.2, 10.2.x and greater devices

The remote control viewer application runs on both Windows And Mac OS 10.2.x devices.

Read this chapter to learn about:

- "Using the remote control viewer" on page 151
- "Connecting to devices" on page 152
- "Remote controlling devices" on page 152
- "Using the drawing tools on remote devices" on page 153
- "Adjusting remote control settings" on page 153
- "Optimizing remote control performance" on page 154
- "Chatting with remote devices" on page 156
- "Transferring files to remote devices" on page 156
- "Running programs on remote devices" on page 157
- "Rebooting remote devices" on page 157
- "Changing device remote control security" on page 157
- "Using remote control logging" on page 158
- "Customizing the viewer and remote control agents" on page 159

Using the remote control viewer

Use the remote control viewer to remotely access a device. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users--you and the end user. You can do anything at the remote device that the user sitting at it can do.

You can do a lot more than just remote control a device from the viewer window. Once the viewer connects to a device, you can choose from these tasks:

- **Remote control:** Remotely view and control a device.
- **Chat:** Remotely chat with a device.
- **File transfer:** Remotely transfer files to and from your computer to another device. In essence, this works as though you've mapped a drive to remote device.
- **Reboot:** Remotely reboot a device.
- **Draw:** Displays drawing tools you can use to draw on the remote screen.

You can do multiple viewer tasks on a device at the same time. When you activate a viewer task, the interface for that task appears in the viewer window.

Once you've taken control of a remote device, its screen appears in the viewer window. Because the viewer window often isn't as big as the remote device's screen, you'll either need to use the autoscroll feature to scroll up, down, and side to side, or use the **Move Remote Screen** icon to maneuver more easily around the different areas of the remote screen. Also, autoscroll automatically scrolls the window as the mouse pointer approaches the viewer window's edge.

You can also increase the viewer window displayable area by disabling items in the View menu, such as connection messages, the toolbar, or the status bar. Use the **View** menu's **Full screen** option to completely remove the viewer window's controls. If the remote screen's resolution exceeds yours, autoscroll will still be necessary.

If you want to speed up the viewing rate or change the viewer window settings, use the items under the **Options** menu. To remotely chat, transfer files, or reboot the device, use the items under the **Tools** menu or the toolbar.

Connecting to devices

Before you can do any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see connection messages and status in the **Connection messages** pane, if that is visible. If it isn't, you can toggle it by clicking **View | Connection messages**.

To connect to a device

1. In the network view, from the shortcut menu for the device you want to remote control, click **Remote control**, **Chat**, **File transfer**, or **remote execute**.
2. Once viewer window appears and connects to the remote device, you can use any of the remote control tools available from the viewer's **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File | Stop connection**.

Remote controlling devices

Once you've connected to a device, often you'll want to view it remotely.

To view a remote device

- Click **Tools | Remote control**. If options in the **Tools** menu are dimmed, that means you aren't connected to a device.

To view different areas of a remote device screen

1. Move the mouse pointer to the edge of the viewer window. The window scrolls automatically.

OR

1. Click the **View another part of the remote screen** icon.
2. Your cursor becomes a hand that you can click, drag, and release to view various areas of the remote screen.

Using the drawing tools on remote devices

Once you're remotely viewing a device, you can use the drawing tools on it. The drawing tools can help you explain to users what you're doing or highlight information on the remote screen for users to look at. When you use a tool to draw on the screen, both you and the remote user can see what you've drawn. The drawn images stay on both your screens until you click the eraser in the drawing tool palette.

You have three drawing tools to choose from:

- **Pencil:** Use the pencil tool to make freehand drawings. You aren't limited to a shape with the pencil tool.
- **Box:** Use the box tool to draw a rectangle around something on the screen. Click where you want a corner of the rectangle to be, and while holding down the mouse button, drag it over the area you want boxed. Release the mouse button when you're ready for the rectangle to be drawn.
- **Pointer:** Use the pointer tool to point at objects on screen. When you hold down the left mouse button, the pointer tool is active and a red dot appears under the mouse pointer that makes it easy for users to see where the pointer is. When you release the left mouse button, the dot disappears. You can't change the dot color and it doesn't leave a trail like the pencil tool does.

You can also use the line thickness and line color drop-down lists to change how your drawings will look. Changes to these items only affect new things that you draw.

When you're done drawing, click the eraser button on the drawing palette or close the palette.

Adjusting remote control settings

Use the **Options** dialog's **Change settings** tab (**Tools | Options**) to adjust the remote control settings.

- **Allow autoscroll:** Enables the viewer window to scroll as you move the cursor closer to the window border. The closer you move to the border, the faster the scrolling occurs.
- **Lock out the remote keyboard and mouse:** Locks the remote device's keyboard and mouse so that only the user running the viewer can control the remote device. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards to paste between local and remote computers:** Synchronizes the keyboards between the local and remote device so you can paste information between the two devices.
- **Blank the remote computer screen:** Blanks the remote device's screen so only the user running the viewer can see the user interface display on the remote device.
- **Lock the remote computer when the session ends:** When the session ends, activates the operating system's lock feature.

- **Auto keyboard mapping:** You should keep this option checked. It remaps the target device's keyboard so it matches the administrators. This helps ensure what the administrator is typing appears correctly on the target device. This is especially useful when the administrator and target keyboards are based on different alphabets or languages.
- **Enable old agent compatibility (pre-8.5 agents):** LANDesk Software changed remote control security and added a new remote control viewer in version 8.5. If you have remote control agent versions on your network that are pre-8.5, you can check this option to allow the new remote control viewer to communicate with these older agent versions.

Using alternate names

Depending on how you've configured the remote control agent on managed devices, users on a device that's being remote controlled can double-click the remote control status icon in the Windows system tray and see the computer name and user name of the administrator that is remotely controlling them. If you don't want your real computer or user names to be visible from remote devices for security reasons, you can specify an alternate user name and/or computer name that appears in the remote control status dialog on remote devices.

To use alternate names

1. Click **Tools | Options**.
2. On the **Change settings** tab, check **Use alternate names**.
3. Specify the names you want users at remote devices to see.
4. Click OK.

Optimizing remote control performance

Use the **Options** dialog's **Optimize performance** tab (**Tools | Options**) to optimize remote control performance for these connection types:

- Slow connection (modem)
- Medium connection (broadband)
- Optimize for fast connection (LAN)
- Custom connection

Changing the optimization setting dynamically adjusts color reduction, wallpaper visibility, and remote windows appearance effects (the ones you can adjust in **Display Properties | Appearance | Effects**), such as transition effects for menus and tooltips.

Remote control always uses a highly efficient compression algorithm for remote control data. However, even with compression, it requires a lot of data to send high color depth information. You can substantially reduce the amount of remote control data required by reducing the color depth displayed in the remote control viewer. When the viewer reduces the color depth, the viewer has to map the full color palette from the remote desktop to a reduced color palette in the viewer. As a result, you may notice colors in the remote control window that don't accurately reflect the remote desktop. If that's a problem, select a higher-quality compression setting.

Another way you can optimize performance is to suppress the remote wallpaper. When you do this, remote control doesn't have to send wallpaper updates as parts of the remote desktop are uncovered. Wallpaper often includes bandwidth-intensive images, such as photographs. These don't compress well and take time to transfer over slower connections.

The final way you can optimize performance is to use a mirror driver on the remote device. For more information, see the next section.

Using the mirror driver

The mirror driver provides many benefits. The main benefit is that it provides a Microsoft-supported way of capturing screen output without requiring modifications to the existing video driver. This allows the remote control mirror driver to behave in a standard way that can cause fewer problems on devices.

The other benefit is that the mirror driver doesn't use as much processing power from the target device. If you're remote controlling devices that have a 1.5 GHz or slower processor, the mirror driver can provide noticeable performance improvements over faster network connections. On slower network connections, remote control performance is limited more by bandwidth than processor utilization.

The standard remote control agent is always installed on devices. When the mirror driver is installed with it, the standard agent and the mirror driver coexist. You can't uninstall the standard remote control driver and use only the mirror driver.

Changing viewer hot key settings

The remote control viewer supports the following hot keys:

- **Enables hot keys** (Ctrl + Alt + H): Enables/Disables hot key availability. Hotkeys are enabled by default.
- **Close viewing session** (Ctrl + Alt + S): Disconnects the current viewing session. The remote control viewer window stays open.
- **Send Ctrl-Alt-Delete** (Ctrl + Alt + D): Sends Ctrl+Alt+Delete to the target device.
- **Lock out remote keyboard and mouse** (Ctrl + Alt + K): Enables/Disables the target device's local mouse and keyboard.
- **Full screen toggle** (Ctrl + Alt + M): Toggles the remote control viewer between windowed mode and full screen mode.
- **Send Ctrl+Esc** (CTRL + Alt + E): Sends CTRL+ESC to the target device.

You can change a hot key by clicking in the box next to it and pressing the new key combination. The print screen or pause/break keys can't be part of a key combination.

Sending CTRL+ALT+DEL to Vista devices

The default local security policy on Windows Vista won't allow CTRL+ALT+DEL from a remote control viewer. To change this, do the following.

To allow CTRL+ALT+DEL on Vista devices

1. In the **Start** menu's search box, type **gpedit.msc** and press **Enter**.
2. Navigate to **Local Computer Policy | Administrative Templates | Windows Components | Windows Logon Options | Software Secure Attention Sequence**.
3. Double-click **Disable or Enable Software Secure Attention Sequence**.
4. Click **Enabled**, and in the drop-down list click either **Services** or **Services and Ease of Access applications**.
5. Click **OK**.

Chatting with remote devices

You can use the remote control viewer to remotely chat with a user at a remote device. This feature is useful if you need to give instructions to a remote user whose dial-up connection is using the only available phone line. Users can respond back using the chat window that appears on their screen. You can only use chat on devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

If you want to save the messages from a chat session, you can. Any text appearing in the gray area of the chat session will be saved to a text file.

To chat with a user at a remote device

1. Click **Tools | Chat**. A section of the viewer window turns into a chat area.
2. In the lower left section of the chat area, type in a short message. Click **Send**.

Your message will appear on the remote device's screen. A user can respond by typing a message and clicking **Send**. The user also can click **Close** to exit out of a chat session.

To save messages from a chat session

1. In the chat area of the viewer window, click **Save messages**.
2. In the **Save as** dialog, type in a filename and click **Save**.

Transferring files to remote devices

You can use the remote control viewer to transfer files to and from your computer to the remote device. In essence, this works as though you've mapped a drive to the remote device. You can only transfer files to/from devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To transfer files to a device

1. Click **Tools | File Transfer**. Windows Explorer appears.
2. Select a file to transfer by clicking the filename. From the file's shortcut menu, click **Copy**.
3. Scroll down the Windows Explorer tree to **LANdesk Remote Control**. You should see the name of the remote device you're currently controlling.
4. On the remote device, select a folder to paste the file to, then right-click and click **Paste**.

Similarly, you can also transfer files from a remote device to your computer.

Running programs on remote devices

You can launch programs on remote devices. Use the Run box on the viewer toolbar to enter the remote program's path and filename. Since the program will be launched on the remote device, the path and filename you enter must be present on the remote device.

To run a program on a remote device

1. In the viewer's **Run** box, enter the program path and filename. If you don't know either, you can drop down the list and click **Browse**. This opens a dialog that allows you to browse the remote device's folders.
2. Click the **Remote execute** button to the right of the **Run** box.

Rebooting remote devices

You can use the remote control viewer to remotely reboot a device. You can only remotely reboot devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To remotely reboot a device

1. Click **Tools | Reboot**.
2. In the **Timeout (seconds)** edit box, enter the time that a user will have before the device is rebooted. The maximum delay is 300 seconds.
3. In the **Remote user prompt** box, type in a brief warning message that a user will see on the device before it's remotely rebooted.
4. You can save your settings by clicking **Save these settings**.
5. Click **OK**.

The warning message will appear on the device, with a countdown showing how much time remains before the reboot. The user has the option of clicking **OK** to immediately reboot, or **Cancel** to not accept the request. A message box will appear on your computer telling you if the user cancelled the request. If the reboot has taken place, you'll see a message in the session messages area of the viewer window.

Changing device remote control security

Management Suite has a high level of control over devices when granted access rights. The device controls remote access security. It stores its remote access security settings in the registry.

You can change remote control settings and security model on clients by updating the agent configuration settings (**Tools | Agent configuration**), and from the updated configuration's shortcut menu, clicking **Schedule update**. Once you deploy the update to devices, their agents will use the settings you specified.

For more information, see "Deploying remote control" on page 681.

Using remote control logging

By default, Management Suite logs remote control actions, including the device remote controlled and the console doing the remote controlling. You can disable remote control logging if you want or purge remote control log entries older than a date you specify. The remote control agent on each managed device stores log information in C:\Program Files\LANDesk\ldclient\issuser.log. The inventory scanner reads this file and stores the data in the core database.

If logging is enabled, you can view these remote control reports (**Tools | Reporting/Monitoring | Reports**), and in the **Reports** tool, click **Reports | Standard reports | Remote control**:

- Remote Control History by Client
- Remote Control History by Console
- Remote Control History for Managed Computer
- Remote Control Summary

To enable or disable remote control logging

1. Click **Configure | Remote control logging**.
2. Check or clear the **Enable remote control logging** option, depending on your preference.

To purge the remote control log

1. Click **Configure | Remote control logging**.
2. Enter the date you want purged. All entries older than this date will be deleted.
3. Click **Purge Now** to execute the purge.

If managed devices are using the "Windows NT security" remote control model, there are some additional steps you need to take to make sure that the remote control reports show the right information. With the "Windows NT security" model, both the remote control operator and managed devices must be members of the same Windows domain. You also need to make sure the domain accounts for all remote control operators are in the **Remote control operators** group in the **Remote control** agent configuration page. If you don't do this, the remote control report will show the local user as the remote control operator, rather than the actual operator.

Changing the remote control mode on target devices

The LANDesk remote control agent on devices accepts two types of connections:

- Direct connections from the LANDesk remote control viewer window.
- Management Gateway connections through a management gateway.

The remote control agent only listens for one type of connection. If you want to change the connection type the agent listens for, double-click the remote control status icon in the target device's system tray and click **Switch mode**. This toggles the agent between direct mode and gateway mode. Text in the remote control status dialog shows which mode the remote control agent is currently in. You can either have remote users toggle this for you or you can do it through a remote control session. If you do it through a remote control session, the session will disconnect once you click the **Switch mode** button.

LANDesk System Manager doesn't support the Management Gateway, so this button will always be dimmed on devices managed by System Manager.

Customizing the viewer and remote control agents

The remote control viewer has command-line options you can use to customize how it works. You can also adjust the remote control agent registry keys on devices if necessary. Normally these registry keys are set by the remote control agent configuration that you deploy to devices.

Viewer command-line options

You can launch the remote control viewer using a command-line option that immediately opens a viewer window, connects to a specific device, and activates the viewer features you want, such as remote control, chat, file transfer, or device reboot.

Remote control command-line options use the following syntax:

```
isscntr /a<address> /c<command> /l /s<core server>
```

If your core server uses certificate-based security or integrated security for remote control, you must use the /s parameter to specify the core server.

Option	Description
/a<address> >	Contact a device at a particular TCP/IP address. The TCP/IP address may include both numeric- and name-style addresses, separated by semicolons. You can also specify the hostname.
/c<command> >	<p>Start the remote control viewer and run a particular feature. (See command names below.) You can specify multiple /c arguments on one command line. For example:</p> <pre>isscntr /agamma /c"remote control" /c"file transfer"</pre> <p>You can choose from these features:</p> <p>Remote control: Open a remote control window</p> <p>Reboot: Reboot the given device</p> <p>Chat: Open a chat window</p> <p>File transfer: Open a file transfer session</p> <p>System info: Opens a window displaying information about the device, including OS, memory, and hard drive space.</p>

Option	Description
/l	Limit the viewer interface so it only displays the features you specify with /c.
/s<core server>	If you're using certificate-based security, use this option to specify the core server to authenticate with. This option is helpful if you're remote-controlling clients in a multi-core environment. If your core server uses certificate-based security or integrated security for remote control, you must use the /s parameter to specify the core server.

Example 1

Opens the viewer window. Any changes made, such as sizing the connection messages window or setting performance options are retained from the last time the viewer window was used.

```
isscntr
```

Example 2

Launches a remote control session connecting to the device named "gamma." (Note that there is no space and no punctuation between "/a" and "gamma.")

```
isscntr /agamma /c"remote control"
```

Example 3

Launches a remote control and chat session connecting to the device named "gamma". Remote control first attempts to try to resolve the name "gamma". If this fails, it attempts to connect to the numeric address 10.10.10.10:

```
isscntr /agamma:10.10.10.10 /c"remote control" /c"chat"
```

Port 9535 is used to communicate between the viewer and agent computers. If devices running `issuser.exe` are configured to use a port other than 9535, the port must be passed as part of the address given to `isscntr.exe`. For example, to remote control a device with address 10.4.11.44, where `issuser.exe` is configured to use port 1792 as the verify port, the command line would be:

```
isscntr /a10.4.11.44:1792 /c"remote control"
```

Macintosh agents still use ports 1761 and 1762 to communicate, but you can still use `isscntr.exe` in Management Suite 8.7 to remote control.

The NetWare agent uses port 1761.

Troubleshooting remote control sessions

This section describes problems you may encounter when remote controlling a device and possible solutions.

I can't remote control a device

Check that the device has the LANDesk agents loaded.

To check that the LANDesk agents are loaded:

- In the console's network view, click **Properties** from the device's shortcut menu. Click the **Agents** tab and view the loaded agents.

To load the remote control agent

- Create an agent configuration task in the console and push it to the device, or map a drive from the device to the core server and run the appropriate device configuration task.

Can't transfer files between the console and a target device

Check to see if you're running Norton AntiVirus*, and if its Integrity Shield is turned on. If the Integrity Shield is turned on, you must have temporary privileges that let you copy to the directory that the Integrity Shield is protecting.

Software distribution

This chapter explains how to use LANDesk Management Suite to distribute software and files to devices throughout your network.

Read this chapter to learn about:

- [Software distribution overview](#)
- [Understanding package types](#)
- [Understanding the available delivery methods](#)
- [Setting up the delivery server](#)
- [Configuring Windows 2003 Web servers for software distribution](#)
- [Distributing a package](#)
- [Working with distribution owners and rights](#)
- [About file downloading](#)
- [Updating package hashes](#)
- [Running packages from the source server](#)
- [Using software distribution with packages on a distributed file system \(DFS\)](#)
- [Configuring preferred package servers](#)
- [Using Targeted Multicast with software distribution](#)
- [About byte-level checkpoint restart and dynamic bandwidth throttling](#)
- [Running an application under the context of the currently logged-on user](#)
- "Using MSI distribution packages" on page 181
- [Distributing software to Linux devices](#)
- [Troubleshooting distribution failures](#)

Software distribution overview

Software distribution enables you to deploy software and file packages to devices running the following operating systems:

- Windows 95B/98SE
- Windows NT (4.0 SP6a and higher)
- Windows 2000/2003/XP/Vista
- Mac OS X 10.2.x, 10.3.x, and 10.5x
- RedHat Linux 7.3, 8.0, 9, and Enterprise Linux v3/v4/v5 (AS, ES and WS)
- Suse Linux Server 9 and 10, and Linux Professional 9.3

Devices receiving the software distribution packages must have the following LANDesk agents installed:

- Standard LANDesk agent (formerly known as CBA)
- Software distribution agent

Software distribution features include:

- LANDesk Targeted Multicasting® features that minimize bandwidth use when distributing large packages to many users—without dedicated hardware or router reconfigurations

- Delivery methods enable detailed control over how tasks complete
- Easy task scheduler integrates with the inventory database to make target selection easy
- Real-time status reporting for each deployment task
- [Policy-based distributions](#), including support for create push tasks supported by policy
- Distribution to Mac OS 9.22 and Mac OS X devices
- Mobile device support, including bandwidth detection, checkpoint restart, and the ability to complete the job using a policy
- Full-featured package builder
- Ability to distribute any package type, including MSI, setup.exe, and other installers

If you don't have an existing package that you want to deploy, you can use Management Suite's package-building technology to create a standalone executable program for the required software installation. Once you have a package, store it on a Web or network server called a "delivery server." Through the console, you can schedule distribution using the **Scheduled tasks** window. The core server communicates the package's location (URL or UNC path to the device), and the device then copies only the files or the portions of the files it needs from the delivery server.

For example, if you're reinstalling a software program because some of its files were corrupted or missing, the system copies only the damaged or missing files, not the entire program. This technology also works well over WAN links. You can store the package on multiple servers, and then schedule devices to use the server appropriate to their needs (that is, location proximity, bandwidth availability, and so on).

Software distribution will also resume interrupted package downloads. For example, if a mobile device was in the process of downloading a large package and that device disconnects from the network, once the device reconnects the download resumes right where it left off.

In Management Suite, software distribution consists of these main steps:

1. **Create or obtain a software package.** The software package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux RPM package, or a package created with Management Suite's package builder. Put the package on your delivery server.
2. **Create a distribution package (Tools | Distribution | Distribution Packages).** The distribution package contains the files and settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, command-line parameters, additional files needed to install the package, and so on. These settings are stored in the database and create a distribution package. Once you create a distribution package, the information is stored in the database and can easily be used in multiple tasks.
3. **Create a delivery method (Tools | Distribution | Delivery Methods).** The delivery method defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push and/or policy distributions. Don't create a delivery method every time you want to distribute a package. Delivery methods allow you to define best practices for deploying software. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.
4. **Schedule the distribution job in the Scheduled tasks window (Tools | Distribution | Scheduled Tasks).** Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

5. When the scheduled time occurs, the scheduler service will start the scheduled task handler which deploys the package using the options selected in the delivery method. These may include:
 - If a delivery method that uses multicast is selected, multicast is used.
 - If a push delivery method is selected, the service contacts the software distribution agent on each device and informs it that the package is ready for installation.
 - If a policy base delivery method is selected, the package becomes available for download.
6. The software distribution agent obtains the package from its local cache, a peer on the network, or the delivery server and processes it on the device by installing or removing the packaged files.
7. After the package is processed, the software distribution agent sends the result to the core server, where it's recorded in the core database.

Separating distribution tasks into two parts, distribution packages and delivery methods, simplifies the distribution process. Now you can create delivery method templates that are independent of a particular package. For example, you could create a default Targeted Multicast delivery method template, and whenever you have a package you want to multicast, you can deliver the package using that template without having to reconfigure the distribution package or the delivery method.

If you have different people in your organization that create packages and distribute packages, these changes help simplify job roles and task divisions. Package creators can now work independently from package deliverers.

Understanding package types

Software distribution supports these package types:

SWD package

These are packages built with the Management Suite Package Builder (installed separately). For more information see "[Building Packages](#)."

MSI

These are packages in the Windows Installer format. You must use a third-party tool to create MSI packages. These packages consist of a primary .MSI file and can include supporting files and transforms. Transforms customize how MSI packages are installed. If your MSI package consists of multiple files, make sure you add all of them in the **Distribution package** dialog.

Executable

In order for an executable package to be used by software distribution, it must meet the following criteria:

- The executable must not exit before the installation is complete.
- The executable must return zero (0) for a successful installation.

As long as the executable meets these two criteria, any executable can be used for installing the package. You can include additional files for executable packages.

Batch file

Batch file packages are based on a Windows/DOS batch file. You can include additional files for these distribution packages. The successful completion status of the batch file package is based on the value of the errorlevel system environment variable when the batch file has finished running.

Using batch files in tasks on Windows 95/98 devices

In Windows 95/98, when command.com launches a batch file that contains a Windows executable, the batch file will launch the executable and continue executing commands in the batch file without waiting. The core will receive a result when the batch file ends, not necessarily when the Windows executable ends. In this case, the core won't know if the Windows executable ran correctly and it will report a successful completion if the rest of the DOS commands ran successfully.

If the batch file launches a DOS executable, the batch file will then wait for the executable to finish before continuing on. For DOS executables, the core will receive a result when all processes have ended.

Macintosh

Any Macintosh file can be downloaded, though Management Suite won't download directories. Install packages (.PKG) can contain directories. They must be compressed. If the file downloaded has an extension of .SIT, .ZIP, .TAR, .GZ, .SEA, or .HGX, Management Suite will decompress the file before returning. (Users should make sure that Stuffit Expander* has its "check for new versions" option disabled; otherwise a dialog may interrupt script execution.)

Linux RPM

These are packages in Linux RPM format. These packages must be stored on a Web share for Linux RPM distribution to work.

Understanding the available delivery methods

Software distribution provides these delivery methods:

- **Push:** The packages may be multicast out to the managed devices. The core server then initiates package installation at the managed devices.
- **Policy:** The core server makes the packages available for download. When a managed device checks for available policies, the package will be returned. Depending on the policy type, devices may install the package automatically or make the package available to users for them to install when they want.
- **Policy-supported push:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it.

- **Multicast (cache only):** Multicasts the package to the target devices, no other action is taken on the managed device. The result is the package is cached locally on managed devices. Use this option to multicast the package to a few devices on each multicast domain. You can then create a task that uses the **Peer download (only install from cache or peer)** option. This allows you to regulate network bandwidth used for the distribution so it doesn't span multicast domains.

Software distribution core server components

The following components of software distribution run or reside on the core server:

- **LANDesk scheduled task handler:** This program (ScheduledTaskHandler.exe), launched by the scheduler service, starts a distribution job.
- **LANDesk scheduler service:** The console stores information about scheduled jobs in the database. The scheduler service (SCHEDSVCS.EXE) monitors the information in the database to determine when tasks should be run.
- **Distribution package:** When you select a software distribution package in the **Distribution package** window, it stores this definition in the database. This definition is used by Management Suite when creating the commands that will be sent to the devices to install the packages.
- **Software distribution packages:** A package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux package, or a package created with Management Suite's package builder. In most cases, the software package needs to contain everything necessary to install the application you're distributing.

For users of Management Suite versions prior to 8.5

Management Suite 8.5 reorganizes the way software distribution works in the Management Suite console. Software distribution is now divided into two parts:

- **Distribution packages:** Use this window to create distribution package. Once you've created a package or have an existing package you want to distribute, this window lets you configure the package for Management Suite.
- **Delivery methods:** Use this window to define how packages you've configured in the **Distribution packages** window will be delivered. For example, you can choose a Targeted Multicast distribution or a pull distribution.

If you've used versions of Management Suite prior to version 8.5, you'll also notice that application policy management is no longer on the **Tools** menu. Policy management is now part of the **Distribution packages** and **Delivery methods** dialogs. Legacy APM packages are upgraded to distribution packages, delivery methods, and scheduled tasks. Scripts remain unaltered.

Setting up the delivery server

The delivery server is the server that stores the software distribution packages. It can be either a Web server or a Windows NT/2000/2003 server. We recommend that for best results, the packages be URL-based. In general, properly configuring a URL is less work than configuring a UNC path.

HTTP package shares need to have the Internet Guest Account added with at least read privileges, since the packages will be accessed via anonymous HTTP.

UNC package shares need to have the Domain Computers group added with at least read privileges.

Delivery server	Requirements
Web server	Microsoft Internet Information Server 5.0 or higher running on Windows NT or Windows 2000/2003, or any HTTP 1.1 compliant Web server with byte range support.
Network server	Windows NT 4.0 or Windows 2000/2003

To configure a Web server for software distribution

These steps explain how to create a virtual directory on a Web server and enable it for browsing. In general, virtual directories need to allow reading and directory browsing, and anonymous access to the virtual directory must be enabled. Execute must not be set or the share won't work correctly. You also may want to disable write permissions so devices can't change the directory's contents.

1. Create a directory on the Web server where you want to store your software distribution packages. The usual location for such a directory on an IIS Web server is a subdirectory in the c:\inetpub\wwwroot directory.
2. Copy the packages to this directory.
3. From the Control Panel, double-click **Administrative Tools** and then **Internet Services Manager**.
4. In the right panel, double-click the icon with the device's name and then click **Default Web Site**.
5. In an empty area in the right panel, right-click and select **New**, then click **Virtual Directory**.
6. From the wizard, click **Next** and then enter an alias for your directory. Click **Next**.
7. Either enter the path or browse to a path and click **Next**.
8. In the Access Permissions dialog, enable **Run script** and **Browse**. This enables you to browse packages when creating a distribution package. Click **Next** and **Finish**.
9. From the shortcut menu for the virtual directory you just created, click **Properties**.
10. On the **Documents** tab, clear the **Enable default content page** option and click **OK**. Default pages can interfere with the share's ability to provide a directory that can be browsed.
11. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** box. Make sure **Integrated Windows authentication** is checked. Also make sure **Digest authentication for Windows domain servers** is cleared.
12. To enable **Port 80** on the Web server, in the left panel, right-click **Default Web Site**.
13. Click **Properties**. In the **Web Site Identification** dialog, the **TCP Port** box should display 80. If it doesn't, click **Advanced** to add the port.

14. Ensure that the Web site is available by opening a browser and entering the URL for your Web server and virtual directory. For example, if the name of your Web server is Test and the name of the virtual directory is Packages, enter the following URL:

`http://Test/Packages`

A list of the packages you have copied to this directory should appear.

The size and number of packages you put in this directory is limited only by available disk space. Subdirectories can be created to logically group packages. Each subdirectory that's created must have the access permissions set, as described in the [To configure a Web server for software distribution](#) task.

Once you copy the packages to a package share on a Web server, they're staged and ready to be copied to the target devices. When scheduled, the URL or UNC path of the package is passed to SDCLIENT.EXE (the device agent) as a command-line parameter. SDCLIENT.EXE manages the file transfer, starts the installation, and reports the status. Although the HTTP protocol is used for the file transfer, the status report is returned through the standard LANDesk agent.

The Web server communicates with the device to ensure that the package copies correctly. If the package transmission is interrupted during the download, the Web server can use the HTTP protocol to restart the download at the point where it stopped. The Web server doesn't check, however, to ensure that the package was installed correctly. That traffic is TCP-based, and it returns the status to the core server using the standard LANDesk agent.

Configuring a file server for software distribution

Devices that don't have a browser must receive distribution packages from a UNC path on a Windows NT/2000/2003 network server. This can be the same folder as the one you set up on your Web server. If you're using [preferred servers](#), you can configure authentication credentials for your UNC package share there, without having to configure a null-session share.

If you aren't using preferred servers or preferred server credentials, you'll need to make your package share null-session, which allows users to access the share without having to provide alternate credentials. Use the SYSSHRS.EXE utility to create a null-session share folder.

To configure a network server for software distribution

1. To set up a shared folder on your network server, right-click the folder you want to share and then click **Sharing**.
2. Click **Share this folder** and click **Permissions**.
3. Add the **Everyone** and the **Guest** groups, but grant them only read permissions. In a domain environment, also add the **Domain Computers** group and grant only read permissions. Apply the changes.
4. From your network server, click **Start | Run** and browse to the LDMAIN\Utilities folder on your core server.
5. Run the **SYSSHRS.EXE** utility. Although this utility states that it's for Windows NT devices, it also works on Windows 2000/2003 devices.
6. Check the shared folder you set up and click **Apply** and then **Close**.
7. Copy the software distribution packages to this folder on the network server.

The size and number of packages you store on the network server is limited only by the available disk space.

For more information about the SYSSHRS.EXE utility, download the SHARES.EXE package from <http://www.landesk.com/support/downloads/Resource.aspx?pvid=12&rtid=10> and extract the documentation.

Using null-session shares with Windows Server 2003

In addition to the steps included in online help, configuring a null-session share on a Windows Server 2003 server requires the following policy changes (you can launch the Group Policy Object Editor by entering gpedit.msc at the Windows Run prompt):

- **Let permissions apply to anonymous users** must be enabled for the Everyone and Guest groups.
- **Restrict anonymous access to Named Pipes and Shares** must be disabled.
- **Shares that can be accessed anonymously** must include the name of the null session share.

Windows Server 2003 cannot be used for a network null-session share if asp.net is installed. If you set up a null-session share on a Windows 2003 server on which asp.net is installed, when you attempt to create a distribution package, the core will try to authenticate using the asp.net user credentials and will fail.

Configuring IIS 6 Web servers for software distribution

Windows 2003 uses IIS 6 as its Web server. When hosting packages on an IIS 6 Web server, there is some additional configuration you need to do:

- Configure the virtual directory that hosts your packages.
- Register a MIME type with IIS.

IIS 6 handles virtual directories differently than IIS 5 (IIS 5 was the Windows 2000 Web server). On an IIS 6 server, if you select a directory and from its shortcut menu make it a Web share, the directory registers itself in IIS 6 as a Web application rather than a virtual directory. The problem is that as a Web application, when trying to select an executable file, the Web server attempts to run the file as a Web application rather than download the file to the user.

The resolution is to go into IIS, change the shared directory from a Web application to a virtual directory, and turn off execute permissions.

When hosting files on an IIS 6 server, files without a registered MIME file type will result in an HTTP error 404, File Not Found. This will result in the multicast and/or installation of the file failing unless you register MIME file types.

To register MIME file types

1. Launch Internet Information Services (IIS) Manager.
2. Expand the local computer in the tree.

3. Click **Web Sites | Default Web Site**.
4. From the package Web share's shortcut menu, click **Properties**.
5. Click the **HTTP Headers** tab.
6. Click **MIME Types**.
7. Click **New**.
8. In the **Extension** box, enter an asterisk (*).
9. In the **MIME Type** box, enter any name.
10. Click **OK** twice and apply the changes.

Distributing a package

A distribution package consists of the package file you want to distribute, any additional files needed by the package, and settings that describe the package components and behavior. You must create the package before you can create the distribution package definition for it.

These instructions explain how to create a software distribution package. For the package to execute correctly, the software distribution package must exist on either a network or Web server and the devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices.

1. Create a distribution package for the package you want to distribute.
2. Create a delivery method.
3. Schedule the package and delivery method for distribution.

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools | Distribution | Distribution Packages**.
3. From the shortcut menu of the package group you want, click **New distribution package |** the package type you want to create.
4. In the **Distribution package** dialog, enter the package information and change the options you want. Note that you must enter the package name, description, and primary file. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the package type and owner you selected.

To create a delivery method

1. If you've already configured a delivery method that you want to use, or you are using one of the default delivery methods, skip to the next procedure, "To schedule a distribution task."
2. Click **Tools | Distribution | Delivery Methods**.
3. From the shortcut menu of the delivery method you want to use, click **New delivery method**.
4. In the **Delivery Method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method and owner you selected.

To schedule a distribution task

1. Click **Tools | Distribution | Scheduled tasks**.
2. Click the **Create software distribution** task toolbar button.
3. On the **Distribution package** page, select the distribution package you created.
4. On the **Delivery Methods** page, select the delivery method you want to use.
5. Click **Save** to save your changes.
6. From the network view, drag targets onto the task in the **Scheduled tasks** window. Targets can include individual devices, computer groups, LDAP objects (user, machine, and group), LDAP queries, and inventory queries.
7. From the task's shortcut menu, click **Properties**.
8. The **Target devices** page shows the devices that will receive this task.
9. On the **Schedule task** page, enter the task name and the task schedule.
10. Return to the **Overview** page and confirm the task is configured how you want it to be.
11. Click **Save** when you're done.

View the task progress in the **Scheduled tasks** window.

Working with distribution owners and rights

In environments where there are many Management Suite users, it can get confusing knowing which distribution packages, delivery methods, and scheduled tasks each user is responsible for. To help with this problem, Management Suite makes the user that created the distribution package, delivery method, or scheduled task the default owner of that item. Only the owner and RBA Administrators/Software distribution configuration users can see these private items.

Private items appear under the **My delivery methods**, **My packages**, or **My tasks** trees. Administrative users can see items for all users under the **User distribution packages**, **User delivery methods**, and **User tasks** trees.

When users create a distribution item, the **Description** page has a **Package owner** option. Users can select **Public** if they want all console users to see that item. Administrators can select a specific user in addition to **Public**.

Once a user has created an item, they can change the owner by clicking **Properties** on the item's shortcut menu. Once a non-administrative user sets an item to public, they can't make the item private again. Only an administrator can do that.

These RBA rights affect distribution item visibility:

- **Administrator:** Create and view public and private distribution items. Can view private distribution items for all users.
- **Software distribution configuration:** Create and view public and private distribution items. Can only see their private distribution items.
- **Software distribution:** View and use existing public distribution items and items owned by themselves. Can't create new distribution items.

Using multiple distribution packages in a task

Push-based software distribution tasks can include a preliminary package and a final package. When using multiple packages, the packages are installed in order one at a time. The previous package must return a successful task status on all targeted devices before the next package begins installing.

Preliminary and final packages are useful in cases where you want to run commands before and/or after the main package. For example, you could create a batch file package that executes commands to configure the target device for the main package. After the main package finishes installing, you could specify a final batch file package that does any post-configuration. Any package type can be a preliminary or final package, but the delivery method must be push. The policy-supported push delivery method doesn't support preliminary and final packages.

You can specify preliminary and final packages when you schedule a distribution task. The **Scheduled task - properties** dialog's **Distribution package** page has the **Preliminary package** and **Final package** options. Before you can click one of these options, you must go to the **Delivery method** page and select a push delivery method. To do this, click **Push** for the **Delivery type** and click the **Delivery method** that you want to use.

To use multiple distribution packages in a task

1. Create the packages you want to use in the task.
2. Click **Tools | Distribution | Scheduled tasks**. Click the **Create software distribution task** toolbar button.
3. On the **Delivery method** tab, click **Push** as the **Delivery type** and click the **Delivery method** that you want to use.
4. On the **Distribution package** tab, click the **Package type** and **Distribution package** that you want to use.
5. Click **Preliminary package**, **Main package**, or **Final package**, depending on when you want that package installed, and click **Set**.
6. Repeat steps 4 and 5 for any other packages you want installed for this task. You can only have one package in each stage and you must always have a **Main package**.
7. Finish configuring the task and schedule it.

About file downloading

Software distribution has several methods for getting the file down to the device for installation. These include:

- Obtaining the file from the multicast cache
- Obtaining the file from a peer
- Downloading directly from the remote source

When a file needs to be downloaded, the device software distribution agent, SDClient, first checks the cache to determine if the file is located in the cache. The cache is defined as either C:\Program Files\LANDesk\LDClient\sdmcache or the path stored in the "Cache Directory" under the multicast registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM\Distribution\Multicast

The structure of files in the cache will be identical to the structure of the files on the Web or network server. This allows multiple packages to have files with the same name and not cause problems.

If the file isn't in the cache, SDClient will typically attempt to download the file from a peer in the network. You can configure the delivery method to require a peer download.

If the file can't be obtained from a peer, SDClient will download the files directly from the UNC or URL source. You can configure the delivery method so that if the file is to be obtained from the source, only one device in the multicast domain will download the file from the source location. Under most circumstances when downloading from a UNC share, this requires the UNC share to be a NULL session share. If the file to be downloaded is URL-based, SDClient will download the file from the Web site.

In either case, SDClient will put the file in the multicast cache. After it is put in the multicast cache, SDClient processes the downloaded file.

When a file is downloaded into the cache it will remain in the cache for several days, but is eventually deleted from the cache. The amount of time that the file will remain in the cache is controlled by the delivery method used when deploying the package.

Updating package hashes

Because many package files are obtained from peers in the network, the files are verified prior to installation. The integrity of the files are verified by comparing the MD5 hash of the file to the MD5 hash generated at the core server.

When a distribution package is first scheduled, Management Suite downloads the files and calculates the hash values associated with the primary file and any additional files used by the distribution package. If the hash stored with the package doesn't match the hash value SDClient computed on the target device, the download isn't considered valid.

If you make any changes to the package outside of Management Suite, such as updating the package contents, you need to reset the hash, or any scheduled tasks using the updated package will fail.

To reset a package hash

1. Click **Tools | Distribution | Distribution packages**.
2. From the shortcut menu for the package whose hash you want to update, click **Reset file hashes**. This can take a few minutes on large packages.

Running packages from the source server

Software distribution normally downloads package files to the local device's cache and then installs the package from the cache. This may not work well if a package or application expects installation files to be in a specific folder structure, such as with the Microsoft Office installer, or if the application installation doesn't use all source files for every installation.

For cases like these, you can instead have the local software distribution agent run the file directly from the source, whether that's a preferred server or the source specified in the package. When you enable run from source, software distribution won't download package files to the local cache, nor will it run the package from a peer.

When using run from source with packages stored on Web shares, the primary file must be an MSI file or SWD package. With UNC shares, the primary file can be any file type.

To create a delivery method that uses run from source

1. Click **Tools | Delivery methods | Network usage**.
2. Click **Use run from source to deploy files**.
3. Finish configuring the delivery method.

Using software distribution with packages on a distributed file system (DFS)

Distributed file systems (DFS) use several servers to provide files that are available from a single file share. Software distribution's default method of bandwidth detection in a DFS scenario ends up using the root server to calculate bandwidth, which may not be the actual server that provides the file. Software distribution now provides an optional way of calculating bandwidth. With this new method, bandwidth detection retrieves a small portion of the actual file being distributed. This way, software distribution calculates bandwidth from the server providing the file.

This alternate bandwidth detection method isn't enabled by default. You can enable this option from the `ntstacfg.in#` file in the core server's `ldlogon` folder. Once you update this file, the changes become part of new or updated agent configurations. You must redeploy your agent configuration to devices for the change to take effect.

Look for this section in `ntstacfg.in#` and make the necessary changes.

```
; The following registry values control detecting bandwidth by file
download
; change the UseDownloadForBandwidth value to 1 to enable use of file
download for bandwidth detection
; the DownloadSize value should be entered as a Hex value between 400 and
FFFF(1024 bytes to 65535 bytes).
REG1=HKEY_LOCAL_MACHINE,
SOFTWARE\LANdesk\ManagementSuite\WinClient\SoftwareDistribution\UseDownloa
dForBandwidth, 0, , REG_DWORD
REG2=HKEY_LOCAL_MACHINE,
SOFTWARE\LANdesk\ManagementSuite\WinClient\SoftwareDistribution\Downloa
dSize, 2000, , REG_DWORD
```

Configuring preferred package servers

You can specify the default server that devices will check for software distribution packages. This can be important in low-speed WAN environments where you don't want devices downloading packages from off-site servers. When you specify preferred servers, you can also specify the credentials managed devices should use to authenticate with each preferred server. You can also specify the IP address ranges that preferred server will be available to.

When using preferred servers with a distribution job, only the server portion of the UNC or URL file/package path is replaced; the rest of the path must be the same as what was specified in the distribution task. If the file isn't on the preferred server, it will be downloaded from the location specified in the distribution package. The only distribution method that doesn't support preferred servers is Multicast (cache only).

The core server also uses preferred servers. The core server uses distribution package hashes to verify distribution packages in scheduled tasks. The core server will first try to generate these hashes from a preferred server. Using a local preferred server makes the hashing process much quicker. If the package isn't available on one of the preferred servers, the core server falls back to generating the package hash from the path specified in the distribution package. You generally won't want the core server pulling a large package over the WAN link for hashing, so hashing files on a server that's local to the core will be much faster and use less low-speed bandwidth.

Managed devices store the preferred server list locally in the `preferredserver.dat` file. To create this file, a device communicates with the core server and then makes a filtered list of preferred servers (based on IP address range limits, if any). The device then does a bandwidth check to each preferred server and saves the top three servers in the `preferredserver.dat` file. Note that the bandwidth check doesn't produce guaranteed reliable results. For example, a server that's close by may have a high load at the time the agent checks, so it may get bumped off even if normally it's the best candidate.

The distribution agent updates the `preferredserver.dat` file every 24 hours or when the IP address changes. Not every device has to go through this process. Devices share their preferred server lists with peers. This is the process managed devices go through to maintain a current preferred server list:

1. If `preferredserver.dat` is in the local file cache, the distribution agent uses it.
2. If `preferredserver.dat` is on a peer, the agent retrieves the file from that peer.
3. If `preferredserver.dat` isn't available locally or on a peer, the device contacts the core server, creates a filtered preferred server list, and saves that locally as `preferredserver.dat`.
4. If `preferredserver.dat` is empty or if none of the preferred servers respond, the agent checks for a preferred server list in the local registry.

If none of these steps results in an available preferred server, the local agent uses the distribution path specified in the distribution job.

To configure preferred package servers

1. Click **Configure | Preferred server**.
2. Click **Add** to add a new server, or click an existing entry and click **Edit**.
3. Enter the server information. If you want to use IP address ranges that you want this server to be available to, enter them and click **Add**.
4. Click **Test credentials** to make sure the credentials you provided work.
5. Click **OK**.

Storing preferred package servers in the registry

The easiest way to manage preferred servers is with the **Server credentials** dialog (**Configure | Preferred server**). If you want to configure a fallback list of preferred servers that will be used if there are no servers in the preferredserver.dat file, you can create the following registry key on managed devices, and set the value to the preferred package server name. You can specify multiple package servers by separating them with semicolons.

- HKEY_LOCAL_MACHINE\Software\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\PreferredPackageServer

Here's a sample registry entry:

- [HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution]\PreferredPackageServer ="Server1;Server2;Server3"

Customizing the number of servers stored in preferredserver.dat

By default, the preferredserver.dat file contains three servers whose test results gave the highest bandwidth at the time of the bandwidth check, in order. You can change the number of servers stored in preferredserver.dat by updating this line in the ntstacfg.in# file in the core server's Idlogon folder. Valid numbers range from 0 to 7. Once you update this file, the changes become part of new or updated agent configurations. You must redeploy your agent configuration to devices for the change to take effect.

```
; Settings for the lddwnld/ldredirect files, the DynamicPreferredServers
is the
; maximum number of preferred servers that will be stored. Set this to 0
to disable
; the dynamic preferred server functionality.
REG51=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DynamicPre
ferredServers, 3, , REG_DWORD
```

Customizing preferred server prioritization

In order to prevent delays when the most preferred servers do not have a package, the redirection logic will start to prefer servers that have been actually providing files to the device. You can change the preferred server prioritization in preferredserver.dat by updating these lines in the ntstacfg.in# file in the core server's Idlogon folder:


```

; In order to prevent delays when the most preferred servers do not have a
package
; the redirection logic will start to prefer servers that have been
actually
; providing files to the client. The following registry options control
when a
; server is moved up the list. The ServerHistoryUseCount value indicates
the number
; of times a server must be used before it will be moved to the start of
the list,
; the ServerHistoryCacheTime value indicates how long it should be
remembered (in seconds).
REG52=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHist
oryUseCount, 3, , REG_DWORD
REG53=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHist
oryCacheTime, 3600, , REG_DWORD

```

Understanding UNC authentication

When you add preferred servers (**Configure | Preferred server**), you also provide credentials that devices should use when accessing the preferred server. For security reasons, make sure these credentials provide read-only access. Devices obtain these credentials from the core and use them to authenticate with that preferred server. When using preferred servers added to the **Server Credentials** dialog, you no longer have to configure your package shares to be null-session shares, as was necessary with previous versions. As long as the credentials you provide for the preferred server work with the package share (Click **Test credentials** in the **User name and password** dialog), managed devices should be able to access the share.

About byte-level checkpoint restart and dynamic bandwidth throttling

Management Suite 8 and later versions support distribution byte-level checkpoint restart and dynamic bandwidth throttling. Checkpoint restart works with distribution jobs that SWD first copies to the device cache folder (by default, C:\Program Files\LANDesk\LDClient\SDMCACHE). When a bandwidth controlling option is selected, the files get copied to the device cache first, and checkpoint restart allows interrupted distributions to resume at the point where they left off.

Dynamic bandwidth throttling specifies that the network traffic a device creates has priority over distribution traffic. This option also forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you select this option and leave the **Minimum available bandwidth** percentage at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. Increasing the minimum available bandwidth preserves approximately the amount of device bandwidth you specify for distribution if the distribution needs network bandwidth and there is contention for bandwidth on the device.

If you're reinstalling or repairing an SWD package or an MSI package, you may not want to use the dynamic bandwidth throttling option, because these package types normally only download the files they need. Using dynamic bandwidth throttling in this case would force a full download of the package when a repair might normally only require a small portion of the package.

Dynamic bandwidth throttling isn't available on Windows 95, Macintosh, or DOS devices. Windows 98 and Windows NT devices can use dynamic bandwidth throttling if they have Internet Explorer version 4 or later installed.

You can configure collective bandwidth throttling so that only one device from the multicast domain will download from the remote source. You can also configure the amount of bandwidth used when downloading from the source. This feature is available on all versions of Windows systems. Collective bandwidth throttling isn't available on Macintosh or DOS systems.

Using Targeted Multicast with software distribution

LANDesk Targeted Multicast technology makes it possible to distribute large packages to many users across the network with a minimum of network traffic. Targeted Multicast features require no additional hardware or software infrastructure, and require no router configurations to allow multicast packets. You get the extraordinary benefits of multicast technology with none of its traditional headaches.

Targeted Multicast is designed to work with your existing software distribution packages. When you use Targeted Multicast, you can easily distribute software, even in WAN environments with multiple hops and low connection speeds (56k). Targeted Multicast uses HTTP for delivery from a Web site to a subnet representative. Management Suite's inventory scanner provides all the subnet information to the Targeted Multicast service.

Targeted Multicast provides unique benefits that standard methods of "multicast" don't provide. Inventory-based targeting of devices enables you to send a package to a selected group of computers that fit specific criteria via a multicast. Targeted Multicast is also simplified because there's no need to configure routers to handle deliveries.

When compared to conventional software distribution methods, Targeted Multicast significantly reduces the time and bandwidth needed to deliver software packages. Instead of sending a package across the wire for each device, only one transfer is made for each subnet. Bandwidth savings increase as the number of devices on each subnet increases.

You can activate Targeted Multicast from the delivery method properties by checking the **Use Multicast to deploy files** option on the **Multicast** page of the **Delivery methods** properties. Multicast is available in policy supported push, push, and multicast (cache only) delivery methods. Underneath the **Multicast** page you will find several pages that allow the multicast to be configured.

When you start a distribution using Targeted Multicast, you'll see the **Multicast software distribution** window. This window contains detailed information about how the distribution is proceeding. For more information about what each field means, click the **Help** button on the **Multicast software distribution** window.

Both Windows and Macintosh OS 10.2 devices support Targeted Multicast. Additionally, you can multicast OS deployment images.

Using peer download

Peer download is a Targeted Multicast option that forces targeted devices to install a package from the devices' local cache or from a peer on the same subnet. This option conserves network bandwidth, but for the package installation to be successful, the package must be in the local cache or a peer's cache.

If you don't select the **Peer Download** option, the Targeted Multicast device agent will still attempt to conserve bandwidth by checking the following locations for package files in this order:

1. Local cache
2. Peer on the same subnet
3. Package server

Copying files to the local multicast cache folder

You have the option of copying one or more files to the local multicast cache folder using multicast. This option copies a file to the target devices' local cache. It doesn't install the file or do anything else with it. This option is useful for getting files to multicast domain representatives or a device in each multicast domain. You can do an initial deployment to domain representatives and then redo the deployment with the peer download option to ensure devices only download the package from a peer on their subnet.

Configuring Targeted Multicast

Before using Targeted Multicast, you need to make sure the Targeted Multicast components are in place on the subnet you're distributing to. Targeted Multicast requires Management Suite 8 agents and a multicast domain representative.

To manually specify which computers will be multicast domain representatives

1. In the network view, click **Configuration | Multicast Domain Representatives**.
2. Add domain representatives by dragging the computers you want to be representatives from the network view into this category.

Targeted Multicast will use the first computer that responds per subnet in the **Multicast domain representatives** group.

Only Windows computers can be multicast domain representatives. If you are using multicast to distribute packages to Macintosh computers, make sure there is at least one Windows computer in the multicast domain that can act as a domain representative for the Macintosh computers. If you only have a few Windows computers in a predominantly Macintosh environment, it's best to manually specify Windows domain representatives in the Multicast Domain Representatives group.

You can throttle multicasts by changing the **Minimum number of milliseconds between packet transmissions** option in the **Packet timing** page under the **Multicast** page on the **Policy-supported Push, Push, and Multicast** delivery method windows.

You can also customize Targeted Multicast options in the Configure Management Suite Services dialog. To configure the Targeted Multicast service, click **Configure | Services | Multicast** tab. Click **Help** on that tab for more information.

Running an application under the context of the currently logged-on user

LANDesk Management Suite performs most application installations and other tasks using full system privileges. Some application installations and other tasks need to be performed as the system's current user. As part of the release of LANDesk Management Suite 8.7 SP2, a new utility, the STARTASUSER.EXE application, is available that makes it possible to run an application under the context of the currently logged-on user.

STARTASUSER.EXE will launch the supplied command line in the context of the user currently logged onto the system. STARTASUSER.EXE supports the following command line format:

```
startasuser.exe [///silent] [///timeout=x] [///?] command line...
```

If no user is logged onto the system when STARTASUSER.EXE launches, the application returns the standard Windows ERROR_NOT_LOGGED_ON (1245) error.

All of the command-line options for the STARTASUSER.EXE application are preceded with three forward slashes (///); this is done to prevent confusion with command line options of the launched application.

The command line options are outlined in more detail below.

///silent

This option results in the created process being started as hidden, this should prevent any windows of the application displaying.

///timeout=x

This option controls the timeout (in seconds) for the launched application. If the launched application has not completed before the specified timeout has occurred, the startasuser.exe application will exit with the standard windows error WAIT_TIMEOUT (258).

///?

This option causes command line usage to be displayed to stdout. Because STARTASUSER.EXE is a windows application, the help will not display in the command prompt by default. Use the following command line to display help from within a command prompt:

```
startasuser.exe ///? | more
```

command line...

After any STARTASUSER.EXE options, specify the full command line for the application to be run.

The following two examples show how to use the STARTASUSER.EXE application to launch an executable or install an MSI.

To run an executable (in this case, regedit) as the currently logged-on user

1. Create a batch file with the following command line:
startasuser.exe ///timeout=300 regedit.exe
2. Save the batch file on a file server set up for use with software distribution.
3. In the LANDesk Management Suite console, click **Tools | Distribution | Distribution packages**.
4. From the **My distribution packages** group shortcut menu, click **New distribution package | New batch file package**.
5. Add the batch file saved in step two as the main distribution package.
6. Save the distribution package.

This package can now be used in a software distribution task and will result in the regedit application being launched in the context of the user currently logged on.

To install an MSI package as the currently logged-on user:

1. Create a batch file with the following command line:
startasuser.exe msiexec.exe /I <name>.msi
2. When creating the batch file replace <name> with the name of the MSI package to be launched. Add additional MSI command-line options if needed.
3. Save the batch file on a file server set up for use with software distribution.
4. On the same file server, preferably at the same location, add the MSI package and any additional files.
5. In the LANDesk Management Suite console, click **Tools | Distribution | Distribution packages**.
6. From the **My distribution packages** group shortcut menu, click **New distribution package | New batch file package**.
7. Add the batch file saved in step two as the main distribution package.
8. Save the distribution package.

This package can now be used in a software distribution task and will install the MSI package using the currently logged on user.

Using MSI distribution packages

Management Suite supports MSI installation with full status reporting and MSI package recognition. The MSI distribution package type is Management Suite's preferred method of software distribution. Understanding the MSI parameters will help you set up MSI packages and delivery methods.

Using MSI command-line parameters with software distribution

When installing an MSI distribution package, Management Suite leverages the MSI API calls. MSI installations use two different types of command-line parameters:

- Option parameters
- Property reference parameters

Msiexec-specific switches can't be used as part of software distribution when using an MSI distribution package.

Option parameters

Option parameters are the switches that are used by the Microsoft installation tool, Msiexec.exe. For example, the /q switch, is a common switch for Msiexec that silences an unattended installation.

In the **Distribution package-properties** dialog, MSI option parameters shouldn't be entered in the **Install/Uninstall options** page's **Command line** box. Instead, Management Suite handles these parameters with settings in the MSI distribution package or in the delivery method. More information on Msiexec options can be found at: <http://support.microsoft.com/?kbid=227091>.

Property reference parameters

Property references, also known as public properties, are specific to the MSI file. The parameters are passed to the MSI installation APIs directly. They can be used in the **Command line** field of an MSI distribution package's **Install/Uninstall options**.

The syntax of property references is PROPERTY=VALUE. A common property reference is the Transforms property. This is the property that calls up a .mst (transform) file. More information on property reference parameters can be found at: <http://support.microsoft.com/?kbid=230781>.

The information on an application's public properties can be obtained from the software installation documentation, the application's official web site, or by contacting the software vendor directly.

Running an MSI silently

In Management Suite, running an MSI silently is automatically handled under the **Feedback and timing** section of a delivery method. To run an MSI silently, go to the **Feedback and timing** page for the desired delivery method and click **Hide all feedback from user**.

Automating an MSI installation

For many MSI's, silencing the MSI also automates the installation. In such cases, all you need to do to automate an MSI installation is select **Hide all feedback from user** in the delivery method.

Sometimes a property reference is required for the installation to complete. In such cases the MSI installer will prompt for a value. During an automated installation, no such prompt will occur. The MSI installation will fail with the standard MSI error 1603, Fatal error during install. Required public properties should be assigned a value in the distribution package's **Command line** field.

Using a transform file with an MSI installation

Answer files for MSI's are called transform files and end with a .mst extension. Not all MSI installations need a transform file; however, a transform file can be used if there are too many property references that need their values changed or assigned. If supported by the application, an answer file may be created to pass in all property reference parameters.

If a transform file is required but not provided during the installation, error 1603, Fatal error during install, will be the result. Often the software vendor will have the information needed or a tool to create a transform file for their specific MSI. For example, to deploy the volume license version of Microsoft Office 2003, a transform file should be used. Microsoft has a tool called the Custom Installation Wizard that installs as part of the Office 2003 Resource Kit. The Office 2003 Resource Kit can be downloaded from the following web site:

- <http://download.microsoft.com/download/0/e/d/0eda9ae6-f5c9-44be-98c7-ccc3016a296a/ork.exe>

If the vendor doesn't have the needed information or such a tool, Microsoft provides a tool called Orca that can create a transform file. For additional assistance, refer to the Orca help file.

Handling reboots with an MSI installation

Management Suite handles MSI reboots using the **Reboot** page in the delivery method properties. LANDesk will automatically pass both the REBOOT=REALLYSUPPRESS and the /NORESTART parameters when **Never reboot** is selected in the delivery method.

The **Always reboot** option passes the /FORCESTART parameter.

Reboot only if needed allows the MSI to handle the reboot. If feedback is enabled, the user can be prompted as to whether to reboot. It is important to know that MSIs support custom actions. If a custom action initiates a reboot, Management Suite can't prevent this.

MSI checklist

If a deployment involves an MSI, follow this checklist.

- I have the correct version of the installation files, including the MSI and all additional files, for a volume license deployment.
- I have the information from the software vendor on how to automate and silence the software installation and configuration, and how to handle reboots.
- I know what public property parameters I need to pass to the MSI.
- I know whether this MSI needs a transform file to install and if so I have created one.

Distributing software to Linux devices

Once you've deployed the Linux agents, you can distribute software to your Linux devices. The initial Linux agent deployment uses an SSH connection. Once the agents are installed, the core server uses the standard LANDesk agent to communicate with the Linux server and transfer files. To distribute software to a Linux device, you must have Administrator rights.

You can only distribute RPMs to Linux devices. The Linux agents will automatically install the RPM you distribute. The RPM itself isn't stored on the server after installation. You can install and uninstall the RPM you specify using software distribution. You can only use push delivery methods with Linux software distribution. For Linux software distribution, the settings in the push delivery method are ignored, so it doesn't matter which push delivery method you select or what the settings in it are.

The distribution follows this process:

1. The core server connects to the Linux device through the Standard LANDesk agent
2. The device downloads the package
3. The device runs a shell script that uses RPM commands to install the RPM package
4. The device sends status back to the core server.

You can store Linux RPMs on HTTP shares. Linux software distribution doesn't support UNC file shares. For HTTP shares, make sure you've enabled directory browsing for that share. If you use an HTTP share on a Windows device other than the core, you need to configure IIS with the correct MIME type for RPM files. Otherwise, the default MIME type IIS uses will cause the RPM to fail to download the file.

To configure the RPM MIME type on Windows devices

1. From Windows **Control Panel**, open **Internet Services Manager**.
2. Navigate to the folder that hosts your distribution files. From that folder's shortcut menu, click **Properties**.
3. On the **HTTP Headers** tab, click the **File Types** button.
4. Click **New Type**.
5. For the **Associated Extension**, type **rpm**. Note that rpm is lowercase.
6. For the **Content type**, type **text/plain**.
7. Click **OK** to exit the dialogs.

Once you've hosted the files on your package share, create a new Linux distribution package in the **Distribution packages** window, associate it with the delivery method you want, and schedule the delivery.

Understanding Linux software dependencies

When you click **Save** in a Linux package's **Distribution package-properties** dialog, software distribution parses the primary RPM and any dependent RPMs you selected for dependencies those RPMs require. These dependencies then appear in the **Missing libraries** dialog. Checking a dependency in this dialog tells software distribution to not prompt you about it again. You can check dependencies you know are installed on managed devices. This dialog is for your information only. If a dependency is missing on a target device and you didn't specifically include that dependency as a dependent package, the RPM probably won't install successfully.

Troubleshooting distribution failures

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, let the software sit for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll outs occur should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Scheduled task can't find package

If the scheduled task indicates that the package can't be located, make sure that the package can be viewed from the device.

If the package is URL-based, you can check to make sure it is accessible by using a Web browser. Remember, if your DNS is set up to resolve the package, you'll need to verify that the package has been distributed to all of the Web servers.

If the package can be viewed from the device but still does not download properly, the problem may be that the URL or UNC based package share doesn't allow anonymous access. Check the permissions on the UNC or URL share and make sure it allows anonymous access. For UNC locations, make sure it has properly been configured as a null session share.

Bandwidth detection doesn't work

One of the most common problems that can occur is having PDS set up for bandwidth detection. In device setup, one of the common base agent options is to choose between PDS and ICMP for device bandwidth detection. When a device is configured to use PDS for bandwidth detection, it will only detect between RAS and non-RAS connections. So, if you configure a distribution to only work with high speed connection and the package installs on a computer with a WAN connection, check and make sure it is configured to use ICMP and not PDS.

Policy-based management

LANDesk Management Suite enables you to manage sets of applications on groups of devices using policy-based management feature.

Read this chapter to learn about:

- "About policy-based management" on page 186
- "Configuring policies" on page 187
- "Applying scope to application policies" on page 190
- "What users see on their devices" on page 190
- "Using the local software deployment portal" on page 190

About policy-based management

Policy-based management (known as application policy management in earlier Management Suite releases) helps you easily manage sets of applications on groups of devices. Like any other scheduled task, policies require:

- An SWD package, MSI, executable, batch file, or Macintosh package that you create.
- A delivery method that supports policies, either policy or policy-supported push.
- Policy targets for the distribution packages, such as the results of an LDAP or core database query.
- A scheduled time at which the policy should be made available.

Policy-based management periodically reruns queries you have configured as part of the policy, applying your policies to any new managed devices. For example, perhaps you have a Department container in your LDAP directory that contains user objects. Any user whose Department object is "Marketing" uses a standard set of applications. After you set up a policy for Marketing users, new users who are added to Marketing automatically get the correct set of applications installed onto their computer.

Use the LANDesk Management Suite console to configure application policies, which are stored in the core database.

Policy-based management can deploy these file types:

- SWD packages
- Microsoft Installer (MSI packages)
- Single-file standalone executables

- Bat files
- Macintosh packages

Here's the task flow for policy-based management:

1. Make sure the software distribution agents are on your devices.
2. If you don't have a package for the application you want a policy for, create one. For more information, see "Software distribution" on page 162.
3. Use the distribution packages window create a package definition for the package.
4. Create or select an existing policy-based delivery method.
5. Create a software distribution task in the **Scheduled tasks** window and select the package and delivery method from above.
6. Select the targets for the policy, this can include any combination of individual devices, database queries, device groups, LDAP items, and LDAP queries.
7. Schedule the task to run. When run, the distribution package will be made available for pull.
8. The policy-based management service on the core server periodically updates the policy target list by reevaluating the LDAP/database query results. This helps ensure that the core database has a current set of targeted users/computers.
9. A user logs on to a device, connects to the network, or otherwise starts the policy-based management agent.
10. The core server's policy-based management service determines the applicable policies based on the device's device ID and the logged-in user or LDAP device location.
11. The policy-based management service sends the policy information back to the policy-based management agent.
12. Depending on how you've configured the device to handle policies, the user selects the policies to run or the policies run automatically. Only recommended or optional policies are available in the list on the device. When an unprocessed recommended policy is in the list, it's checked by default. Periodic policies appear in the list once their execution intervals have lapsed. Selected policies execute sequentially.
13. The policy-based management agent sends the policy results to the core server, which stores the results in the core database. Policy-based management status is reported to the core server using HTTP for enhanced reliability. This status is reported in the Scheduled tasks window.

Configuring policies

Policy-based management an SWD package, MSI, executable, batch file, or Macintosh package for any policy you create. You can either create the packages ahead of time or you can create the packages while creating the policy. We recommend that you create the packages ahead of time to test them and ensure that they work before using them in a policy.

Normal distributions and policies can use the same distribution package. The difference is in the deployment, not the package creation. There are two delivery methods that support policy based distribution:

- **Policy delivery methods:** The policy-only distribution model. Only devices meeting the policy criteria receive the package.

- **Policy-supported push delivery methods:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it.

The main difference between standard delivery methods and the policy-based delivery method is the policy-based **Delivery methods** dialog has a **Job type and frequency** page.

The job type and frequency options affect how target devices act when they receive the policy:

- **Required:** The policy-based management agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.
- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.
- **As desired:** Can be installed by users at any time.

To create a policy-based distribution

1. In the console, click **Tools | Distribution | Delivery methods**.
2. From the shortcut menu for either **Policy-based distribution** or **Policy-supported push distribution**, click **New delivery method**.
3. Configure the delivery method options you want. Click **Help** for more information on each page.
4. Set the **Job type and frequency** options you want.
5. Click **OK** when you're done.
6. Click **Tools | Distribution | Scheduled tasks**.
7. Click the **Create software distribution task** toolbar button.
8. Configure the task options you want and click **OK**.
9. With the policy-based distribution task selected, drag the policy targets to the right window pane.

Policy-based distributions take effect as soon as the policy task is started and there are targets resolved. Policy-supported push distributions take effect after the initial push-based distribution completes. [Adding static targets](#)

Policy-based management can use static targets as policy targets. Static targets are a list of specific devices or users that doesn't change unless you manually change it. Add static targets by selecting individual devices from the network view as targets. Individual LDAP devices can't be added as static targets.

Adding dynamic targets

Policy-based management can use queries to determine policy targets. As of Management Suite 8, queries are stored only in the core database. For more information on queries, see "Database queries" on page 104.

Dynamic targets can include network view device groups, LDAP objects, LDAP queries, and inventory queries.

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct agent software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager and Scheduled Tasks Application Policy Manager.

Windows 95/98 and NT devices need to be configured to log in to the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management application policy management. As of this printing, more information on installing Active Directory client support was available here:

<http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utills/dsclient.msp>

In order to target a device from LDAP, each Windows NT/2000/2003/XP device must have a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged in to the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows NT domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools | Distribution | Directory Manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "LDAP queries" on page 108.

Adding additional targets

When creating a policy-based task, it is often a good idea to initially deploy the policy to a small target set. This is done so that if problems are encountered when deploying the policy it will only impact a small set of users. Once the results of the deployment to the small set of users have been validated, add additional targets to the policy. When new targets are added to an active policy task, the policy immediately becomes available to the newly-targeted devices or LDAP items.

Applying scope to application policies

Multiple scopes can filter the policy-based management target details pane for a target lists. However, the final scope that a policy uses is always the scope of a task owner. If the policy task is listed in **Common tasks**, and another Management Suite user with a different scope looks at the target details pane for the task (let's call this second person a target list "editor"), the target details pane is filtered by the editor's scope. In this case, the editor may not see all the targets the policy will be applied to in the target details pane, because the editor's scope may not allow them to see all targets in the creator's scope.

What users see on their devices

Application policies are always processed using a pull model. Devices check with the core server for new policies that might apply to them. When this check occurs, a dialog appears at the device showing only unprocessed, recommended and optional policies, not required policies. When an unprocessed, recommended policy appears in the UI, it is checked by default to encourage the end user to process it.

Once a policy is processed, it may still show up in the UI if it's set up to run periodically. If this is the case, it will continue to be selected, event if it's a recommended policy. A policy may also continue to appear in the UI if it wasn't applied correctly.

Users can manually launch the policy-based agent by clicking **Start | Programs | LANDesk Management | Policy-based delivery**.

Using the local software deployment portal

The software distribution agent on managed devices also provides a software deployment portal. The portal checks the local software distribution cache for policies that apply to the local device/user. The portal then displays a Web page listing available policies. Users can select a policy from the list and click **Download selected** to install the packages associated with the policy.

To use the software deployment portal

1. On the managed device, click **Start | Programs | LANDesk Management | LANDesk Software Deployment Portal**.
2. Click the policy you want to apply.
3. Click **Download selected**.

This chapter explains how to use LANDesk Management Suite Package Builder to create software packages. You may also want to refer to "Appendix C: Additional software distribution information" on page 625.

Read this chapter to learn about:

- "Setting up a package-building computer" on page 191
- "Package-building overview" on page 191
- "Running the Package Builder wizard" on page 193
- "Uninstalling software distribution packages" on page 194

Setting up a package-building computer

The package-building computer should be a dedicated computer with a clean installation of its operating system. The clean installation is necessary because the package-building process captures all elements added or modified on the package-building computer.

Because you can distribute packages only to clients running the same operating system as the package-building computer, you should have a separate package-building computer, or a separate drive partition, for every operating system you distribute to. You can also use a single computer with multiple OS images as your package-building computer.

Any preinstalled software on the package-building computer reduces the Package Builder's ability to recognize changes. For this reason, your package-building computer must be as generic and clean as possible. This rule also applies to the CONFIG.SYS and AUTOEXEC.BAT files and other configuration files that the application installation process may modify.

To install the package-building software

1. From your package-building computer, browse to **ENUSETUP.EXE** in the LDMAIN\install\Package_Builder folder of the core server.
2. Double-click **ENUSETUP.EXE**, then click **Next**.
3. Type in the location of the folder where you want to install the package-building software, then click **Finish**.

Setup puts three items on the package-building computer:

- **Package Builder wizard:** Used to automatically create software distribution packages. It takes a "before" snapshot of the computer's state, has you install the software, takes an "after" snapshot of the computer's state, and builds a package from the differences in the snapshots.
- **Enhanced Package Builder:** Used to manually create, modify, and edit software distribution packages.
- **Package Builder wizard help:** Online help that describes the Package Builder wizard.

Once the Package Builder software is installed on your computer, you can use this computer to create and edit software distribution packages. The Package Builder stores packages on the local hard disk by default. Once these packages are built, you must move them from the package-building computer to the package share on your delivery server.

Package-building overview

You can use the Package Builder wizard to automate the process of taking snapshots and compiling them into standalone packages. As shown below, the process includes four steps:

1. Taking a pre-installation snapshot
2. Installing the application or making a computer configuration change
3. Taking a post-installation snapshot
4. Restoring the package-building computer

1. Taking a pre-installation snapshot

To build a software package, use the Package Builder to scan the local hard drive. You can specify exactly which portions of the drive are scanned in the Scanning Options page. This scan checks the system registry and all the directories and files on the local computer. After you install new software on the system, the Package Builder uses this information to detect what changes were made to the computer; it then compiles these changes to create the software distribution package. This information is stored in the Temporary Work Directory. Specify this directory in the Options page of the Package Builder wizard.

Package Builder scans all local drives by default. If you don't plan to make any changes to a local drive during the installation, remove it from the scan to speed up the pre-scan process. For best results, allow the Package Builder to scan the drive partition where the operating system is stored, plus the drive where you intend to install the software or change the configuration.

If, at any time during the package-building process, the hard drive space on the package-building computer gets low, the Package Builder will stop, display a warning, allow you to provide more drive space, then continue the package-building process.

Even if you remove all the local drives from the scan list, the Package Builder still scans the system files and folders, as well as the computer's registry.

2. Installing the application or making a computer configuration change

Once the pre-installation snapshot is created, the Package Builder prompts you to install the application software to distribute as a package.

You can install multiple applications in a single package, but you should install only suite-type applications with this process. If you install multiple applications as one distribution package and later want to omit one, you must first remove the entire group and then install a new group of applications. If you want to install multiple packages to your managed clients, you should edit the software distribution script so that it installs several different packages during the distribution.

The Package Builder monitors the installation during this step, then waits until the installation is finished to continue with the wizard pages. You can then customize the finished program. For example, if the install program creates an uninstall icon that you prefer not to distribute to clients, you can delete the icon before the post-installation snapshot in step 3, omitting it from the package. You can also add new icons to specific program groups, which provides a single point of access for all your users.

You need to provide any setup information requested by the system, and answer all questions presented during the software setup. The Package Builder cannot perform these tasks for you, but it will save the information as part of the package.

If you want to change only some of the system settings on clients, or if you want to copy a collection of specific files, you can create a package without using the snapshot process.

When you're satisfied that the application software or the configuration changes are ready, return to the wizard and click Next to start the post-installation snapshot.

3. Taking a post-installation snapshot

In this step, the Package Builder takes a second snapshot of the package-building computer and compares it with the pre-installation snapshot. By analyzing the differences, the Package Builder can identify any changes that have occurred on the computer, and then build a package distribution configuration script. This file has a .CFG file extension, and is located in the c:\Program Files\Intel\Package Builder\Working folder on the package-building computer.

This .CFG script file describes the changes to the registry, the file system, the desktop, and other system resources. It does not create a removal control file however, so you must add an uninstall option manually, either when you edit the script or when you schedule it for distribution.

Once these changes are saved, the Package Builder wizard offers the option to compile the .CFG file into an executable file, or to open it in Package Builder to make additional changes. Click Edit to open the new .CFG file in Package Builder and make your modifications. When you're satisfied with the installation, click Build to create the package.

Once finished, a page appears showing that the package was created and stored in the default directory on the package-building computer.

4. Restoring the package-building computer

Once you finish the package-building session, you should restore the package-building computer to its pre-installation state. This process ensures that the computer is in a clean state for the next package build. ESWD doesn't include a process for restoring the computer to a clean state; therefore, you should use a computer-imaging program such as the LANDesk imaging tool that is part of OS Deployment, Symantec's Ghost*, and so on to restore the client's operating system.

If you use a utility like Ghost to restore the package-building computer, you will also delete the .CFG file that was used to create the package. If you want to keep these files available, either to use in future packages or to edit at a later time, you can store them on a network share drive. Just specify a network location in the Options page of the wizard to preserve these files.

By default, each new system scan is stored in a new working directory, but you can use the same folder again if you prefer to overwrite the old system scan. Some users keep software images of multiple operating systems on a single package-building computer. This solution provides optimum flexibility when creating software packages, without dedicating multiple computers specifically for software package building.

Running the Package Builder wizard

As described earlier, building a software distribution package is a two-phase process. The first phase creates an installation script (.CFG) file in the Package Builder working directory. This script contains all the client instructions for installing the software. The second phase builds the software distribution package. The package contains the instructions plus the files.

To run the Package Builder wizard

1. From your package-building computer, click **Start | Programs | LANDesk Management | Package Builder wizard**.

2. Click **Scan Options** to configure the scan process. On this page, you can select which directories the wizard monitors for changes and whether the wizard creates a backup to return the client to its present state after the package has been created. When you're finished modifying the form, click **OK**.

At least one logical or physical disk drive must be monitored

The Package Builder wizard needs to monitor at least one logical or physical disk drive to track system information changes. If you clear the default drive selection in the Scan Options page, and set it to monitor no drives, the wizard will exit.

3. Click **Build Options** to configure user-specific settings for Windows NT and Windows 2000/2003/XP systems. You can select to have these settings applied to the logged-in user (or the default user if no one is currently logged in) or to all users. These user-specific settings include Start Menu items, shortcuts, and registry settings for the HKEY_CURRENT_USER key. To return, click **OK**.
4. Click **Next**. The wizard will check out your system.
5. Select the method you want to use to install the application:
 - If the installation program is locally available (such as a SETUP.EXE program), click **Browse** to locate the installation program, select it, and then click **Monitor**.
 - If the installation program is on an autorun CD, click **Next** and insert the CD.
 - To make other types of changes for a software distribution package (such as copying files or creating desktop shortcuts), click **Next** and run the appropriate utility.
6. Follow the prompts to install the software.
7. When the installation is complete, enter a name for the package. We suggest you enter a name that includes both the software and the operating system; for example, WinZip_Win2K for a package that installs WinZip on a Windows 2000/2003 client.
8. Click **Compare**.
9. When the .CFG file has been created, click **OK** and then **Build**.
Note: The .CFG file can be customized and then built into a package. For more information, see "[Scripting guide for .CFG files](#)" in Appendix C.
10. When the build completes, the wizard will put the package in the Onefile folder of the Package Builder Working directory. The package will be an .EXE file with the name you selected. Click **Finish**. You can manually test this package by clicking the .EXE file.

The next task is to set up the delivery server and copy this package to it. For more information, see "[Setting up the delivery server](#)."

Uninstalling software distribution packages

ESWD has the following methods for uninstalling packages that have been created and distributed to your clients:

- Uninstall command in Package Builder
- Uninstall option in the console
- Uninstall package with Package Builder wizard

Uninstall command in Package Builder

You can enable the Package Builder Uninstall command on all packages distributed to clients. If you use this command, packages create their own uninstall executable in the application's default directory on the client when they're installed. You can then create a script to activate that uninstall file on the client and remove the package.

Advantages to this method include:

- The uninstall is triggered by the script, and the installed files are completely removed.
- All file counters are correctly decremented during the uninstall. This means that shared .DLLs that affect other programs on the client aren't removed.

Disadvantages to using this method include:

- The Uninstall command must be included when you create the initial package.
- Uninstall prompts the user to remove the application. If the user responds "No," the package isn't uninstalled. You can't hide this prompt from users.
- The uninstall file is on the client, so a user could uninstall the software package without your knowledge. The uninstall file shows up in Control Panel | Add/Remove Programs.
- You must know the correct path to access the file.

The following example illustrates the syntax for creating a script that triggers the uninstall file to uninstall WinZip on the client:

```
[MACHINES]
REMEXEC0="C:\Program Files\WinZip\UninstallINSTALL.EXE"
REMEXECO is the Remote Execute command.
```

"C:\Program Files\WinZip\Uninstall INSTALL.EXE" is the complete path to the uninstall file. Quotes are required if there are spaces in the path names. The default name for this file is "Uninstall" + the name of the software distribution package.

Once you have created a script that targets an uninstall package, schedule it to be sent to your users, and the package will be uninstalled.

Uninstall option in the console

You can use the tools in the console to uninstall distributed packages. From the console, click **Tools | Distribution packages**, and create a new SWD package. On the **Install/Uninstall options** page, click **Uninstall** and finish configuring the package. This sets a "remove all" flag in the package so that everything installed in the installation script is removed.

The advantages of this method include:

- The uninstall executable is not on the client.
- This executable can uninstall software distribution packages that were not built with the Uninstall command.

Uninstall package with Package Builder wizard

If the above methods do not produce the desired results, there is one other option. You can use the Package Builder wizard to create a package of the uninstall process on the package-building computer, then distribute it to your clients.

This is not a recommended procedure

If the application you're uninstalling uses shared .DLLs, this method could remove .DLLs that are required by other applications.

To create an uninstall package

1. Start the **Package Builder wizard** on your package-building computer. The application you want to remove from your clients should be already installed with the same defaults as your clients.
2. Click **Next** to start the pre-snapshot phase, then click **Next** again. *Don't click the Browse button.* If you click Browse, you will start the installation process for another application; this procedure is for uninstalling an application.
3. When the pre-snapshot is complete, press **Alt+Tab** to switch to another application. *Don't click the Browse button.*
4. Click **Start | Settings | Control Panel** to display the Control Panel window.
5. Double-click the **Add/Remove Programs** icon to display the Properties dialog. In the **Install/Uninstall** tab, click the application you want to remove, and click **Add/Remove**. If the application has its own uninstall program, you should run it now.
6. Once the application is uninstalled, press **Alt+Tab** to return to the Package Builder wizard.
7. Enter the **name** for this uninstall package, and click **Compare** to start the post-snapshot phase. Once this is complete, the Congratulations dialog appears. Click **OK** to close it.
8. When the Ready to Build dialog appears, click **Build**, then click **Finish** to complete the package-building process.

You can distribute this package to clients.

Software license monitoring

Software license monitoring gives you the tools to implement complete, effective software asset management and license compliance policies.

IT administrators often find it challenging to track product licenses installed on numerous devices across a network. They run the risk not only of over-deploying product licenses, but also of purchasing too many licenses for products that turns out to be unnecessary. You can avoid these problems by using the **Compliance** tree to monitor and report on product licenses and usage across your organization. Compliance features include:

- **Passive, low-bandwidth monitoring:** The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth. The agent continues to monitor usage for mobile devices that are disconnected from the network.
- **Reporting:** The power of compliance monitoring rests in its data-gathering capabilities. Use the data to track overall license compliance and to monitor product usage trends.
- **Product license downgrading:** For certain products, you can set up license downgrading so that newer versions of a product can loan a license to older versions, keeping your devices license compliant at all times.

Software license monitoring features include:

- Ability to scan for both known and unknown applications, and a disposition tool to define and track previously unknown applications.
- Automatic product discovery scans for new applications on managed devices and gathers data on which files are associated with those applications.
- Application launch denial to keep unauthorized software from running even on devices disconnected from the network.
- Full integration with LANDesk asset management for current, complete information about installed applications.
- Extensive application usage and license compliance reporting.
- Extensive license monitoring and reporting features, including number of times each licensed application was launched, last date used, and total duration of application usage.
- Easy configuration of license parameters, including number purchased, license type, quantity and serial number.
- License purchase information, including price, date purchased, P.O. number, and reseller information.
- Installation tracking and reconciliation, including the license holder and physical location of the device the license is installed on, as well as additional notes.
- Aliasing to track software when vendor information or filenames change.

If you've used software license monitoring in Management Suite versions prior to 8.5, be aware of the following changes:

- Licenses are now tracked by group. For example, you can have the same product in different groups, and the licenses for that product will be tracked independently.
- In the **Compliance** tree, you can specify a scope for a product group. Products within that group will only count and report on licenses for devices that are within the specified scope.
- License management is done through the **Compliance** tree. The **All products** tree shows products you can manage and usage information for those products.

Read this chapter to learn about:

- "Monitoring software license compliance" on page 198
- "How compliance monitoring works" on page 199
- "Configuring products to monitor" on page 199
- "Using scopes with products" on page 204
- "Denying product and file execution" on page 206
- "Creating product and vendor aliases" on page 208
- "Viewing license compliance and product usage/denial trends" on page 206
- "About LDAPPL3" on page 210
- "Exporting and importing software license monitoring data" on page 212

Monitoring software license compliance

The **Software license monitoring** window is designed to let you monitor and manage the software that's installed on your devices. Navigate the window from the left pane, where you can see these categories in the **Software license monitoring** tree:

- **Compliance:** In this tree view, you can monitor usage and license compliance for products across your organization and view license compliance/usage for all devices. You can configure product licenses and define which devices are to be associated with product groups.
- **Denied products for all devices:** In this tree view, you can see all products you have denied access to. Managed devices won't be able to run these products.
- **Inventory:** In this tree view, you can edit the list of files the inventory scanner uses to identify your devices' software inventory. You can also specify those files that should be denied execution on your devices.
- **Aliases:** In this tree view, you can create product or vendor aliases. An alias ensures that you can correctly account for all installed executables from a specific vendor if the vendor name changes, or for a product if its vendor and name change. This feature is especially useful if you're monitoring products in the **Compliance** tree and need to maintain accurate information about your licenses.

The **Product definitions** group has these sub-categories:

- **All:** In this tree view, you can see all predefined, custom, and automatically discovered products.
- **Automatically discovered:** In this tree view, you can see products discovered on managed devices by GatherProducts.exe, which is launched by the inventory scanner. For more information, see "Step 2: Associate files with products" on page 200.
- **Custom:** In this tree view, you can see products that you've created and predefined product definitions that shipped with Management Suite.

You can configure products by specifying which files they contain and setting up product license downgrading. Drag products from the **Product definitions** view into a group in the **Compliance** view so you can configure them for monitoring. You can also import and export data appearing in the **Software license monitoring** window for use on other Management Suite 8 core servers you may have on your network. This feature is useful if you need to ensure that software license monitoring information is synchronized on all of your version 8 core servers.

How compliance monitoring works

The software monitoring agent installs on your devices as part of the default device configuration setup. The agent records data about all installed applications on a device.

Use the **Software license monitoring** window to monitor installed applications. After you indicate the product files and licenses that you want to monitor, the following occurs:

- Management Suite detects devices that have the applications installed that you want to monitor and displays this list in the **Software license monitoring** window. The inventory scanner on managed devices updates usage information each time it runs.
- During the next scan, the scanner reads the usage data collected by the software monitoring agents and sends this data to the core server. Management Suite then updates the **Software license monitoring** window with information for the specific licenses and products you're monitoring.

About mobile devices

For mobile devices disconnected from the network, the software monitoring agent continues to record data and caches it. After the device reconnects to the network, the next scan detects and sends that data to the core server. The **Software license monitoring** window is then updated with the latest license compliance, usage, and denied application data for those mobile devices.

Configuring products to monitor

To begin monitoring products for license compliance and usage trends, you must complete four different procedures within the Software License Monitoring window:

"Step 1: Setting up compliance groups" on page 199

"Step 2: Associate files with products" on page 200

"Step 3: Adding product license information" on page 202

"Step 4: Making changes available to managed devices" on page 203

Step 1: Setting up compliance groups

In the left pane under **Compliance**, set up a tree of product groups and individual products. You can group products any way you want, for example:

- By department
- By vendor/publisher, such as Adobe or Microsoft
- By specific categories, such as Unauthorized Files
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage trends. For example, under an Adobe group, you might add products such as Photoshop* and Illustrator*.

The **All products** tree view provides a list of preconfigured products you can use. When using a preconfigured product, you need to make sure the monitored files match the versions on your network.

To set up a compliance group

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the **Compliance** shortcut menu, click **New group**.
3. Enter the new product group name. If you're using scopes to define which devices are to be associated with the product group for the purpose of determining compliance, assign a scope to the group. For more information, see "Using scopes with products" on page 204.
4. To add products under this group, right-click the group name and select one of the following:
 - **Add product:** To add an already defined product.
 - **New licensed product:** To add a new product, which will also appear in the **All products** tree view.
5. Enter the product name.

To edit compliance items

- To edit properties for a product: In the left pane, in the product name shortcut menu click **Properties**. Enter the product name, version, publisher name, if you want to deny its use to devices, and if you want to match all files (that is, require that all files associated with this product be installed on the device before a license is counted as used). Click **OK**.
- To delete or rename a product group or product: In the left pane, in the group or product name shortcut menu, click **Delete** or **Rename**.

Step 2: Associate files with products

By associating files with products, you define the files that must reside on a device in order for the product to be considered installed on that device and to be monitored. Files are identified by these attributes: name, size, and version.

By default, if any one file associated with a product is found on a device through the process of inventory scanning, then the product is considered to be installed on that device. If you want to require that all files associated with a product be found on a device in order for the product to be considered to be installed on that device, then use the **Match all** feature as described above in the "To edit compliance items" task.

Software license monitoring automatically gathers data on what files are associated with which discovered products. When the inventory scanner runs, it launches GatherProducts.exe. This program scans for new applications by looking for install signatures in the registry and by looking for new application shortcuts. On managed devices, GatherProducts.exe stores discovered product information as XML files under ..\LDClient\Data\proddefs. The inventory scanner sends new and changed product definition XML files to the core server so they can be added to the database.

Automatically-discovered products that include a GUID (Globally Unique Identifier, a unique 128-bit number) in their name were gathered from the local registry's MSI database. Automatically-discovered products that don't have a GUID in their name were gathered from shortcuts. The number of files associated with automatically-discovered products varies and depends on the product.

In the **Automatically discovered** tree view, there are **Discovery date** and **Last used** columns. Use these columns to help decide whether particular automatically-discovered products are worth monitoring.

You can also select files to associate with products from categories under the **Inventory** tree. After you associate a file to a product, that file will also appear in the **Inventory | Views | In monitored product** category. When selecting files, you must pick versions that exactly match those found on your network. If the filename or size doesn't match, then the file won't be found and the product won't be monitored for compliance.

Software license monitoring puts files into these categories that you can select from:

- **Discovered but not in product:** Files that also appear in the discovered on computers list but aren't currently associated with a product. Use this list to view files that you may want to associate with a product for monitoring license compliance and usage trends.
- **Discovered on computers:** All files that have been discovered on your devices. You can sort the right-pane columns to get a clear understanding of each file's status, such as if it's associated with a monitored product, being scanned by the inventory scanner, etc. If discovered files have the status of **To be dispositioned**, this means they were discovered during a software scan but have not already been dispositioned to be scanned by the inventory scanner. A file must be dispositioned to be scanned by the inventory scanner before it is regularly scanned.
- **In monitored product:** Files that are associated with a product for monitoring license compliance and usage trends. You can't move these files from the **Inventory** tree; they're only shown for reference.

Alternatively, you can check the **All products** tree for preconfigured products. If a product there matches one you want to monitor, you can drag it to the **Compliance** tree and configure it there.

To associate files to a product

1. Browse to the desired product.
2. In the product's shortcut menu, click **Files**.
3. On the **Files** tab, click **Add**.
4. Use the **Find** box to enter a word, then use the **In column** drop-down menu to specify if the word is part of the file's vendor, product, or filename. You can also use the **File list** drop-down menu to specify the Inventory tree category you want to search.
5. Click the **Search** toolbar button.
6. Select the file or files from the returned list, then click **Add** to add it to the files list of this product.

If necessary, you can manually add files. For more information, see "Adding files to LDAPPL3" on page 212.

After you have associated the files to the product, Management Suite detects the devices currently running the product (as indicated by the last software scan) and populates the **Software license monitoring** window with that information. After the next software scan, you can view the usage report to see devices that have run the product, or the denial report to see devices that have attempted to run the product.

To view a product usage report

- In the **Compliance** tree, from the product's shortcut menu, click **Usage report**.

To view a product denial report

- In the **Denied products for all devices** tree, from the product's shortcut menu, click **Denial report**.

You can also find out which products have the same version of a file associated with the by using the **Find in product** option.

To find which products have a file associated with them

1. Click **Inventory | Views | In monitored product**.
2. Find the file you want to search on, and from its shortcut menu click **Find in product**. The cascading menu shows you which products have that same file and file version associated with them. Clicking a product takes you to that file in the product.

To find where files are installed on devices

1. Click **Inventory | Views | In monitored product**.
2. Find the file you want to search on, and from its shortcut menu click **Where installed**.

To turn on or off managed device software execution reporting and product definition reporting

1. On the core server, click **Start | Programs | LANDesk | LANDesk Configure Services**.
2. Click the **Inventory** tab | **Advanced settings** button.
3. Change **Send all executed software** and **Send product definitions** as necessary, and click **Set**. 1 is on, 0 is off. The default is 1 (on).
4. Click **OK**, and restart the inventory service when prompted.

Step 3: Adding product license information

You need to add license information to a product for the product to be monitored for license compliance. If you only want to track product usage, you can skip this procedure.

After you set up license information for a product, if you ever see a red icon with an exclamation point appearing next to the product group, this means that one of the products in the group isn't license compliant. Expand the product group to find the non-compliant product, then view its associated information in the right pane.

If you see a yellow icon with an exclamation point, the licenses for that product are underused, and you have more licenses than you have installations.

To add product license information

1. Click **Compliance | product group | product**.
2. In the product's shortcut menu, click **Manage licenses**.
3. In the **Product licenses** dialog, click **Add**, and use the tabs to enter the license, purchase, and tracking information that's relevant to your organization.
4. When finished, click **OK**.

Step 4: Making changes available to managed devices

You must use the **Make available to clients** button for any product changes to take effect on managed devices. Once you click this button, software license monitoring updates the product definition files. The next time devices do an inventory scan, the scanner gets the updated product definition files from the core server and applies any changes.

Configuration changes involving automatically discovered products aren't part of the **Make available to clients** process. Restarting the inventory service or waiting for database maintenance to run are the only ways to update ignored products or product definition list changes.

Tracking licenses using the Match all files option

You may encounter a situation where you need to track licenses for two or more products that contain an executable of the same name and size. In such a case, you also need to configure software license monitoring so it monitors a file unique to each product. By selecting **Match all files** and using both the executable and a unique file to identify license usage, you specify that all files associated with a product (as found in its **Files** list) need to be installed on a device before a product license is considered used. This ensures that the scanner can correctly track the products licenses.

The following two examples help explain when you would select **Match all files**:

- If you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. Software license monitoring won't monitor these other files for compliance (only executables are monitored for compliance, but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license).

Note: If you add files whose extensions are different than .EXE to a product (in order to use the **Match all files** option, you must first edit the LDAPPL3.TEMPLATE file to include files having those extensions in a software scan). By default, LDAPPL3.TEMPLATE only specifies executables. For more information, see "Editing the LDAPPL3.TEMPLATE file" in Appendix A.

- If you're monitoring 10 licenses for Office XP Standard (that includes Word, Excel, Outlook, and PowerPoint), as well as 10 licenses for Office XP Pro (that includes the same applications, in addition to Access), you face the problem of wanting to monitor two distinct product licenses that contain executables of the same name and size. The scanner can't distinguish between license types by tracking individual files, nor by using just the **Match all files** option for both products.

In this case, you must go one step further by adding an Office XP Pro executable to the Files container of XP Standard (for example, Access), marking that executable as **Not in product**, and selecting **Match all files**. This ensures that the software monitoring agent won't record an Office XP Pro license as an XP Standard license, which would occur if only **Match all files** was turned on. Marking a file as **Not in product** tells the inventory scanner, which is responsible for recording license information for a device, that the file must not exist on the device for a license to be recorded for the product.

To mark an executable as not in product

1. Click **Compliance | product group | product**.
2. In the product's shortcut menu, click **Files**.
3. Select the file you want to search to exclude, and from its shortcut menu click **Not in product**.

Using scopes with products

The Management Suite administrator can create scopes to define sets of devices. A scope defines a set of devices from a database query, a directory location, or a device group. These scopes can be assigned to Management Suite users to limit the managed devices they can see while connected to a core server.

When connected to a core server, the Management Suite administrator can see every device managed by that core server. Management Suite users, on the other hand, are restricted and can only see the devices that reside within the scopes assigned to them. For more information, see "Role-based administration" on page 59.

With Management Suite 8.5 and later versions, you can now assign scopes to monitored products. In the Compliance tree, you can assign scopes to a product group. Products within that group will only count and report on licenses for devices that are within the specified scope.

For example, this allows you to group products by department and track licenses by department. If you didn't use scopes, and marketing had 50 licenses for WinZip and Engineering had 50 licenses for WinZip, you wouldn't be able to tell if engineering had exceeded their license and was borrowing from marketing.

With scopes, you can put the marketing and engineering devices in different scopes. You can then have marketing and engineering groups under the compliance tree, and include Winzip in both groups. Once you add the marketing and engineering scopes to their respective group, you'll be able to track the marketing and engineering licenses separately.

Before applying scopes to monitored products, you must create scopes in the **Users** window (**Tools | Administration | Users**).

To apply scope to a product

1. Put your products into groups that align with the scopes you want to apply.
2. From the shortcut menu for the group you want to apply a scope to, click **Scopes**.
3. Click **Add** and click the scope you want. Click **OK**.
4. In the **Scopes** tab, remove the **Default All Machines** scope. Deleting this allows the newly selected scope to be applied.
5. Click the **Refresh** toolbar button and verify the scope is working the way you want it to.

Downgrading product licenses

The **Software license monitoring** window lets you "downgrade" licenses for certain products: if you have two versions of the same product installed on your network, you can set up the newer version to loan licenses to the older version.

By exercising your downgrade rights, you can prevent the older version from exceeding its license count. For example, you could configure Office XP to provide licenses to Office 97 when Office 97 licenses are exceeded, ensuring that devices can still run Office 97 applications while staying within compliance.

This feature is useful only for products where the vendor permits license downgrading. Microsoft, for example, allows this for many of its products. To verify that license downgrading is permissible for a product, refer to your license agreements.

The following scenarios (in addition to the one mentioned above) describe when you can downgrade licenses:

- Product #1 loans licenses to products #2 and #3: For example, you could configure Office XP to loan licenses to Office 97 and Office 2000.
- Products #1 and #2 loan licenses to product #3: For example, you could configure Office 2000 and Office XP to loan licenses to Office 97.

To downgrade a product license

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance | product group | product**.
3. From the product's shortcut menu, click **Properties**.
4. On the **Downgrades** tab, click **Add**.
5. Select a product that you can give licenses to, then click **Add**.
6. To set up a second or third product to give licenses to, repeat step 3. The order in which the downgraded products appear in the list is important. Products ranked lower in the list will only get licenses if the products above them haven't used all of the available licenses. To move a product up or down in the list, select it and click **Move up** or **Move down**.

Only downgrade a product if your licensing for that product allows it.

You can monitor license downgrades in the product's **Manage licenses** dialog.

Denying product and file execution

You can prevent devices from executing products you specify. From a product's shortcut menu in the **All products** tree, you can click **Deny use of this product**. When devices try to run a denied product, they'll see a message box telling them their system administrator has prevented access to that program. You can restore normal access to a product by unchecking the **Deny use of this product** option in the **All products** tree. All denied products appear in the **Denied products for all devices** tree.

All files in the **Files** list of a denied product will be denied on devices. The **Match all files** product option state doesn't affect denied products.

You can also deny individual file execution. When denying individual file execution, note that the denial is based on filename only. Any filename matching a denied filename will be denied execution. To deny file execution, select the file you want to deny in the **Inventory | Files** tree and from its shortcut menu click **Deny use of this file**. This moves the file to the **Inventory | Files | To be denied** tree.

You must click the **Make available to clients** button for any product changes to take effect on managed devices.

Viewing license compliance and product usage/denial trends

One of the most powerful features of the **Software license monitoring** window is the ability to track overall license compliance and monitor product usage and denial trends. The following types of data appear in the right pane of the Compliance tree:

- **Overall license compliance:** Shows overall license compliance for all defined product groups
- **Product group license compliance:** Shows compliance at the product group level
- **Product usage report:** Shows usage information at the device level
- **Product denial report:** Shows denied executables at the device level

Because compliance calculation can take a while when there are lots of managed devices, the **Compliance** view only updates when you click the software license monitoring window's **Refresh** toolbar button. Once you click **Refresh**, the **Compliance** tree item name changes to show the last update time.

To view overall license compliance

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance**, and click the **Refresh** toolbar button. In the right pane, overall compliance data for all defined groups will appear, such as:
 - **Name:** Names of the defined product groups
 - **Complies:** Shows if licenses are compliant for a product group
 - **Out of compliance:** Number of out-of-compliance licenses for a product group
 - **Licenses not deployed:** Number of licenses not being used for a product group
 - **Licenses:** Total number of licenses available
 - **Installations:** Number of installations detected

- **Loaned:** If license downgrading is active, how many licenses the product is loaning
- **Borrowed:** If license downgrading is active, how many licenses the product is borrowing.

You can also click a product group to see compliance for a single group rather than all groups.

To view a product usage report

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance | product group**, and the product you want a report on. In the right pane, usage data for this product will appear, such as:
 - **Device name:** Name of device
 - **Last used:** Last time the .EXE was run on the device
 - **Last user:** Username of last user to log in to the device
 - **# Executions:** Number of times the .EXE has run on the device
 - **Duration (minutes):** Number of minutes the .EXE has run on the device
 - **Days since last used:** The last time the user started the product
 - **Discovery date:** The date the product was first detected
 - **Reset date:** When the usage history was reset last
 - **Last reset date:** The last time the usage history was cleared from the core database and device registry. The date comes from the core server.

To view a product denial report

- In the **Denied products for all devices** tree, from the product's shortcut menu, click **Denial report**. In the right pane, denial data for this product will appear, such as:
 - **Device name:** Name of device
 - **Last user:** Username of last user to log in to the device
 - **# Denials:** Number of time the .EXE was denied.
 - **Last reset date:** The last time the usage history was cleared from the core database and device registry. The date comes from the core server.

You can sort these columns by clicking the column header. You can also double-click a device name to open a window showing the inventory on that device.

When you view product reports in the **Compliance** tree, the reports are filtered by the configured scopes. If you want to view a global report, view the report from the **All products** tree. From a product's shortcut menu in the **All products** tree, click **Usage** report.

Printing or exporting data in report format

You can print any of the Compliance tree data in report format or export it to a variety of file types, such as Crystal Reports*, Adobe Acrobat*, Microsoft Excel*, and so on.

To print or export data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance** and expand the tree to view the product data that you want to print or export. (This data will appear in the right pane.)

3. Click the **Print** toolbar button to open the data in report format.
4. To print the report, click the **Print** toolbar button.

Resetting usage and denial report data

You can clear the data for your monitored products' usage or denial reports. Clearing the data lets you reset the counter so you can begin tracking applications from a certain point on. The reset affects all devices, and it clears the device registries and the core database of all past usage and denial report data. For this reason, it's important to print or save any usage or denial reports you may want to keep before resetting. When you reset the usage and denial report data, you do so for all monitored products.

To reset usage and denial report data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Right-click **Compliance** and select **Reset usage information**.
3. When prompted, click **Yes** to complete the reset.

On large databases, the reset can take a long time. If the reset times out, your DBA can reset the usage manually by entering the following SQL command:

```
UPDATE FileInfoInstance
SET SCM_TotalSessionTime = NULL,
SCM_SessionCount = NULL,
SCM_SessionsDenied = NULL,
SCM_LastUser = NULL,
SCM_LastSessionTime = NULL
```

Creating product and vendor aliases

Use the **Aliases** view to create product or vendor aliases. An alias ensures that you can correctly account for all installed products by:

- **Normalizing executable file data:** An alias lets you make consistent the information the core database needs to correctly identify an installed product. For example, the file information provided by a vendor isn't always consistent. Files scanned into the core database for various Microsoft products may show the vendor name as being Microsoft Corp, Microsoft @, or just Microsoft. If you were to run a query on "Microsoft @" products, you would get only a partial list back of Microsoft products installed across your network. By creating a vendor alias of "Microsoft Corp" for all of your Microsoft products, you ensure that those products all have exactly the same vendor name.
- **Updating executable file data:** An alias lets you update file information if the product name or vendor changes after installation. For example, sometimes vendor or product names change because a company has been newly acquired or divested, or a company has renamed its product after several versions. If this occurs with your applications, use aliasing to associate new vendor or product names with the originals, ensuring that the core database can continue to identify your executables accurately. This feature is especially useful if you're monitoring products in the **Compliance** tree and need to maintain accurate information about your licenses.

About the Aliases view

The right pane of the **Aliases** view shows the original vendor and name for a product, as well as any new vendor and/or product names that you may have added. A software scan must occur before a new alias will appear in the **Software license monitoring** window or in Asset reports that include data about your device's software.

You can create two types of aliases in the **Alias properties** dialog:

- **Vendor:** An alias for all installed products of a certain vendor (enter the original vendor name and a new vendor name).
- **Product:** An alias for a specific product (enter original vendor and product names, as well as new ones). A product alias that includes a new vendor will always take precedence over an alias created for all products of a certain vendor.

Aliases you create will show up in the tree views for **Aliases**, **Compliance**, and **Inventory**, as well as in any asset reports that include device software data.

To create an alias

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the left pane's **Aliases** shortcut menu, click **Create alias**.
3. In the **Alias properties** dialog, enter the original vendor and original product name, as well as the new vendor and/or new product name for the application. Click **OK**.

To delete an alias

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the left pane, click **Aliases**.
3. In the right pane's **Aliases** shortcut menu, click **Delete**.

After you delete an alias, the core database reverts to using the original vendor and product name.

Editing software inventory

Use the **Software license monitoring** window's **Inventory** tree to configure the files you want scanned or ignored by the inventory scanner. The inventory scanner uses this configuration data to identify your devices' software inventory. The scanner recognizes software applications in three ways:

- Filename
- Filename and size
- Information included in an application's executable file

About the Inventory tree

The Inventory tree contains two panes that show the following details.

- **Left pane:** This pane shows a Files and Views tree.
 - **Files:** Displays the categories you can use to organize the files:
 - **To be scanned:** Files in your core server's LDAPPL3 that the scanner can identify on devices.
 - **To be dispositioned:** Files that have been discovered on devices but are unknown to the scanner. You must move these files into other categories before the scanner can identify them.
 - **To be excluded:** The scanner ignores all occurrences of a file that you move here. If you delete a file from **To be excluded**, it appears in the **To be dispositioned** category.
 - **To be denied:** Execution is denied for all occurrences of a file that you move here. End users who attempt to run a denied executable will see the program run for a few seconds before it closes down. If you delete a file from **To be denied**, it appears in the **To be dispositioned** category.
 - **Views:** Displays the following file lists in the right pane:
 - **Discovered but not in product:** Files that also appear in the **discovered on computers** list but aren't currently being monitored in the **Compliance** tree. Use this list to view files that you may want to begin monitoring for license compliance and usage trends.
 - **Discovered on computers:** All executables that have been discovered on your devices. You can sort the right-pane columns to get a clear understanding of each file's status, such as if it's in a monitored product, or if it's currently in one of the above file categories. If discovered files have the status of **To be dispositioned**, this means they were discovered during a software scan, but aren't in the **To be scanned** list. A file must be in the **To be scanned**, **To be excluded**, or **To be denied** list before it's regularly scanned, excluded, or denied on devices.
 - **In monitored product:** Files that are monitored for license compliance and usage trends in the **Compliance** tree. You can't move these files from the Inventory tree; they're only shown for reference.
- **Right pane:** This pane changes depending on the item you select in the left pane.

About LDAPPL3

LDAPPL3 is the new version of LDAPPL.INI that shipped with older versions of Management Suite. Unlike the past, you shouldn't edit this new file directly in a text editor, because the data is now stored in the core server's core database. The next time the server writes a new version of this file, changes made directly with an editor will be lost. All edits to software descriptions contained in LDAPPL3 must be made from the **Software license monitoring** window.

As shipped with Management Suite, LDAPPL3 contains descriptions of several thousand applications, providing a baseline of executables that your devices may have installed. Use this window to select the executables listed in LDAPPL3 that you want the scanner to identify, exclude, or deny on devices. If an executable isn't listed in LDAPPL3, you can add it. For more information, see "Adding files to LDAPPL3" on page 212.

By default, LDAPPL3 contains descriptions of executables (.exe files only). If you want the scanner to also identify other types of application files (.DLLs, .COMs, .SYSes, and so on), you can manually add those files to any of the categories under the Inventory | Files tree *after* editing the LDAPPL3.TEMPLATE file to include all files of that type in a scan. For more information, see "Editing the LDAPPL3.TEMPLATE file" on page 602.

By default, the inventory scanner only scans for files listed in LDAPPL3. If you want to scan all files on devices, you can change the scanning mode to all files. Note that a mode=all scan mode can generate inventory scan files from devices that may be several megabytes in size. After the initial scan, the inventory scanner sends only delta scans, which will be much smaller. For more information, see "Editing the LDAPPL3.TEMPLATE file" on page 602.

Distributing LDAPPL3 to devices

Beginning with Management Suite 8, The inventory scanner can use HTTP for LDAPPL3 file transfers. This allows the scanner to support Targeted Multicast features like polite bandwidth and peer download. Peer download allows devices needing LDAPPL3 updates to check with the core server for the latest version's date, then devices will broadcast to peers on their subnet to see if a peer has the update in its multicast cache. If a peer has the update, the file transfer happens on the local subnet without generating network traffic across routers or WAN links. For more information on Targeted Multicast and peer download, see "Using Targeted Multicast with software distribution" on page 178.

Editing LDAPPL3

By default, LDAPPL3 pre-populates the **Inventory | Files** categories of **To be scanned** and **To be excluded** when you set up Management Suite. From these categories, you can edit LDAPPL3 by using a file's shortcut menu to select a new category.

Once you edit the core's LDAPPL3, you need to make the most recent changes available to devices the next time they run an inventory scan. Do this by clicking the **Make available to clients** toolbar button. This action compresses the core's LDAPPL3 by 70 percent, which enables the scanner to update the devices' corresponding LDAPPL3 without using significant bandwidth. (The device's LDAPPL3 is installed as part of the default device configuration setup). Both the device and core version of this file must be synchronized for the scanner to know which files to scan identify, exclude, or deny on devices.

If you don't want to wait for the next inventory scan to update your device LDAPPL3 files, you can make the edits available to devices in these ways:

- **By using your device logon scripts:** In the **Client setup** window, you can specify that your devices' local LDAPPL3 automatically receives updates from the core's .INI file each time a device boots.
- **By scheduling a job to push LDAPPL3 down to devices:** Use the **Scheduled tasks** window to schedule a time to push down the core's LDAPPL3 to each of your devices. By default, LDAPPL3 is located in the core's LDLogon shared folder.
- **By updating the LDAPPL3 automatically during inventory scans:** To automatically update the device's LDAPPL3 during an inventory scan, add a /i switch to the shortcut that launches the inventory scanner on devices.

To edit the core's LDAPPL3 file

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.

2. Click **Inventory | Files**, then click **To be scanned** to view the list of files that the scanner currently detects on devices, or click **To be excluded** to view the list of files that the scanner currently ignores on devices. These are the two LDAPPL3 categories that are populated by default when you set up Management Suite.
3. In the right pane, scroll down to locate the files that you're interested in moving to another category. Or use the **Find** box to search for a file by entering a full or partial filename with the wildcard asterisk (*) and clicking the **Search** toolbar button. The correct file should appear in the list. You can edit LDAPPL3 by using a file's shortcut menu to select a new category.
4. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Adding files to LDAPPL3

If you need to add new files to an LDAPPL3 category, you can do so by one of two methods.

To add individual files

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Inventory | Files**, then click the LDAPPL3 category the file should go into. See "About the Inventory tree" on page 209.
3. Click the **New file** toolbar button.
4. In the **File properties** dialog, enter the filename and properties, or browse for the file. By selecting the file via browsing, the fields will automatically populate with the filename and size. When adding files to the excluded or denied lists, enter the file name. If you enter file size of 1, any file with that file name matches.
5. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan.

If you want to add files other than executables with an .EXE extension, you must edit the LDAPPL3.TEMPLATE file and set the scanning mode to ALL. By running a Mode=ALL software scan, you can detect not only the device application files that are currently in LDAPPL3, but also all other executables that are unknown to LDAPPL3. The unknown files will populate the **To be dispo**sitioned category, where you can move them into other LDAPPL3 categories.

To run a Mode=ALL software scan, you must edit the LDAPPL3.TEMPLATE file located in the C:\Program Files\LANDesk\ManagementSuite\LDLogon folder of your core server. For more information, see "Editing the LDAPPL3.TEMPLATE file" on page 602.

Exporting and importing software license monitoring data

You can import and export data appearing in the **Software License Monitoring** window for use on other Management Suite 7 and 8 core servers you may have on your network. This feature is useful if you need to ensure that software license monitoring information is synchronized on all of your Management Suite 8 core servers.

You can *export* alias, product, and inventory data to an .XML file for importing into the core database on another core server.

You can *import* an .XML file from another console that you may have on your network. New data will be appended to the existing data. You can choose to overwrite or keep existing data in the core database.

To export LDAPPL3 data to an .XML file

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click the **Export** toolbar button.
3. Click **Only products and files** or **Everything**. Export products and files if you're sharing data with other core servers. Export everything if you're creating a software license monitoring data backup.
4. Enter or browse for the path and filename that you want to export to.
5. Click **OK**.

To import an .XML file containing LDAPPL3 data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click the **Import** toolbar button and select an LDAPPL3 file or an .XML file that has the data you want to import into the core database on this core server.
3. Select whether you want to overwrite or keep existing data. Click **OK**.
4. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Importing XML license data

You can import your organization's application license information into software license monitoring. The XML file must be in a specific format. Note that:

- All headings are required
- Product License Types must be spelled exactly including case and spacing
- All columns must have data
- The file must not be opened when importing
- You can create this file in a spreadsheet application and save it as an XML file

Here are the column headings:

- Product License Type
 - Competitive Upgrade
 - Freeware
 - New Purchase
 - OEM
 - Product Upgrade
 - Public Domain
 - Shareware
 - Unknown
- Quantity

- Serial Number
- Purchase Date
- Unit Price
- Order Number
- Reseller
- Owner
- Location
- Notes

Importing an old LDAPPL.INI into software license monitoring

The software description file in Management Suite 6.62 and older versions was named LDAPPL.INI. If you have a legacy LDAPPL.INI file containing software descriptions in the [Applications] and [Ignore] sections that you want to import into software license monitoring, you can, but the process is somewhat time consuming.

You must first edit the software descriptions in the [Applications] section that you want to import into the newer LDAPPL3. You can also import software descriptions from the [Ignore] section, which you don't have to edit before importing. Though the old LDAPPL.INI contained both software and hardware descriptions among other data, only the software descriptions from these two sections are imported into software license monitoring.

Importing customized hardware information

If you also have customized hardware information in the old LDAPPL.INI that you want to import (such as BIOS information), you must add that data to the LDAPPL3.TEMPLATE file directly. For more information, see "Editing the LDAPPL3.TEMPLATE file" on page 602.

There are two things you must edit in the old LDAPPL.INI to make the information compatible for importing into the newer LDAPPL3:

- In the [LANDesk Inventory] section: Update the Version and Revision lines
- In the [Applications] section: Use a comma to separate the vendor/product field for each application into two fields, one for vendor, one for product. For example:

In the old LDAPPL.INI, if a line reads:

```
<I>, EXCEL.EXE, 9165128, Microsoft Excel, 3.0a
```

You must change the line (by separating Microsoft (vendor) and Excel (product) with a comma) to read:

```
<I>, EXCEL.EXE, 9165128, Microsoft, Excel, 3.0a
```

IMPORTANT!

When importing software descriptions from an old LDAPPL.INI into the Software License Monitoring window, you must modify the data *exactly* as described. **Make sure you back up your database before starting the following procedure.** The better way to import software descriptions is to add the files individually to the categories under the Inventory | Files tree. For more information, see "Adding files to LDAPPL3" on page 212.

To import an old LDAPPL.INI into software license monitoring

Before starting this procedure, make a backup of your original LDAPPL.INI file.

1. Open your LDAPPL.INI in Notepad or another text editor.
2. In the [LANDesk Inventory] section of the file, search for the Version and Revision lines.
3. Change the **Version** line to read **3.0** and the **Revision** line to read **1.00**
4. In the [Applications] section of the file, edit the software descriptions that you want to import. Use the example shown above to ensure that you correctly edit the software description fields.
5. Delete all software descriptions from the [Applications] and [Ignore] sections that you don't want to import.
6. Save and exit out of the file.
7. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
8. In the Software License Monitoring window, click the **Import** toolbar button.
9. In the **Files of type** box, click **LDAPPL3 Files**, then browse to the location of your saved .INI file.
10. Select the file, then click **Open** to import the edited software descriptions into the Software License Monitoring window. Verify that the software descriptions imported into these categories under the **Inventory | Files**: From the [Applications] section to the **To be scanned** category, or from the [Ignore] section to the **To be excluded** category
11. Click the **Make available to clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan.

Unmanaged device discovery

The Unmanaged device discovery (UDD) tool provides a way for you to find devices on your network that haven't submitted an inventory scan to the LANDesk core database. Additionally, Extended device discovery (XDD) uses an agent installed on managed devices to find other devices sending network ARP broadcasts, as well as wireless access point (WAP) devices.

Read this chapter to learn about:

- "Unmanaged device discovery overview" on page 216
- "Discovering unmanaged devices with UDD" on page 217
- "Using extended device discovery (ARP and WAP)" on page 219
 - "Configuring devices to use extended device discovery (ARP and WAP)" on page 220
 - "Understanding IP address filtering with XDD" on page 221
 - "Working with devices found through XDD" on page 221
- "What happens when a device is discovered" on page 223
- "Deploying LANDesk agents to unmanaged devices" on page 224
- "Restoring client records" on page 225

Unmanaged device discovery overview

Unmanaged device discovery (UDD) provides many ways to scan for and detect unmanaged devices on your network.

Here are the basic UDD scanning methods:

- **Standard LANDesk agent:** Looks for the standard LANDesk agent (CBA) on computers. This option discovers computers that have the LANDesk products installed.
- **Network scan:** Looks for computers by doing an ICMP ping sweep. This is the most thorough search, but also the slowest. You can limit the search to certain IP and subnet ranges. By default this option uses NetBIOS to try and gather information about the device.
 - **SNMP:** UDD uses SNMP to discover devices. Click **Configure** to enter information about SNMP on your network.
- **NT domain:** Looks for devices in a domain you specify. Discovers members whether the computer is on or off.
- **LDAP:** Looks for devices in a directory you specify. Discovers members whether the computer is on or off.

UDD also supports some additional scanning and discovery methods.

Be aware that you must check either **Standard LANDesk agent** or **Network scan** before you can select one of the following methods:

- **IPMI:** Looks for servers enabled with the Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.

- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.
- **Intel* AMT:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel AMT** folder.

To automate unmanaged device discovery, you can schedule UDD discovery scans to occur periodically. For example, you could divide your network into thirds and schedule a ping sweep for one third each night.

If you schedule a discovery, the core server does the discovering. Unscheduled discoveries happen from the console that starts it.

Extended device discovery

The UDD tool also supports extended device discovery (XDD) scanning. XDD relies on a device agent (deployed via an agent configuration) that listens for ARP broadcasts and WAP signals on your LANDesk network. The XDD agent on a configured device then checks to see if the broadcasting device has the standard LANDesk agent installed. If the standard LANDesk agent doesn't respond, an ARP discovered device displays in the **Computers** group with reported information in the item list view, and a WAP device displays in the **Wireless Access Points** group with reported information in the list view.

Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

Use extended device discovery to discover firewalled devices

Be aware that the normal unmanaged device discovery methods usually can't discover devices that use a firewall, such as the Windows firewall that is built into Windows XP. The firewall typically prevents the device from responding to the discovery methods that unmanaged device discovery uses. Extended device discovery helps solve this problem by using network ARP traffic to discover devices.

Discovering unmanaged devices with UDD

It's easy to discover unmanaged devices with the basic UDD scan methods.

To discover unmanaged devices with UDD

1. In the unmanaged device discovery window (**Tools | Configuration | Unmanaged device discovery**), click the **Scan network** button.
2. Select the discovery option you want.
3. Enter a starting and ending IP range for the scan. You must enter a range for **Standard LANDesk agent discovery** (CBA) or **Network discovery** to work. The range is optional for **NT domain** and **LDAP**.
4. Enter a **Subnet mask**.
5. Click the **Add** button to add the scan you just configured to the task list.
6. In the task list at the bottom of the dialog, select the scans you want to run and click the **Scan now** button to scan immediately, or the **Schedule task** button to run the scans later or on a recurring schedule. The **Scan now** and **Schedule task** buttons only run scans you've added to the task list and that are selected.

7. Watch the Scan Status dialog for scan status updates. When the scan finishes, click **Close** in the Scan Status and Scanner Configuration dialogs.
8. Click **Computers** in the UDD tree to view the scan results.

Configuring Windows NT domain discovery

The Windows NT domain discovery option won't work unless you configure the scheduler service to log in to the domain with a domain administrator account.

To configure the Scheduler login account

1. Click **Configure | Services** and click the **Scheduler** tab.
2. Click **Change login**.
3. Enter a domain administrator username and password.
4. Click **OK**
5. Restart the scheduler service so the change takes effect. On the **Scheduler** tab, click **Stop**, and once the service has stopped click **Start**.

Using extended device discovery (ARP and WAP)

Extended device discovery (XDD) works outside the normal scan-based UDD discovery methods. The XDD agent can be configured and deployed to managed devices to use the ARP and/or WAP discovery methods. This section describes both discovery methods.

ARP discovery method

Managed devices configured with the XDD discovery agent for ARP discovery listen for ARP (Address Resolution Protocol) broadcasts and maintain a cache (both in memory and in a file on the local drive) of devices that make them. Networked devices use ARP to associate a TCP/IP address with a specific device network hardware MAC address. This communication happens at a very low level and doesn't rely on devices responding to pings or agent communication on specific network ports. Even heavily firewalled devices rely on ARP. Because of this, extended device discovery can help you find devices that normal discovery scans won't find.

When a new ARP broadcast is recognized by a device configured with the extended device discovery agent, the agents that heard the ARP broadcast wait two minutes for the detected device to boot and then each agent waits a random amount of time. The agent with the shortest random wait time pings the new device first, checking for LANDesk agents, and then the agent sends a UDP broadcast to the subnet to let the other agents know that it took care of the ping for that new discovered device. If you have multiple extended device discovery agents installed, this prevents devices from generating excess traffic by all pinging at the same time.

The ARP tables stored by the extended device discovery agent timeout after 48 hours by default. This means that every network device will be pinged once per time out period. Even devices that generate a lot of ARP traffic are only pinged once per timeout period.

Devices with LANDesk agents on them are assumed to be managed and aren't reported to the core server. Devices without LANDesk agents are reported to the core server as unmanaged devices. These devices appear in the **Unmanaged device discovery** window's **Computers** list. ARP-discovered devices show **True** in the **ARP Discovered** column. For ARP discovered unmanaged devices, XDD reports back the following information in the list view columns:

- IP Address
- MAC address
- First scanned
- Last scanned
- Times scanned

WAP discovery method

You can also configure managed devices to listen for wireless access point (WAP) devices on your network, and add any discovered WAP devices to the Wireless Access Points group in the Unmanaged device discovery tool.

For discovered WAP devices, XDD reports back the following information in the list view columns:

- Device name
- MAC address
- First scanned
- Last scanned
- Times scanned
- WAP status (Allowed, Rogue, Active exception)
- Signal strength (use to determine the approximate location of the WAP device)
- Encryption level (the encryption scheme used by the WAP device)
- Manufacturer

Reporting the MAC address

XDD uses the wireless detection API on devices running Windows Vista to obtain the device MAC address and display it in the list view. However, this capability is not supported on devices running Windows XP/SP2.

Configuring devices to use extended device discovery (ARP and WAP)

You can use the Agent configuration tool to configure some of your managed devices with the extended device discovery (XDD) agent so they can act as discovering devices that listen for ARP and WAP signals on the network.

You don't have to deploy extended device discovery to every managed device, though you can if you want to. Deploying the XDD agent to several devices on each subnet should give enough coverage.

To deploy the extended device discovery agent for ARP and/or WAP discovery

1. Click **Tools | Configuration | Agent configuration**.
2. Click the **New** toolbar button.
3. Enter a **Configuration name**.
4. In the **Agent configuration** dialog's **Extended device discovery** page, select one or both of the discovery methods you want to deploy.
5. Specify a setting for the discovery method(s) you've selected. You can select an existing setting from the drop-down list, or click **Configure** to edit a setting or create a new one for this agent configuration.
6. Finish specifying options on the agent configuration. For more information about any page, click **Help**.
7. Click **Save**.
8. Deploy the agent configuration to desired target devices on each subnet.

You can configure various extended device discovery settings for devices with the extended device discovery agent. This agent periodically synchronizes its settings with the core server.

To configure extended device discovery agent settings for ARP and/or WAP discovery

1. Click **Tools | Configuration | Unmanaged device discovery**.
2. Click the **Configure extended device discovery** toolbar button, and select which type of discovery method's settings you want to configure (ARP or WAP).
3. Specify the discovery method scan options as you like. For more information, click **Help**.

4. Click **OK** when done. The next time extended device discovery agents synchronize with the core server, your changes are applied.

Understanding IP address filtering with XDD

We don't recommend that you install extended device discovery on notebook computers, since they may connect to other networks that you don't want to monitor, such as hotel or airport networks. To help prevent discovery of devices that aren't on your network, the core server ignores IP addresses where the first and second IP address octets are plus or minus 10 from that of the core server. For example, if your core server's IP address is 192.168.20.17, extended device discovery on the core server will ignore addresses above 203.179.0.0 and addresses below 181.157.0.0.

You can disable this feature by adding the following DWORD registry key to the core server and setting its value to 0:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\Filter

You can set the Filter value to 1 to enable filtering again.

You can adjust the first and second octet monitoring ranges by adding the following DWORD registry keys to the core server and setting their values to the numeric range that you want monitored (the default is 10 for the first and second octets):

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold1
- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold2

FilterThreshold1 contains the range for the first octet and FilterThreshold2 contains the range for the second octet.

Working with devices found through XDD

Unmanaged devices found through extended device discovery's ARP discovery method appear in the **Unmanaged device discovery** window's **Computers** list. WAP Devices found through extended device discovery's WAP discovery method appear in the **Unmanaged device discovery** window's **Wireless Access Points** list.

From these lists you can perform the normal UDD options, such as moving them to other groups. Right-click a device to access its shortcut menu and use the available options.

You can also import and export extended device discovery exceptions. An exception is a device on the network that isn't manageable or that the administrator knows about but doesn't want extended device discovery to report on.

These exceptions are in a text .CSV file format that consists of comma-separated IP and MAC addresses, in that order, one pair per line. The exceptions export includes all exceptions stored in the database. The exceptions import replaces all exceptions stored in the database with the exceptions you include in the import file.

To export all extended device discovery exceptions

1. Click **Tools | Configuration | Unmanaged device discovery**.
2. Click the **Export extended device discovery exceptions from CSV file** toolbar button.
3. Choose a folder and give the file a name.
4. Click **Save**.

To import all extended device discovery exceptions

1. Create or update a comma-separated CSV file that contains the exceptions you want.
2. Click **Tools | Configuration | Unmanaged device discovery**.
3. Click the **Import extended device discovery exceptions from CSV file** toolbar button.
4. Click **Open**.

Maintaining ARP discovered device records

UDD stores devices found through extended device discovery in the core server's database. If you have a lot of unmanaged devices on your network, this data can grow very quickly. By default, this data is kept for 24 hours. You can customize how long devices found through extended device discovery stay in the database. After the number of days you specify, devices that haven't been rediscovered within that period will be deleted.

To configure the ARP discovery history

1. Click **Tools | Configuration | Unmanaged device discovery**.
2. Click the **Configure ARP discovery history** toolbar button.
3. Change the options you want. Click **Help** for more information.
4. Click **OK** when done.

Extended device discovery reports

There are several XDD reports in the **Reports** window (**Tools | Reporting / Monitoring**, click **Standard Reports | Unmanaged Devices**) that you can view.

Extended device discovery reports include:

- **ARP discovered machines:** Report of current unauthorized devices.
- **ARP discovered machines history:** History of unauthorized devices.
- **Current ARP discovered machines without the agent:** Current devices where the LANDesk agent is either disabled or not working.
- **History of ARP discovered machines without the agent:** History of devices where the LANDesk agent is either disabled or not working.
- **WAP All wireless devices:** Lists every discovered wireless access point (WAP) device irregardless of its status (Allowed, Rogue, Active exception).
- **WAP Allowed wireless devices:** Lists only those discovered WAP devices that are allowed.
- **WAP Discovering devices that detected a wireless access point:** Lists managed devices configured with the XDD agent to use WAP discovery that have actually detected and reported a wireless access point (WAP) device on your network.

- **WAP Rogue wireless devices:** Lists only those discovered WAP devices that are not allowed.

What happens when a device is discovered

When UDD or XDD finds an unmanaged device for the first time, it tries to identify the device type so it can add the device to one of the following groups:

- **Chassis:** Contains blade server chassis management modules.
- **Computers:** Contains devices discovered by UDD scanning methods (and the XDD agent's ARP discovery method)
- **Infrastructure:** Contains routers and other network hardware.
- **Intel AMT:** Contains Intel Active Management Technology-enabled devices.
- **IPMI:** Contains servers that have the Intelligent Platform Management Interface.
- **Other:** Contains unidentified devices.
- **Printers:** Contains printers.
- **Wireless Access Points:** Lists discovered WAP devices (found by the XDD agent).

These groups help keep the UDD list organized so you can more easily find the devices you're interested in. You can sort the device lists by any column heading when you click on a heading.

Moving devices to different groups

UDD may not categorize devices correctly and place them in the appropriate device groups in every instance. If this happens, you can easily drag misidentified devices to the correct group.

UDD tries to discover and report basic information about each device, including the following data that appears in the item list view in the right-hand pane of the tool window:

- **Device name:** The discovered device name, if available.
- **IP address:** The discovered IP Address. UDD always shows this. XDD does not.
- **Subnet mask:** The discovered subnet mask. UDD always shows this.
- **OS description:** The discovered OS description, if available.
- **MAC address:** The discovered MAC address, usually returned if the device has the standard LANDesk agent, NetBIOS, or if the device is on the same subnet as the core server or console that's doing the discovery.
- **Group:** The UDD group the device belongs to.
- **Standard LANDesk agent:** Shows whether the device has CBA on it. You can deploy other LANDesk agents directly to managed devices with CBA loaded.
- **All users:** Users logged in at the device being scanned, if available.
- **Group/Domain:** The group/domain the device is a member of, if available.
- **First scanned:** The date UDD first scanned this device.
- **Last scanned:** The date UDD last scanned this device. This column helps you find unmanaged devices that may not be on the network any more or that were recently found.
- **Times scanned:** The number of times UDD scanned this device.
- **AMT:** Whether the device supports Intel Active Management Technology.

Depending on the device, UDD may not have information for all columns. When UDD finds a device for the first time, it looks in the core database to see if that device's IP address and name are already in the database. If there's a match, UDD ignores the device. If there isn't a match, UDD adds the device to the unmanaged device table. Devices in the unmanaged table don't use a LANDesk license. A device is considered managed once it sends an inventory scan to the core database. You can't drag devices from UDD into the main console network view. Once unmanaged devices submit an inventory scan, they'll be removed from UDD and added to the network view automatically.

You can create custom groups to further categorize unmanaged devices. If you move a device to another group, UDD will leave that device in that group if UDD detects the device again later. By keeping the main **Computers** group organized and by moving devices you know you won't be managing with LANDesk into subgroups or other categories, you can easily see new devices in the **Computers** group. If you delete a group that contains devices, UDD moves the devices to the **Other** group.

You can quickly find devices matching search criteria you specify by using the **Find** toolbar field. You can search for information in a particular column, or in all columns. Search results appear in the **Find results** category. For example, use Find to group unmanaged computers that have CBA by searching for "Y" in the Standard LANDesk agent field.

You can also create an AMS alert when UDD finds unmanaged devices. In AMS, the alert name to configure is **Unmanaged device found**.

Deploying LANDesk agents to unmanaged devices

After you've discovered unmanaged devices using the scan and discovery methods described above, you can deploy LANDesk agents to those devices using one of the following methods:

- Push-based deployments using scheduled tasks and a domain administrative account you've configured for the scheduler. Works for Windows NT/2000/2003/XP devices.
- Push-based deployments using the standard LANDesk agent. If the devices have the standard LANDesk agent, you can do a push-based deployment.
- Pull-based deployment using a login script.

For more information on deploying devices, see Phase 4 in the *Installation and Deployment Guide*.

When organizing devices for agent deployment, you may find it easier to sort the unmanaged device list by the standard LANDesk agent to group for standard LANDesk agent device deployments and to sort by domain for scheduled task deployments.

When deploying to Windows XP devices

Windows XP's default setting forces network logins that use a local account to log in using the guest account instead. If you aren't using a domain-level administrative account and are using a local account for the scheduler service, scheduled tasks will fail because the scheduler service won't be able to authenticate. For more information, see "Phase 4: Deploying the primary agents to devices" in the *Installation and Deployment Guide*.

To deploy LANDesk agents to unmanaged devices

1. Click **Tools | Configuration | Agent configuration** and create a new configuration or use an existing one. From that configuration's shortcut menu, click **Schedule**.
2. Click **Tools | Configuration | Unmanaged device discovery**, and select the devices you want to deploy to. Drag the devices onto the **Scheduled tasks** window. If the **Scheduled tasks** window is a minimized tab, you can drag devices onto the **Scheduled tasks** tab, which opens the **Scheduled tasks** window.
3. If the devices don't have the standard LANDesk agent, click **Configure | Services**, and click the **Scheduler** tab. Make sure the scheduler account is one that will have administrative privileges on the devices you're deploying to.
4. Double-click the deployment script and set a start time. Click **OK** when you're done.
5. Watch the **Scheduled tasks** window for updates.

Restoring client records

Should you ever reset your core database and need to restore device data, you can use UDD to discover all devices on the network. You can then use the discovery results as the target for the "Restore client records" scheduled task.

If the devices have the standard LANDesk agent on them, this task has the devices send a full inventory scan to the core database that each device is locally configured for. The result of this task is those devices that have already been configured will be rescanned backed into the database and the devices will still be pointing to their correct managing core server. The task will fail on devices that haven't been managed by a core server.

To restore client records

1. Use UDD to discover unmanaged devices, as described earlier.
2. Click **Tools | Distribution | Scheduled tasks**.
3. In the **Scheduled tasks** window, click the **Schedule custom script** button.
4. Click **Restore client records**, and from its shortcut menu click **Schedule**.
5. From the UDD **Find results** tree, drag the computers you want restored onto the **Restore client records** task in the **Scheduled tasks** window.
6. From the **Restore client records** task's shortcut menu, click **Properties** and configure the task.
7. Watch the **Scheduled tasks** window for updates.

OS deployment

The LANDesk OS deployment and profile migration feature adds automated remote image deployment and device profile migration capabilities to your network. OS deployment and profile migration streamline new device provisioning and existing device migration, without requiring additional end user or IT interaction once the process starts.

You can schedule deployments and migrations to occur after hours, and by using the LANDesk Targeted Multicast technology to distribute images, you won't saturate network bandwidth by deploying the same image to multiple devices.

Note: For information on installing the OS deployment and profile migration component on your core server, and configuring your OS deployment and profile migration environment, refer to the *LANDesk Management Suite Installation and Deployment Guide*.

Read this chapter to learn about:

OS deployment

- "OS deployment overview" on page 226
- "OS image guidelines" on page 228
- "Customizing images with Setup Manager and Sysprep" on page 230
- "Agent-based deployment" on page 231
- "Creating imaging scripts" on page 232
- "Modifying scripts" on page 234
- "Multicasting OS images" on page 234
- "Viewing image status reports" on page 236
- "PXE-based deployment" on page 237
- "Using PXE representatives" on page 237
- "Booting devices with PXE" on page 239
- "Configuring the PXE boot prompt" on page 240
- "Using LANDesk managed boot" on page 240
- "Using the PXE boot menu" on page 241
- "Using the PXE holding queue" on page 242

OS deployment overview

The OS deployment (OSD) feature provides two methods of deploying OS images to devices on your network:

- **Agent-based deployment:** Uses the device's existing Windows OS and installed LANDesk agents to deploy images. For more information, see "Agent-based deployment" on page 231.
- **PXE-based deployment:** Allows you to image devices with empty hard drives or unusable OSes. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet. For more information, see "PXE-based deployment" on page 237.

If you use Microsoft's Sysprep utility to create your images, OS deployment creates customized SYSPREP.INF files and injects them into each device's image on a per device basis, customizing Windows computer names, domain information, and so on from the core database.

OS deployment includes a built-in imaging tool you can use to create images. OS deployment also supports third-party imaging tools that you may already be using, such as Symantec Ghost, PowerQuest DeployCenter, and Microsoft XImage.

OS deployment can image, deploy, and migrate from these boot environments:

- DOS
- Windows PE*
- Linux

* The LANDesk® PE Toolkit contains Microsoft® Windows® Pre-installation Environment software ("WinPE"), a third party product. In order to use the LANDesk® PE Toolkit, you must have a valid license to use WinPE. If you purchased a license to use WinPE from LANDesk, your use of WinPE is subject to the applicable terms and conditions of LANDesk's End User License Agreement for the licensing of LANDesk software.

Since some of these environments require licensed software, you'll need to provide copies of the licensed software for OS deployment to validate before you can use a particular environment.

WARNING: OS deployment (imaging) should be used with caution. Operating system deployment includes wiping all existing data from a device's hard drive and installing a new operating system. There is a substantial risk of losing critical data if the OS deployment is not performed exactly as described in this document, or if poorly implemented images are used. Before performing any OS deployment, we recommend that you back up all data in such a manner that any lost data may be restored.

OS deployment steps for Windows devices

When planning and implementing a Windows OS deployment operation, follow this sequence of steps:

1. If you're planning on using a DOS or Windows PE imaging environment and you haven't validated your licenses already, validate them by clicking the **Credentials** toolbar button in the **Operating system deployment** window. Insert the operating system CDs as prompted. You only need to do this once. The Linux boot environment doesn't require license validation.
2. (Optional) Run the Microsoft Setup Manager and Sysprep utilities on the device whose image you want to capture.
3. Create or reuse a image capture script in the **OS deployment window**.
4. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture. (Watch the **Custom Job Status** window updates for success or failure).
5. Create or reuse an existing image deployment script in the **OS deployment window**.
6. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
7. Target devices running Windows OSes and LANDesk agents will begin the image deployment job when scheduled (agent-based deployment).

8. Target devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

Read the relevant sections below for detailed information about each of these steps.

OS deployment steps for Linux devices

The following is a list of constraints imposed on Linux installations.

1. The root (/) partition must be of filesystem type ext2, ext3, or xfs.
2. The root partition CANNOT be contained in an LVM PV (Logical Volume Manager - Physical Volume), but MUST be a partition (physical, or extended in the drive's MBR (Master Boot Record).
3. The last partition is the only partition that can be expanded; therefore it, too, must be of filesystem type ext2, ext3, or xfs.
4. You must specify which partition the root partition is on (i.e., hda3 or sda2)

Note: Linux PE only supports IDE devices. Serial ATA and SCSI are not supported. If you want to image these devices you must use a third-party imaging tool

When planning and implementing a Linux OS deployment operation, follow this sequence of steps:

1. Create or reuse a **Linux configuration** image capture script in the OS deployment window.
2. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture. (Watch the Custom Job Status window updates for success or failure).
3. Create or reuse a **Linux configuration** image deployment script with the OS Deployment/Migration Tasks wizard.
4. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
5. Target devices running Windows OSes and LANDesk agents will begin the image deployment job when scheduled (agent-based deployment).
6. Target devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

OS image guidelines

You can create OS images with the LANDesk imaging tool or other imaging tools. When you run the OS Deployment/Migration Tasks wizard to create an imaging script, you are prompted to specify the image type and imaging tool. The wizard automatically generates command lines for the LANDesk imaging tool, Symantec Ghost 7.5, and PowerQuest DeployCenter 5.01.1.

Note: When you install the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT. If you want to use Microsoft XImage, you must copy the files XIMAGE.EXE and XMLRW.DLL into the \\<core>\ManagementSuite\OSD\imaging folder.

If you have a different imaging tool, you can supply the command line for it at the end of the wizard. If you specify a custom command line, the wizard will put your custom line in the right location in the script so that you don't have to edit the script manually.

Understanding the OS deployment imaging environments

When capturing or restoring an image, OS deployment boots the target device into an imaging environment. OS deployment supports these imaging environments:

- **DOS:** License verification requires a Windows NT 4 server CD and a Windows 98 CD. This 7 MB image is the smallest one, reducing the network bandwidth used. It potentially is the slowest at creating and restoring images, and has lower hardware compatibility than the other imaging solutions.
- **Windows PE:** License verification requires a Windows PE 2005 CD and a Windows 2003 SP1 CD. This 120 MB image is the largest one. It has the best hardware compatibility and is potentially the fastest at creating and restoring images. The imaging speed benefits from 32-bit drivers and applications. This imaging environment also supports Microsoft's imaging tools. For more information on how the Windows PE environment works, see "Understanding the Windows PE preboot environment" on page 619.
- **Linux:** No license verification required. This 37 MB image typically has mid-range compatibility and speed. Since it doesn't require any license verification, it also may be one of the most convenient imaging environments.

Note that the imaging environment you choose is independent of the OS you are imaging. For example, the Linux imaging environment has no problems imaging Windows operating systems.

Validate the DOS and Windows PE boot environments by clicking the **Credentials** toolbar button in the **Operating system deployment** window. Insert the operating system CDs as prompted. You only need to do this once. The Linux boot environment doesn't require license validation. The validation dialog also lets you change the **Default preboot environment** for devices in the PXE holding queue. Devices in the holding queue will boot into the environment you select. Your choices are limited to boot environments you have validated.

Image filenames

You should give your images unique filenames. Deploying different images with the same filename simultaneously on the same subnet can cause problems. Depending on how an imaging utility names image files and the imaging environment you're using, (DOS with multi-file Ghost images, for example), you may only have five unique characters in your filename once it is converted to a DOS 8.3 name format.

When capturing images, the LANDesk imaging tool for DOS, Windows, and Linux uses the last six characters of the computer name, followed by a two-digit image number for each file in the image. If you're capturing images from multiple devices at the same time and the last six characters of the computer name aren't unique, you'll experience errors during the capture process.

Symantec Ghost and PowerQuest DeployCenter generally use the first eight characters of the computer name for the image filename, which must also be unique for simultaneous image capture to work correctly.

When capturing images from multiple devices, you have two ways of ensuring that your images have unique names:

- Image one device at a time, renaming each image as it's created.
- Before running the job, ensure that the last six characters (LANDesk imaging tool) or first eight characters (Ghost and DeployCenter) of your Windows computer names are unique.

LANDesk agents and images

You should not include the LANDesk agents in your images. If you use a Sysprep image, OS deployment will install the LANDesk agents on the Windows-based OS after the image is restored.

If your Windows-based non-Sysprep images include LANDesk agents, you will need to delete the LDISCAN.CFG file from the root of the hard drive before imaging. You will also need to delete these keys:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

If you leave these in the image, all devices using the image will have the same core database entry. Alternatively, if you have non-Sysprep images that already have LANDesk agents on them, you can enable the **Reject duplicate identities** option on the **Duplicate device ID** dialog (**Configure | Services | Inventory | Duplicate ID**).

Partitions and images

By default, when OS deployment restores an image on a target device, it deletes any preexisting partitions on that device.

The LANDesk imaging tool supports single-partition and multiple partition images (up to four partitions). In the Linux PE environment, when using the LANDesk imaging tool, you can only deploy/capture one partition at a time.

Non-Windows images

You can use OS deployment to deploy almost any image your imaging tool supports, not just Windows-based images. When deploying non-Windows or non-Sysprep images, make sure you do not select the **Image is Sysprepped** option in the new configuration dialogs.

Customizing images with Setup Manager and Sysprep

You can use Microsoft's Setup Manager and Sysprep utilities when deploying Windows 2000/2003, Windows XP, and Windows XP x64 Edition images. Sysprep customizes a Windows installation so that when the OS reboots, it looks for an answer file (SYSPREP.INF) and reconfigures itself for the new device. Setup Manager creates the SYSPREP.INF answer file that Sysprep uses.

Before creating OS deployment scripts, you should run Microsoft's Setup Manager (SETUPMGR.EXE) and create a SYSPREP.INF answer file for the images you're deploying. You can then use this file as the basis for any OS deployment scripts you create by selecting the **Use existing SYSPREP.INF file as a template** option on the **Specify Sysprep file information** page of the wizard. Any OS deployment script settings you make in the wizard override the equivalent options in the template SYSPREP.INF file.

Using Sysprep on your Windows 2000/XP images allows OS deployment to query the core database for each device you're deploying and to migrate certain user settings, such as:

- Windows computer name
- GUID (the unique identifier used to identify devices in the core database)

You can also set these options globally for images you deploy:

- Time zone
- Volume license key
- Registered name and organization
- Workgroup/Domain/LDAP Organizational Unit (OU)

OS deployment uses information from the core database and from the image deployment script to create a custom SYSPREP.INF for each device you're imaging. OS deployment then injects that SYSPREP.INF into each device's image.

Creating a Sysprep image

To create an image that uses Sysprep

1. On the device whose image you want to capture, make configuration or customization changes to prepare it for imaging.
2. At the root of the device's hard drive, make a c:\sysprep folder.
3. From a Windows 2000 or Windows XP installation CD, open \Support\Tools\DEPLOY.CAB and copy **SYSPREP.EXE** and **SETUPCL.EXE** to the sysprep folder you created.
4. Open a DOS command prompt and change to the sysprep folder. Run Sysprep. If you don't use the reboot option, you'll need to shut down the device from the Start menu once a message appears requesting that you shut down.
5. Boot to DOS and run your imaging tool manually.

For more information on Setup Manager and Sysprep

Refer to Microsoft's Web site for official documentation about the Setup Manager and Sysprep utilities. Sysprep has many powerful features you can use that are beyond the scope of this document.

Agent-based deployment

You can use the agent-based deployment method to deploy OS images to devices running Windows 98, Windows 2000, or Windows XP.

For information on the other method of image deployment, see "PXE-based deployment" on page 237.

Prerequisites

If you're not using PXE to deploy images, devices must meet the following criteria:

- Be in the core database if you have multiprocessor images.
- Have the standard LANDesk agent, Enhanced Software Distribution agent, and Inventory agent loaded. OS deployment uses the Enhanced Software Distribution agent to distribute images. If you'll be multicasting images, you also need to have the Targeted Multicasting agent loaded.

What happens during an agent-based deployment

1. The core server connects to the device and runs any preconfiguration commands you specified in the image deployment script.
2. OS deployment uses the software distribution agent to distribute a virtual boot partition file to the device and modifies the boot sector to boot from this file, then reboots the device.
3. The device boots to DOS or Windows PE (depending on your choice), detects and loads a network driver, then retrieves and installs the image file from the image server.

For non-Sysprep images, the device reboots after the imaging completes. OS deployment considers the job complete after this reboot.

For Sysprep images, agent-based deployment continues in this manner:

4. Before rebooting and loading the image, the DOS or Windows PE agent replaces SYSPREP.INF with a customized file for that device.
5. The imaged device boots and customizes itself based on what is in the SYSPREP.INF file.
6. For Windows images, any post-image commands you specified in the image deployment script are run from the RunOnce registry key.
7. For Windows images, OS deployment runs WSCFG32.EXE using your default device agent configuration to reinstall the LANDesk agents.

Creating imaging scripts

LANDesk OS deployment provides the OS Deployment/Migration Tasks dialogs that let you create and manage both imaging (image capture and image deploy) scripts and profile migration scripts.

With the OS deployment tool you can create scripts that perform the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost, PowerQuest, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a user-initiated profile migration package that can be run locally at individual devices.

- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files to target devices).
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches on devices).

Once you have created a script, you can schedule it to run on devices by using the **Scheduled tasks** tool.

Creating user-initiated profile migration packages

From the OS Deployment/Migration Tasks wizard, you can also access the Collection Manager dialog that lets you create a user-initiated profile migration package (a self-extracting executable file) that can be distributed and run on devices for user-initiated profile migration. For more information, see "Creating user-initiated profile migration packages" on page 279.

If you are deploying an image to PXE-enabled devices, you can add image deployment scripts to the PXE DOS boot menu. This menu is DOS-based and appears on the device during a PXE boot. For more information, see "Using the PXE boot menu" on page 241.

To run the OS Deployment/Migration Tasks wizard

1. Click **Tools | Distribution | OS deployment**.
2. In the **Operating system deployment** window, right-click **My Scripts** and then click the script type you want to create in the shortcut menu to open the wizard. Or, in the window, click the toolbar button for the script type you want to create.
3. Configure the script as necessary. Once complete, the script appears in the **My scripts** group in the **Operating System Deployment** window.

Administrators (users with the LANDesk Administrator right) can copy scripts to user subgroups in the **User scripts** group.

Additional notes on scripts

- Script names need to follow Windows file naming conventions. The wizard uses the script name you enter as the filename. If you use characters that aren't allowed in Windows filenames, you'll get an error about using invalid characters.
- All scripts are stored on the core server, in the \\<core>\LDMain\Scripts directory. If you have multiple consoles, the scripts will appear in the Manage Scripts window of each console.
- The wizard restores the settings on each page from the last script you created. If you change the script type from an imaging task to a profile migration task or a DOS task, the wizard clears the remembered settings.

About Generic DOS tasks scripts

- DOS scripts reboot the selected target devices and run the commands you've specified. These remote commands are sent one line at a time.
- DOS scripts run from the virtual boot partition and go through the same network detection process as normal OS distributions do.

- The "Abort this job if any command fails" option stops execution if one of the commands returns a non-zero DOS errorlevel code. You can view DOS task status in the Custom Job window or with a report.
- For more information about script commands, see Using Custom Scripts, a whitepaper located at <http://kb.landesk.com>.

Modifying scripts

You can modify your scripts at any time, either by reopening the configuration dialog and making changes, or by modifying the script directly in its .INI file and modifying any existing Sysprep settings in its associated .INF file.

Note: With DOS scripts, the only changes you should make are between the REMPINGx=DOS and REMEXECx=reboot.com lines. The other lines in the script manage the virtual boot partition files and boot process.

To modify a script via the dialogs

1. Click **Tools | Distribution | OS Deployment**.
2. Right-click the script and click **Edit** in the shortcut menu (or double-click the script).
3. Advance through the wizard, making your changes.

To modify a script via an .INI file

1. Click **Tools | Distribution | OS Deployment**.
2. Right-click the script and click **Advanced edit**. The script's .INI file opens in Notepad. If this script has Sysprep settings associated with it, the SYSPREP.INF file also opens in Notepad.
3. Make your changes
4. Save the file(s).

Where .INI and .INF files are saved

.INI files are saved to the \\<core>\LDMain\Scripts directory. .INF files are saved to the \\<core>\LDMain\LANDesk\Files directory.

Multicasting OS images

This section discusses deploying images using the LANDesk Targeted Multicast technology. Multicasting is slower than a single distribution. Multicasting throttles bandwidth and stages the image on the target device's hard drive. However, multicasting to four or more devices will usually save enough bandwidth to make this worth it.

Targeted Multicasting supports only single-partition images, not multiple-partition images. Also, when using Targeted Multicasting with OS deployment, images can span up to 10 files.

When multicasting images, the image file is cached on the device before being restored. Your hard drive must have enough space for the image file and the restored files.

Before using multicasting with OS deployment, make sure the multicasting components are in place on the subnet to which you are distributing/deploying image files. Multicast OS deployments may fail if you don't specify domain representatives for each multicast domain in the console's **Multicast Domain Representatives** group. Multicasting requires LANDesk Management Suite 6.62 or higher agents on devices, and a LANDesk Management Suite 6.62 or higher multicast domain representative on the subnet.

If you try to multicast to a subnet that does not have a Multicast Domain Representative, the deployment will start but it will not be able to finish, and you will have to create an OSD boot floppy. For more information, see "Creating an imaging boot disk" on page 606. If your routers forward UDP-directed broadcasts, and there will be Windows devices that can act as multicast domain representatives on the subnet you're deploying the image to, you should be fine using Targeted Multicasting without designating multicast domain representatives. If your routers don't forward UDP-directed broadcasts, you must manually select your multicast domain representatives for each subnet, making sure the representatives you choose aren't among the devices you're deploying images to.

You can manually specify which devices will be multicast domain representatives by adding devices to the **Configuration | Multicast domain representatives** group in the console.

Make sure you don't image any multicast domain representatives in a subnet, because the imaging will fail and leave the devices in an unusable state.

You can throttle multicasts by changing the **Minimum number of milliseconds between packet transmissions** option in the **Configure advanced multicast options** page of the OS Deployment/Migration Tasks wizard.

WARNING: If your Multicasting environment isn't configured correctly and the Targeted Multicasting fails, all target devices may be unbootable unless you follow the directions above.

Setting the Maximum Packet Size for a Targeted Multicast with OSD

If multicast fails with distribution jobs, it may be because the maximum transmission unit (MTU) size on your network is fragmenting packets. Follow the steps below to adjust the MTU that multicast uses.

To set the Maximum Packet Size to 512 bytes for a Targeted Multicast script

1. Click **Tools | Distribution | OS Deployment**.
2. From the script's shortcut menu, click **Edit**.
3. In the Multicast section of the script, add the following line at the end of the section.

```
MAX_PACKET_SIZE=512
```

This string will set the Maximum Packet Size for the Targeted Multicast to 512 bytes. Maximum Packet Size can be set to between 256 and 1464 bytes. A setting above this range, or no setting at all, will force the default setting of 1464. A setting below this range will default to 256 bytes.

4. Save and close the script.

WARNING: The MAX_PACKET_SIZE setting must be at least 28 bytes smaller than the Maximum Transmission Unit (MTU for the network the package is being distributed on. This is determined by adding the size of the IP header (20 bytes) and the UDP header (8 bytes) that are sent with each packet of data. Setting the Maximum Packet Size higher than this limit will cause your distribution to fail.

Viewing image status reports

The device being imaged sends status updates to the core server. You can track status in the Custom Job window or with a report. As OS deployment sends imaging commands to devices, the commands appear in the Custom Job window. Devices being imaged send status updates for each script command that is sent. If image deployment fails for some reason, you can see the command that failed.

Common reasons why imaging fails include:

- Partition corruption
- Problems the imaging tool can't handle
- Network adapter auto-detection can't find a network adapter
- Undetectable network adapter you specified doesn't work. (If the network adapter driver you specify fails to load, that device will be stuck at the DOS prompt). You'll have to manually reboot it.

OS deployment creates a status report for each job, showing if it failed or succeeded on targeted devices.

To view a status report

1. Click **Tools | Reports | All LDMS reports**.
2. Select the **OS deployment success rate** report.
3. From the list of log files, select the file for the job you're interested in viewing.
4. Click **Run**.

At the top of each report will be any jobs that failed on individual devices. Reports also show the details of each job, such as:

- **Machine Name:** For devices already scanned into the core database, this name will be the device name assigned to the device. For PXE-booted devices that haven't been inventory scanned, the machine name will be a MAC address. You can use a .CSV file to import MAC addresses into the core database. For more information, see "Using CSVIMPORT.EXE to import inventory data" on page 607.
- **Duration:** The amount of time each command took to complete.
- **Commands:** Each command that ran as part of the script. If a job failed, this column shows which command caused the failure.

PXE-based deployment

OS deployment supports PXE booting and image deployment. PXE-based deployment provides another method (in addition to agent-based deployment) of automated remote imaging of devices on your network. With PXE support, you can boot both new and existing PXE-enabled devices and either execute an OS deployment script at the device from a custom PXE DOS boot menu, or scan devices into your core database and then schedule an image deployment job with the **Scheduled tasks** tool.

PXE-based deployment is a quick and easy way to image devices in a variety of situations. For example:

- Initial provisioning of new devices
- Imaging devices in a test or training lab
- Re-imaging corrupted devices

LANDesk offers several options for using PXE to deploy OS images. For more information, see "Understanding the PXE boot options" on page 240.

PXE protocol basics

PXE (Preboot Execution Environment) is an industry-standard networking protocol that enables devices to be booted and imaged from the network, by downloading and installing an executable image file from an image server, before the device boots from the local hard drive. On a PXE-enabled device, the PXE protocol is loaded from either the network adapter's flash memory or ROM, or from the system BIOS.

PXE uses the following communication standards: DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol), and MTFTP (Multicast Trivial File Transfer Protocol).

When a PXE-enabled device boots up, it sends out a DHCP discovery request. If a DHCP server implementing PXE is found, the server assigns an IP address to the device and sends information about available PXE boot servers. After completing the DHCP discovery process, the device contacts the PXE server and downloads an image file through TFTP. The imaging script is then executed, loading the OS image from the imaging server onto the device. The image file is referenced by an OS deployment script.

If you want to learn more about PXE and its underlying technologies and functionality, read the PXE Specification v2.1 located at <http://www.intel.com/labs/manage/wfm/wfmspecs.htm>.

Using PXE representatives

PXE support software is installed on your core server as part of the normal OSD installation. However, to enable PXE support, you must first deploy a PXE representative on each subnet of your network where you want PXE support available. PXE representatives provide scalability on your network by deploying OS images to devices in their respective subnets.

Devices on each subnet use normal PXE query and file transfer methods to communicate with their resident PXE representative, which communicates with the core server using Web services (HTTP).

Disable other PXE servers

If there is *any* other PXE server currently running on your network, you must first disable it in order to use LANDesk PXE support.

Deploying PXE representatives

You need to deploy one PXE representative on each subnet where you want to provide PXE boot support. You set up a PXE representative by running the PXE Representative Deployment script on the selected device. This predefined script is available in the Schedule Script dialog (**Tools | Distribution | Scheduled tasks |** click the **Schedule custom script** toolbar button).

You can have multiple PXE representatives on a subnet to help with load-balancing. When this is the case, the first PXE representative to respond to a device's request is the one that will be used to communicate with the core server.

Note: We recommend that you do *not* deploy a PXE representative on your core server.

There are no special hardware requirements for the device you select to be a PXE representative, but it must meet the following software requirements:

- **Operating system:** Windows NT 4, Windows 2000, or Windows XP.

For Windows NT and 2000, ensure that the Microsoft MSI service is running (XP includes MSI by default). If you have installed the latest service pack for either OS, MSI service should be running. Otherwise, you can deploy it to the target PXE representative from the console by following these steps: Click **Tools | Distribution | Scheduled tasks**, click the **Schedule script** toolbar button, select the **MSI service deployment** task, click **OK**, drag the target devices to the window, and click the **Set start time** button to schedule the MSI service deployment.

- **Installed LANDesk agents:** Enhanced Software Distribution agent and Inventory Scanner agent. For information about installing agents, see the *Installation and Deployment Guide*.

To deploy a PXE representative

1. In the console, click **Tools | Distribution | OS Deployment**.
2. In the **Operating system deployment** window, click the **All other scripts** tree item. From the **PXE representative deployment** script's shortcut menu, click **Schedule**.
3. In the console's network view, select the target device on which you want to install PXE services (in this case the core server).
4. Drag and drop the selected device to the **PXE Representative deployment** task in the **Scheduled tasks** window.
5. From the **PXE Representative deployment** task's shortcut menu, click **Properties** and finish configuring the task.

Updating PXE representatives

If you modify the PXE boot option settings (on the **Configure | Services | OS deployment** tab), you need to update all of your PXE representatives by re-running the PXE Representative Deployment script to propagate those changes to PXE representatives on each subnet. However, re-running the script is not necessary if you simply move PXE proxies from the Available proxies list to the Holding queue proxies list. For more information about the PXE holding queue, see [Using the PXE holding queue](#) later in this chapter.

To update or remove a PXE representative

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar icon.
2. To update a PXE proxy, select the **PXE Representative Deployment** script from the list, then click **OK**. Or, to remove a PXE proxy, select the **PXE Representative Removal** script, then click **OK**.
3. Drag and drop the target device(s) to the appropriate task in the **Scheduled tasks** window, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Booting devices with PXE

When a PXE-enabled device boots, the following occurs:

1. The PXE-enabled device sends out a query for PXE services running on a PXE representative on the network.
2. If a PXE representative exists on the subnet, it responds and tells the device to continue to boot using PXE.
3. A PXE boot session is initiated on the device and the PXE boot prompt displays. The default prompt message displays for four seconds and says "Press F8 to view menu." (You can modify these PXE boot prompt settings on the **Configure | Services | OS deployment** tab.)
4. If the **F8** key is pressed before the countdown expires, a preliminary PXE boot menu appears, allowing you to choose from the following boot options:
 - **Local boot:** The device boots to the local hard drive. If no OS is present, an error message appears.
 - **LANDesk managed boot:** The device is added to the console's network view (displays the device's MAC address), where you can schedule an OS deployment script to run on it.
 - **LANDesk boot menu:** The device displays the boot menu you created with the PXE Boot Menu tool, and you can select an OS deployment script to run on it. For more information, see "Configuring the PXE boot prompt" on page 240.
5. If you don't press the **F8** key before the countdown expires, the device will use the default boot option. The default boot option is determined by the following conditions:
 - If the device detects a scheduled imaging job for itself in the core database (either a failed or pending job), the default boot option becomes **LANDesk managed boot**.
 - If the device does *not* detect an image job for itself, the default boot option becomes **Local boot**.
 - The **PXE DOS menu will never become the default boot option**.
6. The scheduled OS deployment script runs on the device.

Understanding the PXE boot options

This section provides information on configuring the PXE boot prompt, and how to use the following PXE boot options:

- LANDesk managed boot
- PXE Boot menu
- PXE holding queue

Configuring the PXE boot prompt

You can control how the PXE boot prompt behaves when devices attempt to PXE boot.

When a PXE-enabled device boots up, a DHCP request attempts to initiate a PXE session by looking for a server (or proxy) running PXE services software (PXE and MFTFTP) services. If the device discovers a PXE server, the PXE boot prompt displays on the device for a specified number of seconds. By pressing the F8 function key during this countdown, you access the PXE boot menu and can select an OS image to deploy on the device.

Note: If you have PXE representatives running on subnets of your network, and you want to implement PXE boot prompt changes to any of those proxies, you must run the PXE Representative Deployment script on the proxy.

To configure PXE boot prompt options

1. Click **Configure | Services**, then click the **OS deployment** tab.
2. Enter a value (in seconds) in the Timeout option. The default value is 4 seconds. The maximum number of seconds you can enter is 60 seconds.
3. Type a message in the Message text box. The default message is "Press F8 to view menu." The maximum number of characters you can type is 75 characters.
4. Click **Apply** to save your changes, or click **OK** to save your changes and close the dialog.

To implement PXE boot prompt changes to a PXE representative

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar button.
2. Select the **PXE representative deployment** script from the list, then click **OK**.
3. Drag and drop the PXE representative from the network view onto the task.
4. Select the **PXE representative deployment** script, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Using LANDesk managed boot

LANDesk managed boot is the default boot option when a PXE-enabled device boots and detects a failed image deployment script or failed DOS task script for it in the core database. You can also select this boot option manually at the device when the boot option menu appears.

Because it allows unattended deployment, LANDesk managed boot is useful for pre-targeting devices for imaging. For example, you could pre-target new devices for a particular OS image even before they arrive by importing a .CSV file containing device MAC addresses into the core database. For more information, see "Using CSVIMPORT.EXE to import inventory data" on page 607.

To pre-target devices with the LANDesk managed boot option

1. Before the PXE-enabled devices are connected to the network, add their identifications to the core database by importing a .CSV file.
2. Schedule an image deployment job for the devices.
3. The imaging job fails because the devices are not yet connected to the network.
4. Connect the devices to your network and boot them.
5. The devices detect a failed imaging job and default to the LANDesk managed boot option.
6. The previous failed image deployment job automatically launches and images the target devices.

Using the PXE boot menu

The PXE boot menu lets you interactively select an image deployment script for a device without having to schedule an image deployment job. This method might be useful when you have to re-image corrupted devices. Before using the PXE boot menu, you must first configure it by adding the OS deployment scripts you want to display in the menu.

You build the PXE boot menu system by creating directories and placing pre-configured OS deployment scripts in those directories. The script's description appears as a menu item in the PXE boot menu on the device.

To configure the PXE boot menu

1. Click **Tools | Distribution | PXE boot menu**.
2. To add a new directory or subdirectory to the menu system, click the **New** toolbar button (or right-click the parent directory and select **New**).

Note: Subdirectories can extend four levels from the top directory.

3. Type a name for the directory. For example, the directory name could describe the OS platform or version number of the images contained in that directory. You can also change the name of the directory at any time by clicking the **Rename** toolbar button (or right-clicking the directory and selecting **Rename**).
4. Click **Tools | Distribution | Manage scripts**, then drag and drop image deployment scripts to the appropriate directory in the PXE Boot Menu window.

Note: A maximum of 18 scripts can be placed in each directory.

5. To save the PXE boot menu, click the **Update** toolbar button. (Note that you must click the Update button here in the console if you want changes to appear in the PXE boot menu on PXE devices when they boot.)

To access the PXE boot menu from a device

1. Boot a PXE-enabled device.
2. When the PXE boot prompt displays, press the **F8** key before the countdown expires. Select **PXE DOS menu**. The menu system that you configured in the console's PXE Boot Menu window appears.
3. To open a directory and view its subdirectories and images, type the number of the directory and press **Enter**. Navigate the menu system and find the image you want deployed on the device. You can press **B** to go back one level, or press **X** to exit the menu system.

Note: If you exit the menu system without making a selection, the device will wait for a scheduled imaging job from the core server.

4. To select an OS image (referenced in an OS deployment script), type the number of the script and press **Enter**. The script runs and the image is loaded on the device.

Using the PXE holding queue

The PXE holding queue is another method for remotely deploying OS images to PXE-enabled devices. This method is especially useful in these situations:

- In a controlled lab environment where you frequently need all devices re-imaged with an identical image.
- For imaging "bare-metal" devices in a lab that can then be moved into their appropriate production environment.

By designating a subnet's PXE representative as a PXE holding queue, all the PXE-enabled devices on that subnet will be automatically added to the PXE holding queue in the console's network view when they PXE boot. You can also add a device to a PXE holding queue by scheduling the PXE - Add to Holding Queue script on the device, or by copying the device directly into the PXE holding queue group in the network view. Devices can then be scheduled for an image deployment job.

To configure a PXE holding queue

1. Set up PXE representatives on your network.
2. Click **Configure | Services**, then click the **OS deployment** tab.
3. Select and move PXE representatives from the Available proxies list to the Holding queue proxies list.
The Available proxies list shows all available PXE representatives on your network, identified by device name. This list is generated by running an inventory scan that detects PXE software (PXE and MTFTP) protocols running on the device. The inventory scan is run automatically whenever a PXE representative is initially set up.
4. Click **Reset**. The Reset button forces all PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the PXE holding queue in the console's network view. These devices can then be scheduled for an imaging job.

Note: The Reset button is enabled when you select a PXE representative in the Holding queue proxies list.

5. Click **Apply**, then **OK** to save your changes and close the dialog.

The next time a device on that subnet boots, it will be added to the PXE holding queue object in the console's network view.

To deploy an image to a device in the PXE holding queue

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar button.
2. Select an OS deployment script from the list, then click **OK**.
3. In the console's network view, open the **PXE holding queue** object, then select the target devices you want to deploy the image to.
4. Drag and drop the selected devices to the **Scheduled tasks** window, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Troubleshooting

Invalid OEM drivers in a Windows PE image will reset a device's boot environment and cause OSD tasks using that image to fail

If you add an invalid OEM driver to a Windows PE image and use that image for a task on a device, the device will boot into the Windows PE from that point onwards and the OSD task won't run. If this happens, do the following to fix the Windows PE image and restore the normal boot environment:

1. On the OSD toolbar, click the **Manage the drivers in the Windows PE image** button.
2. Remove the invalid OEM driver from the PXE-based Windows PE file (under \\pxeserver\...\PXE\System\images\peboot.img) and agent-based Windows PE file (under \\coreserver\ldmain\landesk\vboot\ldvpe1.img).
3. PXE boot the device to the modified Windows PE image by selecting the "LANDesk Managed WinPE" option.
4. Once the image boots, run this command: Diskinfo fix
5. Restart the device and it will boot to the previous OS normally.
6. Execute the OSD task what you scheduled.

Provisioning

- [Introduction](#)
- [The provisioning interface](#)
- [Steps for provisioning a server](#)
- [Provisioning bare metal devices](#)

Introduction

LANDesk server provisioning lets you define all the attributes and features of your servers before they are introduced into your environment. Provisioning uses automation to apply this set of attributes and features to the servers. Provisioning reduces server downtime and makes sure servers are reliable and predictable when they go into your production environment. You can access the provisioning history of each server to find out when and with what it was provisioned, and, if necessary, return it to a previous state. Provisioning supports blade, rack mount, and tower servers, and runs on both Windows and Linux. There is no difference in the way you create templates for either operating system.

Provisioning consists of a series of actions to be executed on a target server. **Actions** are the fundamental unit of provisioning. A **template** is a collection of actions that are executed in a pre-defined order. LANDesk also provides several pre-built provisioning templates to get you started, optimized to work with specific hardware configurations, such as several popular Dell™ and Hewlett-Packard systems. You can combine these provisioning templates with your own master templates, or run these templates with little modification to generically provision a specific Dell- or HP-brand device. You can split the provisioning tasks the way you split the work when setting up a system manually.

Provisioning works equally well on new servers or dynamic servers. You can provision new servers with the precise configuration you require, setting up the configuration before the new server has even arrived. You can use provisioning to reconfigure a server from one purpose (such as an application server) to another (such as mail server), thus changing a server's base function to handle your organization's changing demands.

You can use alerting to let you know when provisioning events occur. For more information, see ["Alerting."](#)

Provisioning agent

The center of provisioning is the agent `ldprovision`, located in the `/ldlogon/provisioning` folder. This agent consists of small applications for each action. The agent resides on the target server. It is placed there through a PXE server or a physical boot media such as a USB drive or a CD. The agent requests a template's configuration settings from a web service on the core server, checks the preboot type tag to ensure it is running in the correct preboot environment, performs the actions in the order designated in the configuration, reboots the device (if necessary), injects a version of itself into the target OS so it can continue working when the real OS loads after the reboot, and sends feedback to the web service on the core. The agent spans any reboots required, immediately moving to the next action after the reboot. Most provisioning work can be done before you receive a new server. You can create a template and create the task for the template to run on the new server. The task will not run until the provisioning agent runs on the new server.

To use full provisioning, users require two user rights. These are the Provisioning - Schedule right and the Provisioning - Configuration right. These rights are automatically enabled for any users with Administrator rights, and can be enabled for any users. For more information, see "[Role-based administration](#)."

Preboot tools

Provisioning requires the ability to boot the server prior to putting an operating system on it. This can be accomplished through PXE or CD/USB drive. PXE is the most convenient way to boot many computers at a time into the same preboot environment. CD or USB drives are highly portable and guarantee that the computer running the preboot environment is the one the administrator intended to provision.

The preboot environment (PE) includes an operating system complete with video, networking, a small inventory scanner, and an agent capable of receiving files and executing commands. This agent executes an imaging tool or scripted install tool to install the OS on the server. The agent initiates the provisioning process. Provisioning supports the Windows and Linux preboot environments.

It is recommended that you install the new operating system using the same type of preboot environment that you are installing. For example, install Windows using the Windows PE and install Linux using the Linux PE. This is because Windows PE does not support EXT2, EXT3, or Reiser file systems, and Linux, though it supports NTFS, may cause problems with misconfiguration, particularly if PXE is isolated from the production network.

You do not need unique boot media for each client system; you can re-use the boot media for other servers.

Differences between OS deployment and Provisioning

Provisioning is much more broad than its predecessor, OS deployment. While OS deployment can be part of the provisioning process, it only encompasses one part of provisioning. Provisioning encompasses the start-to-finish process of preparing a server for safe and secure usage in your environment. The table below shows how provisioning is different from OS deployment.

OS deployment	Provisioning
Driven from the core	Driven from the target server
Work done after server arrives from factory	Most work can be done before server arrives
Encompasses only the OS deployment step of the provisioning process.	Comprises the end-to-end sequence of building a server
Requires one entire image; cannot be broken down	Comprised of smaller templates, which can be modified or swapped out at template level

The provisioning interface

The provisioning interface in the Web console contains three panes. It also contains a toolbar (some buttons are described below).

The left pane consists of all available templates, organized under the folders Public, My templates, and Other users. Each folder's contents are described in the list below:

- **Public:** Both your templates and templates marked as public.
- **My templates:** Templates that you have created. Only you and administrative users can access these templates
- **Other users** (administrative users only): A list of users and their templates.

Public templates are created by users with Administrator rights and are viewable by all users. My templates are visible by others but can only be edited by the template's creator or users with Administrator rights. Each time you use a template not marked public, the instance of the template is locked in history. This instance cannot be deleted, but it can be hidden.

The right pane displays the selected template's properties, including a list of other templates that include the selected template. It also displays the selected group's properties. It contains buttons for creating new templates and template groups, editing and cloning existing templates, creating shortcuts to existing templates, and scheduling templates.

The bottom pane consists of several tabs that open additional provisioning tools.

- **Scheduled tasks:** Opens the global scheduler, allowing you to view provisioning and other management tasks, including the ability to schedule tasks and view the status of tasks.
- **Boot media:** Lets you configure and create boot media.
- **Export templates:** Exports the selected template in XML format. You can export templates to other cores or to send to colleagues in other organizations.
- **Import templates:** Imports the XML of a template into the currently selected template.
- **Install scripts:** Lets you make installation scripts available for use in creating scripted installation actions and deploy image action in templates.
- **Public variables:** Lets you view and set global variables that apply to all provisioning templates.

- **Update templates:** Lets you configure settings for provisioning templates, the template download location, and proxy server settings. Lets you download and import templates from LANDesk.
- **Add drivers:** Lets you add or remove drivers to a WinPE image.

If you double-click a template, the Template view opens. From this view, you can modify the action list (add or delete actions, modify the action order, and so forth). You can modify variables applying specifically to this template, view and modify the list of templates included by this template, or the list of templates that include the template. You can make a template public, view its history (when the template was executed), and view or modify the template's XML code.

New template

The **New template** button is the starting point for creating a new template. To modify a template, select the template and click the **Edit** button on the toolbar. To remove a template, select it and click the **Delete** button. You can only delete templates that have never been used.

New group

You can use provisioning groups to organize your templates in ways to suit your needs. For example, you could create groups based on specific vendors, and additional subgroups based on server models. You can create subgroups up to six layers deep.

Add shortcut

The **Add shortcut** button opens the Provisioning select dialog, from which you can select a template to create a soft link in any location. For example, you could create shortcuts to templates in specific geographic regions. Shortcuts reduce the number of templates; if you change the parent template, the change is also made in all child copies of the template.

Clone existing templates

Once a template has been used, it cannot be changed directly. It can be cloned, and then changed. For this reason it is recommended that templates be smaller in nature so that if any changes are required, you can change that one component of the provisioning configuration.

The **Clone** makes a copy of the selected template. You can modify the copy to save inputting all the settings of a template you want to only modify slightly. If you clone a public template, the copy is placed in the My templates folder and acquires the properties of a private template.

1. Click **Tools | Distribution | OS Deployment**.
2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
3. Select a template and click **Clone**.

The template is cloned in the right navigation pane, with the default name of the original template and the date and time the clone was created.

4. To change the name, description, boot environment, or target OS of the cloned template, right-click the clone, click **Properties**, modify the settings, and click **OK**.
5. To modify the actions, included templates, user variables, or the XML of the cloned template, double-click the clone to open the Template view.

Condense

Use the **Condense** button to minimize all templates within the current template. If there are other templates included in the current template, they will be minimized with the template. Once you condense a template, it cannot be expanded again.

Schedule

Use the **Schedule** button to create a task to execute the template on a target server(s). See "Step 3: Scheduling the template for deployment" below under "Steps for Provisioning a server."

Steps for provisioning a server

On the most basic level, provisioning a server is a simple process consisting of three steps. First, you create a provisioning template, you configure the template with what you want to put down on the server, and you schedule a task to run the template on the server.

Step 1: Creating a template

To provision a server, you create a template. A template is a series of building blocks to be applied to the server. They build upon each other, and can consist of actions, attributes, constraints, and so forth. A template can have one or many actions. Templates may be chained together in a provisioning task in a particular sequence. You can change the task order in a template. The sequence can be changed where applicable (for example, one cannot place a post-OS task before the installation of the OS). There are numerous pre-configured templates for various vendors (HP, Dell, and so forth). Templates are saved as XML in the database.

To create a template

1. Click **Tools | Distribution | OS Deployment**.
2. Click **New provisioning template**.
3. Type a descriptive name in the **Name** box.
4. Type a description in the **Description** box. The Name and Description are displayed in columns in the right pane.
5. Select the boot environment you want the template to preboot the server to (Windows PE or Linux PE).
6. Select a target operating system for the template (Windows or Linux). The boot environment and target OS should match (Windows PE and Windows OS, or Linux PE and Linux OS).
7. Click **OK**.

Step 2: Configuring the template

Once the template is created, it must be configured by adding actions to it. Template actions are sorted into five sections. You can only select actions in each section that can apply to the section (for example, you cannot select Software distribution as an action for the Pre-installation section). You can add any available action to any section, but please be aware that some actions will break the template or may render your system unusable if completed in the improper steps.

1. Double-click the template you just created.
2. In the left navigation pane, click **Action list**.
3. In the middle pane, select the section in which you want the action to occur.
 - **System migration:** Features and components that need to be saved before modifying the system (or migrating a server to other hardware or virtual machine). For example, capturing profile information when migrating to Windows* Vista.
 - **Pre OS install:** Boots into pre-installation environment (Linux PE, Windows PE). For example: RAID configuration.
 - **OS Install:** Stays in pre-installation environment (Linux PE, Windows PE). For example: Installing Windows XP.
 - **Post OS Install:** Stays in target operating system. For example: Patch management
 - **System configuration:** Boots into target OS for additional application installation/execution and system configuration. For example: Installing drivers
4. Click Add.
5. Type a specific name for the action in the **Action name** field.
6. Type a detailed description of the action in the **Action description** field.
8. In the left pane, click **Options** to select options that apply to this action only.
9. In the left pane, click **Action type**, and select an action type from the drop-down list. The buttons on the bottom of the dialog change depending on the action type you have selected. The drop-down list is filtered by the section and target OS settings.
10. When finished, click **OK**.

Step 3: Scheduling the template for deployment

A provisioning task contains template(s), and the server identifier(s) of the target server(s). When a provisioning task begins, the job is associated with the server's Computer record in the database so that the configuration history remains attached to the computer. Configuration tasks cannot be reused with different target servers, but can be reused by specifying another server identifier.

The Scheduled tasks window shows scheduled task status and while the task is running and upon completion. The scheduler service has two ways of communicating with devices: Through the standard management agent (must already be installed on devices), or through a domain-level system account. The account you choose must have the login as a service privilege and you must have specified credentials in the Configure Services utility. For more information on configuring the scheduler account, see "Configuring the scheduler service."

To schedule a provisioning task

When you click Schedule, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that the task has still been created and will appear in the Task list.

Tasks fall under the following folders:

- **My tasks:** Tasks that you have scheduled. Only you and administrative users can see these tasks.
- **All tasks:** Both your tasks and tasks marked as public.
- **Common tasks:** Tasks that users have marked common. Anyone who edits or schedules a task from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.
- **User tasks** (administrative users only) : Tasks users have created.

Provisioning bare metal devices

Provisioning lets you provision bare metal devices. You can begin this process before device is physically present. To do so, you enter a hardware identifier (such as the GUID or Mac address) in the **Identify devices** dialog, and the minimal information required by the automated provisioning agent (Idprovision) is recorded in the database.

1. Create a bare metal server computer entry with the Identify devices dialog.
2. Associate each server with a template.
3. Plug in the devices and provide them an IdProvision boot CD, bootable USB drive, or configure BIOS to network/PXE boot.
4. Power up the devices.

Creating provisioning templates

Use the Template dialog to create a provisioning template. A template is a series of actions or building blocks to be applied to the server in a particular order. A template can have one or many actions. You can change the task order in a template. The action sequence can be changed where the action makes sense, but cannot be changed where it does not make sense (for example, one cannot place a post-OS-specific action before the installation of the OS). There are numerous pre-configured templates for various vendors (HP, Dell, and so forth). Templates are stored as XML in the database.

To create a template

1. Click **Tools | Distribution | OS Deployment**.
2. Select either the **Public** or **My templates** folder.
3. Click **New template** on the toolbar.
4. Type a descriptive name in the **Name** box.
5. Type a description in the **Description** box. The Name and Description are displayed in columns in the right pane.
6. If necessary, select the boot environment you want the template to preboot the server in (Windows PE or Linux PE).

7. If necessary, select a target operating system for the template. The boot environment and target OS should match (for example, Windows PE and Windows OS).
8. Click **OK**.

To change template properties, double-click the template or right-click the template and select **Properties**.

To delete a template

- Select a template, and click **Delete**. Click **Yes**.

You can only delete templates that have not been previously executed (locked)used, and only templates that are not included in other templates. Locked templates can be deleted (removed) from the list view but remain in the database.

Provisioning - boot media

Use the Boot media dialog to create boot media, which can be used to provision servers or to send to remotes sites for provisioning. Provisioning creates a physical media by which to boot the server into a preboot environment . This media can be delivered through a PXE server or a bootable USB device/CD/DVD. A preboot environment consists of an operating system complete with video, networking, a mini-inventory scanner, and an agent capable of receiving files and executing commands. In order for the boot media to work, you must configure the target device to boot from the proper media (in BIOS enable network IPXE or CD/DVD boot).

1. Click **Tools | Distribution | OS Deployment**.
2. Click the **Create provisioning boot media** toolbar button.
3. Click **Download**, click **Run**, and click **Run** again. The USB device must be connected to enable the USB drive option.
4. Select the preboot environment type (Windows or Linux).
5. Select the boot media type (USB drive, bootable CD, or bootable ISO). If you selected USB Drive, enter the drive letter. If you selected Bootable CD, select the CD Burning drive. If you selected Bootable ISO, select the destination path the ISO will be saved to.
6. Click **Create boot media**.

The creation of boot media may fail if the system is low on memory.

Note: When creating a USB boot media, you must have administrator rights. In the case of Microsoft Vista*, you have to download the program and run the program as administrator.

Note: To create CD or ISO media, the device where you run the boot media creation tool must have IMAP2, which is available from Microsoft at <http://support.microsoft.com/kb/kb932716>.

Sharing templates

- [Import a template](#)
- [Export a template](#)
- [View a template's XML code](#)

Use Import templates or Export templates to import or export templates in XML format. You can edit the XML in the XML contents section. You can export templates to send to colleagues in other organizations. The template displays in the following general XML format.

```
<templates>
  <template>

    <name></name>
    <description></description>
    <section>
      <name></name>
      <description></description>
      <action></action>
    </section>

  </template>
</templates>
```

To import a template

1. Click **Tools | Distribution | OS Deployment**.
2. In the bottom pane, click the **Import templates** tab.
3. To bring in code from an outside file into the current template, type the path and file name of the XML file in the **Import file** text box, or click **Browse** and select the file, then click **Import**. This imports the template into the My templates folder.

The file is saved as a .XTP file (XML Template Pages)

To export a template

1. Click **Tools | Distribution | OS Deployment**.
2. In the bottom pane, click the **Export templates** tab.
3. In the top pane, Select the template you want to export, and click **Export**. Click **Save**, select the location you want to save the template to, and click **Save**.

The file is saved as a .XTP file (XML Template Pages). If you are exporting a template containing UTF- only characters, the title will not display correctly in Internet Explorer. The non-displayable characters in the template title will appear as underscores. You can change the template title through the **Save As** dialog.

To view a template's XML code

1. Click **Tools | Distribution | OS Deployment**.
2. Select **Public** or **My templates** or one of their subgroups.
3. Double-click a template, and click **XML**.
4. In the Template view, you can view or edit the XML. To save changes, click **Save changes**.

Update templates

Use this dialog to configure settings for provisioning templates, the template download location, and proxy server settings.

Note: When any scheduled template update task runs, it uses the settings on this dialog that are current at the time, not the settings when the scheduled task was created.

This dialog contains the following options:

Download updates

- **Select download source site:** Specifies which provisioning template content server will be accessed to update your database with the latest provisioning templates. Select the server nearest your location.
- **Select provisioning templates to update:** Identifies which platforms' provisioning templates are updated. You can select one or more platforms. The more platforms you select, the longer the download will take.
- **Import as a new copy:** Import the templates as new templates, not overwriting any templates or groups.

Proxy Settings

If your network uses a proxy server for external transmissions (such as Internet access), use this tab to enable and configure the proxy server settings. Internet access is required for updating provisioning template information.

- **Use proxy server:** Enables the proxy server option (by default, this option is off). If you enable a proxy server, you must fill in the address and port fields below.
- **Address:** Identifies the IP address of your proxy server.
- **Port:** Identifies the port number of your proxy server.
- **HTTP-based Proxy:** Enables the proxy server, if it's an HTTP-based proxy (such as Squid), so that it will successfully connect to and download patches from FTP sites. (Patches hosted at some FTP sites cannot be downloaded through an HTTP-based proxy unless you first enable this option.)
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
 - **Username:** Enter a valid username with authentication credentials to the proxy server.
 - **Password:** Enter the user's password.

To download the latest templates

1. Click **Tools | Distribution | OS Deployment**.
2. Click the **Update templates** button on the toolbar.
3. Select a download source site.
4. Select the vendor-specific templates you want to download.

5. Select **Import as a new copy** to overwrite any existing templates or groups with the same name.
6. Click **Download**. A message denoting Success displays at the top of the dialog.
7. Click **Import** to move the templates to the My templates folder.

Importing installation scripts

Use the Install scripts tab to create a template out of a script or scripts. Install scripts makes installation scripts available for use in creating scripted installation actions in templates. Provisioning supports batch file scripts, shell scripts, and many other scripts. The Deploy image, Scripted install, and Inject script actions use scripts like sysprep.inf or unattend.txt. Install scripts can also insert variables into your scripts; for example, a device name can be inserted into a sysprep.inf file.

To import installation scripts

1. Click **Tools | Distribution | OS Deployment**.
4. Type a name for the script in the **Script name** text box. This name will display in the Installation script dropdown list of the Scripted install action.
5. Type additional details about the script in the **Description** text box.
6. Select the target operating system in the **Target OS** drop-down list.
7. Type the path and file name of the script in the **File name** text box, or click **Browse**, navigate to the script, select it, and click **OK**.
8. Click the **Insert variables into script** checkbox if you want to swap out variables during the script import. When variables are replaced, the ones in the table below will be replaced automatically. Additional custom variables are supported, and the values will be replaced when the template is run.
9. Click **OK** to place the script in the Installation script drop-down list of the Scripted install action.
10. To export the script, select it in the Install scripts box, and click **Export**. Click **Save** and specify a name and location.

Install scripts supports many key value pairs, such as:

Variable	Description
%ldHostname%	The host name
%ldDeviceID%	GUID of the device

If there is a key value pair in the WIN.INF file that already exists as a user-defined variable, Install scripts replaces it with the user-defined variable.

To pass variables through an installation script as a variable (not to be replaced by the provisioning process) encapsulate the variable in double-percents, like %%variable%%.

Notes:

- In Windows, a valid, active, formatted partition must exist before the Scripted install action can occur.

- The network installation source must have drivers for the target device injected correctly or put into the OEM's PnP driver path (for additional information, please refer to the Microsoft installation documentation).
- Currently, only a command-line installation using winnt32 works.
- The file cmdlines.txt is used to append commands to the final OS boot.
- Currently, PXE/RIS is not supported.
- If the installation fails, you can troubleshoot the error by looking in the `\ManagementSuite\ldlogon\provisioning\config` folder to see the installation script with the variables replaced. This strategy also applies to any time you modify a script, or use a script in the Inject script or Deploy image actions.
- The temporary directory used for provisioning is `%systemdrive%\ldprovisioning`.

Linux installation issues

Linux scripted installation is only supported using PXE boot.

When running a scripted install action for Linux, please be aware that each version of Linux checks that you are using the correct CD when you begin an installation. Therefore, you will need a different `initrd` and `linux` (`vmlinuz`) for every version of Linux.

The best way to do this is to copy the boot images from each CD to the PXE and rename them. You should copy them to `\LANDesk\pxe\System\images\x86pc\undi\provlinux`. For example, for Red Hat 4, rename the files to `initrd.rh4as` and `vmlinuz.rh4as`, and for Sles10, rename the files to `initrd.sles10` and `linux.sles10`. Then, when you create a scripted install action, use the correct `initrd.xxx` and `xxxlinux.xxx` in the Scripted install template.

Linux install scripts support many key value pairs, such as:

Variable	Description
ldDNSDomain	The DNS domain
ldInstallServer	The install source server
ldInstallDir	The installation directory. For example, <code>/storage/OS/linux/redhat/enterprise_4as/u3/i386/</code>
ldNameserver1	DNS server 1
ldNameserver2	DNS server 2

Provisioning template variables

Template variables allow for greater portability and customizability in templates. For example, a template may contain very specific file names to copy, paths to install to, or an IP address to export files from, but with user variables in place of these specific items, the template can address more situations or locales because you can simply swap out the variables in the XML code to replace those specific items.

There are four types of variables. They are (in order of precedence)

- **Device:** Variables assigned to a specific device
- **Global:** Variables that are public (available) to all templates
- **Template:** Variables applying only to the assigned template
- **Action:** Variables applying only to a specific action

Note: Variables are case-sensitive.

To define device variables

1. In the **All devices** list, click a device or target a list of devices.
2. In the bottom pane, right-click a device and select **Manage variables**.
3. Type the name of the item (such as IP address) in the **Name** field.
4. Type the value to be replaced in the **Value** field.
5. Select the type.
 - **String:** Enter a string value
 - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
 - **Sensitive data:** Enter the value to be encrypted in the database.
6. Click **Save**.

To define public (global) variables

1. Click **Tools | Distribution | OS Deployment**.
2. Click the **Public variables**.
4. Type the value to be replaced in the **Search value** box. For example, CoreIP.
5. Type the new value in the **Replace value** box. For example, if the Search value is CoreIP, type the IP address you want to replace CoreIP with.
6. Select the type.
 - **String:** Enter a string value
 - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
 - **Sensitive data:** Enter the value to be encrypted in the database.

Note: Use quotes around name with spaces. Most values from the Inventory database can be used.

7. Click **OK**.

Creating unique identifiers for new devices

To create unique identifier(s) for new devices, use a Public variable that is based on the MAC address of the target device as shown below:

Variable (Database) =macAddress	Value = Computer.Network."NIC Address"
Variable (String) = Prefix	Value = UT (User value like location - Optional)
Variable (String) = Suffix	Value = XP (User value like OS - Optional)
Variable (String) = ComputerName	Value = %Prefix%%MACaddr%%Suffix%

Next, use the ComputerName variable in your sysprep.inf or unattend.txt files to uniquely identify the new device.

```
[UserData]
    ProductKey=%ProductKey%
    FullName="Engineering"
    OrgName="LANDesk"
    ComputerName=%ComputerName%
```

To define template variables

1. Click **Tools | Distribution | OS Deployment**.
2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
4. Click **Template variables**.
5. Click **Add**.
6. Type the variable you want to add in the **Search value** text box.
7. Type the value you want to replace in the **Replace value** text box.
8. Select the type.
 - **String:** Enter a string value
 - **Database value:** Enter a database ID string, such as Computer.Network."NIC Address"
 - **Sensitive data:** Enter the value to be encrypted in the database.

Note: Use quotes around name with spaces. Most values from the Inventory database can be used.

9. Click **OK**.

To define action variables

1. Click **Tools | Distribution | OS Deployment**.
2. Right-click a template and click **Edit**.
3. In the middle pane, select an action. In the right pane, click **Edit**.
4. In the Action variables box, click **Add**.
5. Type the variable you want to add in the **Name** text box.
6. Type the value you want to replace in the **Value** text box
7. Select the type.
 - **String:** Enter a string value
 - **Database value:** Enter a database ID string, such as Computer.Network.*nic address*
 - **Sensitive data:** Enter the value to be encrypted in the database.

Note: Use quotes around name with spaces. Most values from the Inventory database can be used.

8. **Click OK.**

Actions:

- [Capture image](#)
- [Configure agent](#)
- [Configure target OS](#)
- [Control service](#)
- [Copy file](#)
- [Create directory](#)
- [Delete file](#)
- [Deploy image](#)
- [Distribute software](#)
- [Download file](#)
- [Execute file](#)
- [Inject script](#)
- [Install service](#)
- [Join domain](#)
- [Map/unmap drive](#)
- [Partition](#)
- [Patch system](#)
- [Reboot/Shutdown](#)
- [Replace text](#)
- [Scripted install](#)
- [Uninstall service](#)
- [Unzip file](#)
- [Update registry](#)
- [Wait](#)

Use the dialog to create new actions for provisioning templates, or to edit the actions of existing templates. Public templates are visible to all users. My templates are not visible to all users, and can only be modified by the template creator or by users with administrative rights.

Actions are broken down into five sections. You can only select actions in each sections that can apply to the section (for example, you cannot select Software distribution as an action for the Pre-installation section). You can add any available action to any section, but please be aware that some actions will break the template or may render your system unusable if completed in the improper steps.

The **Condense** button makes all of the Included templates of the current parent template get included immediately, so that all actions from the included templates get dropped into the parent template. This means that the parent template has no more dependencies. This is useful for exporting templates or making templates Public. Once a template is condensed, it is a new template. One cannot expand a condensed template.

To add actions to a template

1. Click **Tools | Distribution | OS Deployment**.
2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
3. Double-click a template.
4. In the left pane, click **Action list**.
5. In the middle pane, click the section you want to add an action to. You can choose from these sections:
 - **System migration:** Features and components that need to be saved before modifying the system (or migrating a server to other hardware or virtual machine). For example, capturing profile information when migrating to Windows* Vista.
 - **Pre-OS install:** Boots into pre-installation environment (Linux PE, Windows PE). For example: RAID configuration.
 - **OS Install:** Stays in pre-installation environment (Linux PE, Windows PE). For example: Installing Windows XP.
 - **Post-OS Install:** Stays in target operating system. For example: Patch management.
 - **System configuration:** Boots into target OS for additional application installation/execution and system configuration. For example: Installing drivers.
6. Click **Add**.
7. Type a specific name for the action in the **Action name** field.
8. Type a detailed description of the action in the **Action description** field.
10. In the left pane, click **Options** to select options that apply to this action only.
11. In the left pane, click **Action type**, and select an action type from the drop-down list. The buttons on the bottom of the dialog change depending on the action type you have selected. See below for more information on the specific action types.

12. When finished, click **OK**.

Action types

The table below displays the action types and where they fit into sections by default. You can add any action type to any section, but please note that some actions inherently fit in certain sequences in provisioning, and if an action is executed outside its intended sequence, unintended consequences may occur.

Action name	System migration	Pre-OS installallation	OS installation	Post-OS Installation	System configuration
Capture image			X		
Configure agent					X
Configure Target OS				X	
Control service					X
Copy file	X	X	X	X	X
Create directory	X	X	X	X	X
Delete file	X	X	X	X	X
Deploy image			X		
Distribute software					X
Download file	X	X	X	X	X
Execute file	X	X	X	X	X
Inject script	X	X	X	X	X
Install service					X
Join domain					X
Map/Unmap drive	X	X	X	X	X
Partition		X	X	X	
Patch system					X
Reboot/Shutd	X	X	X	X	X

Action name	System migration	Pre-OS installallation	OS installation	Post-OS Installation	System configuration
own					
Replace text	X	X	X	X	X
Scripted install			X		
Uninstall service					X
Unzip file	X	X	X	X	X
Update registry					X
Wait	X	X	X	X	X

Capture image (OS installation section only)

The Capture image action lets you capture an image at the time of OS installation, through the use of the imaging tool you specify. If the tool or the contents to be captured in an image are located on a share, you must place the Map drive action prior to the Capture image action in order to authenticate to the share.

- **Imaging tool:** The path to the location of the imaging tool.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the image is captured.
- **Launch wizard:** Launches the imaging tool's wizard, which takes you through the process of capturing an image.

Note: To avoid the problem of the file system being locked open in WinPE, you must first Sysprep your image. In Windows Vista, follow the steps below.

1. Boot into Vista.
2. Change to the %SystemRoot%\System32\sysprep directory.
3. Run "sysprep /generalize /shutdown".
4. Boot to the PE and run ImageX.

The Windows XP/2003 steps don't require the /generalize and /shutdown switches for sysprep. The /factory switch should work on those operating systems.

Configure agent (System configuration section only)

The Configure agent action lets you select an agent configuration to install on the provisioned server. This action should be the first thing done after the reboot that follows the OS install actions. Configurations are added to the drop-down list as you create them in Agent configuration. This action can only be completed as part of a template that includes either the Scripted install or Deploy image actions, or if the client machine has already been configured with an agent.

- **User name:** Enter the user name of the core on which the agent configuration resides.
- **Use variable for the password:** Click this checkbox to use a variable for the password. This [variable](#) is set in **Template variables** under Sensitive data type.
- **Password:** Enter the password of the core. Confirm the password in the **Confirm password** box.
- **Configuration name:** The name of the configuration. Select a configuration from the drop-down list.

Note: When you install a new service pack, the agent configuration database IDs change. This means that the templates referencing those configurations become outdated. As a result, any provisioning history referencing those configurations will be unable to display the name of the configuration it once referenced, and any template referencing the old configurations will need to be updated before it will run correctly. The configuration name is not displayed in the History page, and if you try to re-schedule this template, it will fail on the Agent Configuration action because of this problem. To fix it, you must clone the template, then open the cloned template, open the **Agent Configuration** action, and assign the configuration you want to use. Then the task will run successfully.

Configure target OS (post-OS installation section only)

This action inserts the provisioning agent (ldprovision) into an image so that the agent can be installed after reboot. It is required for continued provisioning after the new OS starts. For this action to work, the following conditions must be met:

1. The windows system drive must be mounted
 2. The windows file system must be either sysprep?ed or have an agent on the machine
 3. Linux may not have any uncommon file systems (xfs, jfs, bobfs). The reiserfs and ext2/3 Oses are the only current valid supported Oses.
 4. Linux root system may not be on a software raid controller, or be on a software raid (md?s). Real hardware raid configurations are OK, as long as the controller driver is recognized by the PE.
- **Insert unique ID:** Click the checkbox to use the existing device ID, and enter it in the text box.

Note: This action should be performed as the last action in the Post-OS installation section because this action includes a Reboot action.

Control service (System configuration section only)

The Control service action starts, stops, or restarts a specified service. The target OS must be Windows for this action.

- **Display name:** The name of the service.
- **Service control action:** The action to execute on the service. Can be Stop, Start, or Restart.

Copy file (all sections)

The Copy file action copies files to specific locations on the target server. Both the source and destination can be located on a share. If this is so, you must include a Map drive action prior to the Copy file action. The Copy file action can be recursive, meaning that all files/folders below the source path can be copied, maintaining their original structure. Wildcard characters are supported (such as *.exe or Id*.*)).

- **Source path and file name:** The server/share path and file name location of the file to be copied. If you want to copy all files and folders below the source path, no file name is necessary. Wildcard characters are supported.
- **Destination path and file name:** The server/share path and file name location to copy the file to.
- **Copy subdirectories:** Copies all subfolders and files below the source.

Create directory (all sections)

The Create directory action creates a directory in the specified location and can create the parent directory, if needed.

- **Path of the directory:** Type the path to the directory to be created.
- **Create parent directory if needed:** Select the checkbox to create the parent directory.

Delete file (all sections)

The Delete file action removes files in specific locations on the target server. The path can be located on a share. If this is so, you must include a Map drive action prior to the Delete file action. The Delete file action can be recursive, meaning that all files/folders below the source path can be deleted. Wildcard characters are supported (such as *.exe or Id*.*)).

- **Path and file name:** Enter the full path and name of the file to be deleted. Wildcard characters are supported.
- **Delete subdirectories:** Deletes all subfolders and files below the source.

Deploy image (OS installation section only)

This action deploys the selected image to the target server through the use of the imaging tool you specify. If the tool or the image to be deployed are located on a share, you must place the Map drive action prior to the Deploy image action in order to authenticate to the share.

- **Imaging tool:** The path to the location of the imaging tool. If you select "Other" as imaging tool, then the entry for the path and filename of the image needs to contain the complete command line string for the imaging tool.

- **Command-line parameters:** Enter any command-line parameters that will customize the way the file is captured.
- **Launch wizard:** Launches the imaging wizard from the tool, which guides you through the deployment process.

Distribute software (System configuration section only)

This action distributes a software distribution package to the target. This action can only be completed after the agent configuration action, or after agents have been installed on the server.

- **Software distribution package:** Select the package you want to distribute.

Download file (all sections)

The Download file action downloads the selected file using anonymous user (anonymous HTTP login) to a destination you specify. If the files to be downloaded or the destination are located on a share, you must place the Map drive action prior to the Download file action in order to authenticate to the share.

- **Source path and file name:** The current server/share path and name of the file to be downloaded. Downloading files from a UNC path is not supported. If you want to download a file from a UNC path, you should use the Map drive action to map to the UNC path, then use the Copy file action.
- **Destination path and file name:** The location the file is to be downloaded to.
- **Use proxy server:** Enables the proxy server option to download a file. By default, this option is off. If you enable a proxy server, you must fill in the address and port fields below.
- **Address:** Identifies the IP address of your proxy server.
- **Port:** Identifies the port number of your proxy server.
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
 - **Username:** Enter a valid username with authentication credentials to the proxy server.
 - **Use variable for the password:** Click this checkbox to use a variable for the password. This [variable](#) is set in **Template variables** under Sensitive data type.
 - **Password:** Enter the user's password.

Execute program (all sections)

The Execute program action executes the selected file on the targeted server, along with any command-line parameters or return codes you specify.

- **Target path and file name:** The location of the file you want to execute.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the file is executed.
- **Working directory:** The program will be executed with reference to this directory. Any supporting files of the program reside in this directory. Command-line parameters start from this reference point.

- **Expected return value:** The value expected to be returned by the application upon execution. Can be Any, equals (=), less than (<), greater than (>), or Between. If the value is to be anything other than Any, enter the value(s) to be expected in the boxes provided.
- **Insert:** Opens the Environment variable dialog, where you can add an environment variable.
- **Name:** In the **Environment variable** dialog, enter an environment variable of the file. Use double %% to specify environment variables, such as: %%windir%%\system32\calc.exe.
- **Value:** In the **Environment variable** dialog, enter the value of the variable.
- **Remove:** Delete the selected variable.
- **Modify:** Modify the selected variable.

Inject script (all sections)

This action injects a script into the target OS file system. You can inject sysprep.inf into the Deploy image action or unattend.txt into a scripted install action. The Inject script action can only be done after the OS install action and before the first reboot that follows the OS install.

- **Script name:** The name of the script.
- **Target file name:** The location of the script you want to inject.

Install service (System configuration section only)

The target OS must be Windows for this action.

- **Display name:** The name you want to display to represent the service.
- **Service name:** The name of the service.
- **Target path and file name:** The location of the service you want to install.
- **Command-line parameters:** Enter any command-line parameters that will customize the way the service is installed.
- **Service startup type:** Can be Manual, Automatic, or Disabled.
- **Allow this service to interact with the desktop:** Display on the desktop any user interface that can be used by the logged-in user when the service is started. This includes any message boxes the service may invoke during the installation process. If this checkbox is not checked, the template runs without user interaction, assuming the default selections of any service messages. If the service puts up UI during startup, it may cause the template to pause until the dialog is closed.

Join domain (System configuration section only)

Joins target device to a domain or workgroup.

- **Select operation type:** Can be Join domain or Join workgroup.
- **Domain name:** Enter the domain you want to join.
- **Workgroup name:** Enter the workgroup you want to join.
- **Username:** Type the username required to authenticate to the domain.
- **Use variable for the password:** Click this checkbox to use a variable for the password. This [variable](#) is set in **Template variables** under Sensitive data type.
- **Password:** Enter the corresponding password to the username above. Confirm the password in the Confirm password box.

Map/Unmap drive (all sections)

Map a drive or connect to a resource to access vital files to complete actions in a section or disconnect a drive or resource. Please note that some systems do not accept drive mappings below H:.

- **Map/disconnect a drive:** Select whether this action is to map a drive or disconnect a drive.
- **UNC path to map:** Enter the server and share you want to map to.
- **Drive to map:** Enter the drive letter you to map the path above to.
- **User name:** Enter the name of the user credential to log into the drive.
- **Password:** Enter the corresponding password to the username above. Confirm the password in the **Confirm password** box.
- **Use variable for the password:** Click this checkbox to use a variable for the password. This [variable](#) is set in **Template variables** under Sensitive data type.
- **Drive name:** Type the name of the drive you want to disconnect.

Partition (Pre-OS installation, OS installation, and Post-OS installation sections only)

(Boot environment and target OS must be set prior to executing this action). The Partition action lets you complete a variety of actions relating to partitions on the target server. Select partition actions from the **Partition action type** drop-down list. The actions are listed below:

Create partition: Create a partition on the specified disk.

- **Disk ID:** Type the Disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.
- **Partition type:** Select the partition type. This can be Primary, Extended, or Logical.
- **Size:** The size of the partition to be created (in MB).
- **Offset:** A number (in 8-bit byte format) indicating how far into the disk you want to create the partition.

Remove partition: Delete a partition on the specified disk.

- **Disk ID:** Type the Disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.
- **Partition ID:** The partition number to be removed.

Remove all partitions: Delete all partitions on the disk.

- **Disk ID:** Type the Disk ID. On Windows, it is the disk number. On Linux, it is the name of the disk.

Format partition: Create a file system structure on a partition.

- **File system:** For Windows, the file systems are FAT, FAT32, and NTFS. For Linux, the file systems are ext2, ext3, reiserfs, xfs, and linux-swap.
- **Mount point:** For Windows, the drive letter of the partition to be formatted. For Linux, the device name of the partition to be formatted.

Quick format: Click this checkbox to perform a quick format on the partition.

Mount partition: Mount a partition.

- **Disk ID:** The disk number to be mounted.
- **Partition ID:** For Windows, the partition number to be mounted. For Linux, the device name of the partition.
- **Mount point:** For Windows, the drive letter of the partition to be mounted. For Linux, the name of the partition to be mounted. The mount point must exist.

Unmount partition: Unmount a partition.

- **Disk ID:** The disk number to be unmounted.
- **Partition ID:** For Windows, the partition number to be unmounted. For Linux, the device name of the partition.
- **Mount point:** For Windows, the drive letter of the partition to be unmounted. For Linux, the name of the partition to be unmounted. The mount point must exist.

Make bootable: Make a partition bootable.

- **Disk ID:** The disk number to be made bootable. For Windows, this is the disk number. For Linux, this is the name of the disk.
- **Partition ID:** The partition number to be made bootable.
- **Bootable:** Click the check box to make the partition bootable.

Expand partition: Expands the last partition on the drive. Free space must be available.

- **Disk ID:** The disk number to be mounted.
- **Partition ID:** For Windows, the partition number to be mounted. For Linux, the device name of the partition.
- **Final size:** The new size of the partition in MB. If you leave this blank, the partition will be expanded to fill the disk.

Patch system (System configuration section only)

The Patch system action scans the target device for vulnerabilities and remediates them. This action can only run after a Configuration action that installs the Software updates agent is run.

- **Scan only:** Scans the machine for vulnerabilities.
- **Scan and remediate vulnerability:** Scans the machine for vulnerabilities, and patches a single vulnerability.
- **Scan and remediate vulnerability:** Scans the machine for vulnerabilities, and fixes (where possible) the vulnerability.
- **Scan and remediate group:** Scans the machine for vulnerabilities and fixes the vulnerabilities included in the group.
- **Vulnerability ID:** A valid vulnerability ID from Patch Manager. If the ID is not valid, the action will fail.
- **Group ID:** A valid group ID from Patch Manager. If the ID is not valid, the action will fail.

Notes: The core vulnerability definitions should be updated prior to executing this action. All patches to be remediated must be downloaded on the core before executing either remediation option in this action.

Vulnerability groups cannot be created in the Web console. They must be created in the Windows console. Once created, groups appear in the Group ID drop-down list.

Reboot/Shutdown (Reboot - all sections, Shutdown - System configuration section only)

Reboot or shut down the server. A reboot must immediately follow the OS install action. Upon reboot, the provisioning agent restarts the template to continue the progression of provisioning tasks. Use the Reboot action to move from System migration section to OS sections or OS sections to System configuration section. Multiple reboots are supported.

- **Reboot:** Shut down the server and restart it.
- **Shut down:** Shut down the server at the end of the provisioning task and leave it powered down (off)

Replace text (all sections)

Replace text in an existing file.

- **Source path and filename:** The path and filename of the file to have text replaced.
- **Find what (exact match):** The existing text that is to be replaced.
- **Replace with:** The text that is to take place of the existing text.
- **Replace first occurrence, all occurrences:** Replace the new text either the first time it is encountered or each time it is encountered.

Scripted install (OS installation section only)

Install an operating system through the use of custom scripts. There can only be one action that installs an OS.

Windows

- **Path to WINNT32.EXE:** This is a path where winnt32.exe is found within the installation source. This must have been mounted within the Pre-OS Install section (Map drive action).
- **Additional parameters:** Parameters to be passed to winnt32.exe when it is executed. The Provisioning handler automatically fills in the unattend (/unattend) and the source arguments (/s). These are generated from the path that was given in the Winnt32 path, and from the script that has been selected.
- **Installation script:** The unattend file used when installing the operating system.

Linux

- **Location of the initrd:** The location of the Initial RAMdisk file. The default is /x86pc/undi/provlinux/initrd.img.
- **Kernel location:** The location of the Linux kernel.

- **Additional parameters:** Parameters to be passed to initrd when it is executed.
- **Installation script:** The unattend file used when installing the operating system.

Uninstall service (System configuration section only)

Uninstall a service.

- **Display name:** The name of the service to be uninstalled.

Unzip file

Unzip the contents of a package to a predetermined location. This action can restore original structure

- **Source path and file name:** The path and file name of the package to be unzipped.
- **Target path:** The location where the package is to be unzipped. If this is an existing directory/folder, any duplicate filenames will be overwritten.
- **Create target directory if it doesn't already exist:** If the target does not exist, select this checkbox to create it automatically.

Update registry (System configuration section only)

This action adds or removes keys or values to the registry, or imports a registry (.REG) file. Editing the registry incorrectly may damage your system, potentially rendering it inoperable. Before making changes to the registry, you should back up any valued data on your computer. Select an operation from the **Registry operation** drop-down list.

- **Delete key:** Remove a registry key's expected folder and path.
- **Delete value:** Remove the expected value of the key.
- **Create key:** Create a folder on the left side of the Registry Editor.
- **Import value:** Import a registry file.
- **Set value:** Create a value. The data entered is interpreted as a value determined by the Data type drop-down list.
- **Key:** Enter the key to create or delete.
- **Value:** Enter the value to create or delete.
- **Data:** Enter data.
- **Data type:** Select a data type. This can be Unknown value, String Value, Expanded string value, Binary Value, DWORD Value, Multi-String Value, or QWord value.
- **Import file contents:** Type a description of the registry file.
- **Import registry file:** Type the full path to the registry file, or click Browse to find it, then click Import file.

Wait (all sections)

Pause the template execution for a specified time or until a required file has been created.

- **Time to wait (seconds):** Pause the template for a specified number of seconds.

- **File to wait for:** Pause the action until the specified path and file exists. This is useful when an action requires an application to install a file. When the file is created, you can trigger execution of the next action based on the existence of the file.
- **Maximum time to wait:** Waits for the specified time (in seconds). If the time passes and the file never appears, the template continues with the next action.

Provisioning I Included templates

The Template view displays the templates that are included in the current template (included templates are also known as Child templates). You can view the templates, and add templates to the current template. Once a template is included with a template, it is part of the parent template. If you change the included template in its original stand-alone form, it is changed in the parent template package, too.

To add a template to the current template

1. Click **Tools | Distribution | OS Deployment**.
2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
3. Double-click a template.
4. In the left navigation pane, click **Includes**.
5. Click the **Include** button.
6. Using the left navigation pane, navigate to the template you want to include, select it, and click **OK**.

To delete a template from the Included templates list, click **Remove** to remove the selected template.

Provisioning I Included By templates

The Included By view displays a list of other templates that include the current template (templates including the current template are also known as Parent templates).

To view the list of templates that include the current template

1. Click **Tools | Distribution | OS Deployment**.
2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
3. In the right pane, double-click a template.
4. Click the **Included by** button.

Provisioning Includes

The Includes view displays a list of other templates included in the current template (known as child templates or sub-templates).

1. Click **Tools | Distribution | OS Deployment**.

2. Click **Public** or **My templates** to display templates in the right pane. Drill down if necessary.
3. In the right pane, double-click a template.
4. Click the **Includes** link.

Note: To include a template, its boot environment and target OS must match the template setting of the parent template. Not Applicable is treated as a wildcard.

Template properties

Use the Template properties view to display the template information current to the time the template was created.

To view template properties

1. Click **Tools | Distribution | OS Deployment**.
2. Select **Public** or **My templates** or one of their subgroups.
3. Double-click a template, and click **Properties**.

Notes: Any additional information provided at the time the template was created.

Provisioning history

The **History** button lets you view a server's provisioning history by letting you check on the status of a particular task, determining how a particular server was provisioned, or finding out which servers were provisioned with a particular template. When a system is provisioned, all the actions are recorded in the provisioning history.

If you want to put a system back into a known state, you can replay the template that lets you return to that known state. If you want to replay a template, keep in mind that some actions are external to provisioning. Save any software distribution packages, agent configurations, and programs that you download and execute in conjunction with a template. Otherwise you won't be able to replay them.

To view a template's provisioning history

3. Double-click a template.
4. In the left navigation pane, click **History**.

To view the provisioning history by task

1. Click **Tools | Distribution | OS Deployment**.
2. Click the **Schedule template** button on the toolbar.
3. Double-click the task of which you want to view the history.
4. In the lower right pane, double-click the task name you want to view history on (All devices, Active, Pending, and so forth).
5. To view task history, click the log file icon (at the far right).

To view the provisioning history by device

1. From the **My devices** list, double-click the desired device.
2. In the middle pane of the Server information console, select **Logs**, then select **Provisioning history**.
3. Double-click the template you want to view history on.

Note: To get current status of a template that is in the process of executing, click the **Refresh** button to update the history status.

Provisioning group

Use the Provisioning group dialog to create groups of provisioning templates for use in provisioning tasks. You can use provisioning groups to organize your templates in ways to suit your needs. For example, you could create groups based on specific vendors, and additional subgroups based on server models. Later, if you want to modify one of the templates in the group, you only need to remove the template from the group and re-add it to the group in its modified state. You can create subgroups up to six layers deep.

To create a group of templates

1. Click **Tools | Distribution | OS Deployment**.
2. Select **Public** or **My templates** or one of their subgroups.
4. Type a name for the group in the **Name** field.
5. Type a description in the **Description** field.
6. Click **OK**.

To delete a group

1. Select a group, and click the **Delete**.

A group must be empty (no subgroups or templates) before it can be deleted.

Groups in the Public and My templates folders cannot be deleted.

Profile migration

LANDesk's profile migration feature adds device profile migration capabilities to your network. OS deployment and profile migration streamline new device provisioning and existing device migration, without requiring additional end-user or IT interaction once the process starts.

You can schedule deployments and migrations to occur after hours, and by using the LANDesk Targeted Multicast technology to distribute images, you won't saturate network bandwidth by deploying the same image to multiple devices.

Note: For information on installing the OS deployment and profile migration component on your core server, and configuring your OS deployment and profile migration environment, refer to the *LANDesk Management Suite Installation and Deployment Guide*.

Read this chapter to learn about:

Profile migration

- "Profile migration overview" on page 272
- "Profile content" on page 273
- "Creating collections" on page 274
- "Migrating user accounts" on page 274
- "Migrating application settings, templates, and associated files" on page 274
- "Migrating Desktop (PC) settings" on page 276
- "Migrating files and folders" on page 277
- "To create a file rule" on page 277
- "Creating migration scripts with the OS Deployment/Migration Tasks wizard" on page 278
- "Creating user-initiated profile migration packages" on page 279
- "Running user-initiated profile migration packages" on page 280

Profile migration overview

Profile migration complements OS deployment by offering a complete deployment and migration solution. With profile migration, you can preserve the customized desktop and application settings, and personal data files, for all of your users during an upgrade or migration project. Profile migration supports in-place migrations of individual devices as well as remote, large-scale migrations of multiple devices across your network.

Profile migration can best be understood as a two-part process:

1. *Capturing* a source device's unique profile, consisting of user accounts, desktop (PC) and application settings, and data files.
2. *Restoring* the profile to a target device.

For step-by-step descriptions of the profile capture and restore procedures, see "Creating migration scripts with the OS Deployment/Migration Tasks wizard" on page 278.

For page-by-page descriptions of the wizard's interface, see "OS deployment and Profile migration wizard help" on page 697.

Migration methods: scripted and user-initiated

Using profile migration, you can create separate capture and restore scripts with the OS Deployment/Migration Tasks wizard. The script can then be scheduled to run remotely on one or multiple target devices on your network.

Additionally, at the console, you can create self-extracting executable files (called user-initiated packages) that you, or the end user, can run directly from individual devices as a user-initiated profile migration. The user-initiated package launches a program called the LANDesk profile migration wizard. For more information, see "Creating user-initiated profile migration packages" on page 279.

The purpose of these two migration methods is the same; however, there are some differences in functionality. For example, the in-place user-initiated method lets you select which user accounts to migrate, while the scheduled script method does not. The information below refers specifically to the script method. The OS Deployment/ Migration Tasks wizard includes its own online help that describes the functionality of that utility. When running the wizard, click Help on any of the wizard's pages for more information.

Migration paths

Profile migration supports migrating across Windows operating system versions as follows:

- From Windows 95 and 98 SE...to Windows 2000 SP3 or Windows XP
- From Windows NT 4 ...to Windows 2000 SP3 or Windows XP
- From Windows 2000 ...to Windows 2000 SP3 or Windows XP
- From Windows XP ...to Windows XP
- Windows Server 2003 is also supported (for both capture and restore)

Prerequisites

To do a profile migration, devices must meet the following prerequisites:

- Devices must be scanned in the core database.
- Devices must have the standard LANDesk agent (that includes the inventory scanner and local scheduler) and Software distribution agent installed. Profile migration uses the Software distribution agent to distribute files.

Profile content

Profile migration allows you to migrate the following content:

- User accounts
- Application settings, templates, and associated files
- Desktop (PC settings)
- Files and folders

User accounts are migrated by default. Settings and files are migrated according to a user-defined collection of rules (see [Creating collections](#) below for more information). You can create rules for applications, desktop settings, and files and folders.

Creating collections

Use the Collection of Rules dialog to create new collections and edit existing ones. A collection is a user-defined set of application, desktop, and file rules that determines the profile content to be migrated (captured or restored by the migration script).

To create a collection

1. To access the Collection of Rules dialog, first click the **Collection manager** button on the Operating system deployment window, then click **Collections** and click **New**. Or, through the OS Deployment/Migration Tasks wizard, by clicking the **Manage** button on the Select a collection for this profile page of the wizard.
2. Enter a unique name for the collection.
3. (Optional) Enter a description that will help you remember the profile content captured/restored by this collection.
4. Define the content you want to capture/restore with the collection by selecting rules in the Rules list. Use the plus-sign and minus-sign boxes to expand and collapse the tree structure to view all of the Applications, Desktop Settings, and File Rules.

To select a rule, check the corresponding check box; you can select any combination of the rules available in the Rules tree listing when defining a collection.

5. Click OK to save the collection and return to the Collection Manager dialog.

Note: When you delete a collection, the collection is removed from the core server. Any migration script referencing that collection will not run properly. You should also delete the script.

Migrating user accounts

In a scripted profile migration, all discovered local and domain user accounts on the source devices are captured by default (**Important:** Except for the All Users and Default User accounts).

All captured user accounts will be restored to the target devices. A user account that does not already exist on the target device will be created as a new local user account and its settings migrated. Before restoring user accounts, you can enter a default password for these new local user accounts. If a duplicate user account does already exist on the target device, the captured (source) user account's settings will be migrated to the existing user account, but the user's current password is preserved and should be used to log in.

Migrating application settings, templates, and associated files

Persistent application settings, template files, and associated files can be migrated as part of a device's profile. Application programs themselves are *not* migrated during profile migration (however they can be part of an OS image deployment).

Each application's migration is defined by an application rule that can be added to a collection of rules.

Application rules are available for the following MS-Office applications:

- **Microsoft Access**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ade; *.adp; *.mad; *.maf; *.mag; *.mam; *.maq; *.mar; *.mas; *.mat; *.mav; *.maw; *.mda; *.mdb; *.mdbhtml; *.mde; *.mdt; *.mdz; *.mdw
- **Microsoft Excel**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.xls; *.csv; *.dqy; *.iqy; *.oqy; *.rqy; *.slk; *.xla; *.xlb; *.xlc; *.xld; *.xlk; *.xll; *.xlm; *.xls; *.xlshtml; *.xlv; *.xlw; *.dif; *.xlt; *.xlthtml
- **Microsoft Outlook**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ics; *.msg; *.oft; *.pst; *.vcs; *.pab; *.rwz; *.oab; *.oft; *.srs
- **Microsoft PowerPoint**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ppt; *.ppthtml; *.pps; *.ppa; *.pwz; *.ppz; *.pp1
- **Microsoft Word**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.doc; *.dohtml; *.gly; *.rtf; *.wbk; *.wiz
- **Microsoft Office Shared Components**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* autocorrect lists (*.acl), custom dictionaries (*.dic), common toolbars, and all template files for supported Office applications, including: *.dot; *.dothtml; *.htm; *.pot; *.pothtml; *.xlt; *.xlthtml; *.mdn; *.mdz; *.wizhtml
- **Microsoft Internet Explorer**
 - *Supported versions:* 4.0, 5.0, 5.5, and 6.0
 - *Migrated files:* favorites (*.*), cookies (*.txt), *.dat, and ratings files (*.rat)

Other application support

Application rules are also available for the following applications:

- ACT!
- Adobe Acrobat
- Adobe Acrobat Reader
- Adobe Illustrator
- Adobe PageMaker
- Adobe Photoshop
- Lotus 1-2-3
- Lotus Approach
- Lotus FastSite
- Lotus Freelance
- Lotus Notes
- Lotus Organizer
- Lotus SmartCenter
- Lotus Word Pro
- MS ActiveSync

- MS FrontPage
- MS Internet Explorer
- MS NetMeeting
- MS Outlook
- MS Outlook Express
- MS Office shared components
- MS PowerPoint
- MS Visio
- MS Word
- Netscape
- Palm Desktop
- WinZip
- Yahoo Messenger

Application migration considerations

- Upgrade version migration is supported for Office 95 and 97 versions to Office 2000 or XP. For Office 2000 and Office XP, you can migrate applications to the same version.
- If an application is not installed on the target device, that application's settings and files will *not* be migrated, even if they were captured from the source device.
- Note that template files for all of the listed Microsoft applications are migrated as part of the Microsoft Office Shared Components rule. If you want to migrate template files, you must select Shared Components.
- To ensure a successful migration of all the most recent associated settings and files, close all applications before running a profile migration.

Migrating Desktop (PC) settings

Many of the customized and optimized settings on your devices can also be migrated. Each setting's migration is defined by a desktop rule that can be added to a collection of rules.

You can migrate the following desktop (PC) settings:

- Desktop shortcuts, files, folders, and briefcases

Note on briefcases: Remember to run Update All on a briefcase before migrating. Also, if your briefcase has links to files located in a "user-specific" directory that changes from one OS to another, and you migrate to a different OS, the files will be migrated but the links will be broken and need to be recreated.

- My Documents folder
- Mapped network drives

Note on duplicate drive letters: If there is a drive letter already mapped on the target device, that mapped drive is preserved rather than replaced, and the source device's drive letter mapping is not migrated.

- Printers (network)
- Wallpaper
- Screen resolution, color quality, and refresh rate

Note: Empty folders aren't captured.

Migrating files and folders

By creating your own customized file rules, you can migrate individual or multiple files determined by directory location and filename. File rules offer powerful control and flexibility by letting you:

- Create as many file rules as you want and add them to your collections.
- Include and/or exclude files by wildcard naming in a single file rule.
- Specify whether to include subdirectories.
- Redirect files to a new destination on the target device.
- Capture files from any fixed drive on the source device (including disk partitions), and successfully migrate the files even if the target device does not have the same partitioning.
- Retain the captured file's directory structure. If a captured file's associated directory structure does not exist on the target device, the path will be created and the file restored to it.

You can migrate files from a device's *fixed* drives, including disk partitions. Removable media, such as CD-ROM drives, and network shares are not supported. If the target device does not have a matching disk partition drive letter, a new directory named "Migrated_[drive letter]_Drive" is created at the root of the target device's C drive, and the files (along with their associated directory structure) are migrated to that new directory on the target device.

To create a file rule

Use the File Rules dialog to create new file rules or edit existing file rules. A file rule determines which files are migrated, based on the following criteria: drive and directory location; subdirectories; file naming including wildcard support, and destination location.

1. Click **Tools | Distribution | OS Deployment**.
2. In the toolbar, click the **Collection Manager** button.
3. In the Collection Manager dialog, click **File rules** and then click **New** to open the **File Rule** dialog.
4. Enter a unique name for the file rule.
5. (Optional) Enter a description that will help you remember this file rule.
6. Specify all of the options on the dialog (for descriptions of the options, see "About the File Rule dialog" on page 707).
7. Click **OK** to save the file rule and return to the Collection Manager dialog.

When you delete a file rule, the rule is removed from the core server. Any collection that contained that rule provides a notice about this change the next time you open or edit the collection.

Additional file migration considerations

- **Rules and collections:** You can create as many file rules as you like. You then add file rules to collections that may or may not contain other file, application settings, and desktop settings rules.
- **File path (directory structure):** The associated directory structure of a file is preserved by default.

- **Multiple controls in one file rule:** You can have any combination of multiple file inclusion and/or file exclusion controls in the same file rule.
- **File replacement handling:** The file captured from the source device replaces the existing file on the target device IF the captured file is newer than the Date Modified time stamp of the existing file.
- **File size limitation:** Because profile data is stored in sequential Windows cabinet (.CAB files), which have a size limitation of 2 GB, you cannot migrate a single file that is 2 GB or larger. A file of that size is probably not common on devices, but you should be aware of this limitation.
- **Ignore file errors during profile capture:** You can allow a profile capture process to continue even if files designated to be captured report file errors (such as invalid file names, locked files, or files that change size during the capture). The profile capture completes, and file errors are recorded in the log file. To do this, on the OS Deployment/Migration Task wizard's initial page, select **Capture profile**, and then click the **Continue with file capture errors** checkbox.

Creating migration scripts with the OS Deployment/Migration Tasks wizard

The steps below outline the basic procedures for capturing and restoring a device's profile using the OS Deployment/Migration Tasks wizard. For more information about each of these steps, click the **Help** button located on each page of the script wizard.

Note: For capturing and restoring a profile with a user-initiated migration package, see the online help included with the LANDesk profile migration wizard.

To create a profile capture script

1. Click **Tools | Distribution | OS Deployment..**
2. In the **Operating system deployment** window, right-click **All OSD/profile migration Scripts** and then click the PE configuration type you want to create in the shortcut menu to open the wizard. Note that only Windows and DOS PE configurations can capture profiles.
3. Select **Capture profile**, and then click **OK**.
4. On the **General** page, enter a description for the script.
5. On the **Collections** page, identify what profile information you want to collect by specifying the rule collection you want to use. Select an available collection that you already created, or click manage create a new collection or edit an existing collection
6. On the **Storage UNC** page, enter a UNC path and authentication credentials for the location where you want to store the profile data.
7. Click **Save** to create the profile capture script.

Using the **Scheduled tasks** tool, you can now schedule the script to run on one or more target devices on your network.

Storing profile data for multiple devices (and multiple users)

Profile data is stored in Windows cabinet files (.CAB) in a directory structure located under the specified UNC path. If you run a profile capture script on multiple devices, each device's profile data is stored in a separate directory named after its unique Windows computer name. Likewise, if multiple users are discovered and captured on the same source device, each user's profile data is stored in a separate subdirectory (of the device's directory named after the user login name). In other words, every migrated device has its own profile storage directory and contains a subdirectory for every captured user account on that device.

To create a profile restore script

1. Click **Tools | Distribution | OS Deployment..**
2. In the **Operating system deployment** window, right-click **All OSD/profile migration Scripts** and then click the PE configuration type you want to create in the shortcut menu to open the wizard. Note that only Windows and DOS PE configurations can capture profiles.
3. Select **Restore profile**, and then click **OK**.
4. On the **General** page, enter a description for the script.
5. On the **Profile storage** page, enter a UNC path and authentication credentials for the location where the profile data is stored, and enter a default password for migrated new local user accounts (if left empty, the password is automatically set to "password").
6. Click **Save** to create the profile restore script.

Using the **Scheduled tasks** tool, you can now schedule the script to run on one or more target devices on your network.

Note: Windows 2000 SP3 and Windows XP are the only supported *target* Windows OSes.

Profile migration log file

Profile migration (both the scripted and user-initiated method) creates a "rolling" log file named PROFILEMIGRATION.LOG, that is saved in the user-specified profile data storage directory. Relevant information, such as time, specific operation, and status, are appended to the existing log file for each subsequent capture and restore operation. When the log file reaches 64 KB in size, it is renamed PROFILEMIGRATION.OLD and a new .LOG file is created. You can view this log file in any text editor.

Creating user-initiated profile migration packages

The User-Initiated Package dialog lets you create a self-extracting executable file that can be run on devices as a user-initiated profile migration.

User-initiated migration packages can be run on your devices, as well as computers that are not managed by LANDesk.

To create a user-initiated migration package

1. Click **Tools | Distribution | OS Deployment**.
2. In the toolbar, click the **Collection Manager** button.
3. In the **Collection Manager** dialog, Select **User-initiated packages**, and then click **New**.
4. Enter a unique name for the package. Do not type the filename extension here; the .EXE extension will be appended automatically to the name you enter.
5. Select a collection from the displayed list. The collection you select determines the profile content applications, desktop settings, and files. You can select only one collection per migration package.
6. To build the package, click **OK**. This may take some time, depending on the amount of profile content defined in the collection you selected.

The user-initiated migration package (.EXE) is saved by default to the following directory on your core server: c:\Program Files\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables.

When you delete a user-initiated package, the package is removed from the core server. Other copies of the package may still exist depending on how and where you distributed the package to users.

Running user-initiated profile migration packages

You can distribute the user-initiated profile migration package to devices via e-mail or removable media and run it at the device, or you can store the package on a network share and run it from a device with access to that share.

The package launches a program called the LANDesk profile migration wizard that includes its own online help file. For more information, including step-by-step instructions for capturing and restoring a profile with user-initiated migration packages, click **Help** on any of the LANDesk profile migration wizard's pages.

Executive dashboard

The executive dashboard provides important data to corporate officers and IT managers, enabling them to have continual oversight of the business in several key areas. This enhanced visibility of the business allows executives to make informed management decisions and quickly respond to critical issues.

- [Executive dashboard overview](#)
- [Using dashboard widgets](#)
- [Configuring the executive dashboard](#)

Executive dashboard overview

The executive dashboard consists of a series of widgets (informative charts, diagrams, dials, and meters) that enables executives to monitor the health or status of their business. Each widget is considered a miniature application due to its limited, yet very specific functionality. Widgets are also characterized by providing information with little or no input. The widgets are used exclusively in the dashboard, which keeps vital information at your fingertips, ready when you need it.

The executive dashboard is installed as a component of the Web console on a core or additional console. You access it from a Web browser. You are required to have the basic Web console right to access the executive dashboard, and you must be a member of the Windows NT **LANDesk Management Suite** group. Only users with the LANDesk Administrator right are given a link to the executive dashboard from the Web console. In order for other non-administrative users to access the executive dashboard, they must be provided with the URL, whether it be by an administrator or another executive who previously received the URL, and authenticate to the Web console.

In a multi-core server environment (where more than one core server exists in the core.asp file), you will be prompted to select the core server containing the data you want to view. If the credentials for logging into the Web console match the server credentials, you will not be prompted for any further authentication. If they aren't the same, you will be prompted to authenticate to the roll-up or core server. For more information, see [Multi-core support](#).

Note: You need to have your Internet settings properly configured to be prompted to authenticate to a core server when your login credentials for the Web console and the roll-up or core server don't match. From your Web browser, click **Tools | Internet Options | Security | Custom Level**. Under **Authentication**, select **Prompt for user name and password**.

The following browsers are supported and can be used to view the executive dashboard:

- Internet Explorer* 6.x with SP 1
- Mozilla* 1.6 and 1.7
- Mozilla Firefox* 1.0.x

Using dashboard widgets

Multiple widgets can exist in the dashboard at any given time. You have complete control over what widgets are visible and can freely move them anywhere you want within the dashboard. You need Macromedia Flash* Player 8 in order for the widgets to function properly. If your browser doesn't have the correct version of Flash, you should be prompted to install the application the first time you access the executive dashboard.

SANS top 10

The **SANS top 10** widget shows the number of devices vulnerable to one or more of the top ten security vulnerabilities in Windows on a per quarter basis.

Patch vulnerabilities

The **Patch vulnerabilities** widget shows the percentage of devices vulnerable to one or more known operating system and application vulnerabilities. All vulnerabilities are categorized based on severity. The arrows and corresponding percentages define the trending performance over a 24-hour time period.

LANDesk publishes vulnerability definitions based on official vendor security bulletins, and then uses these definitions to check for the operating system or application vulnerabilities.

Security threats

The **Security threats** widget shows the percentage of devices affected by one or more Windows system configuration errors and exposures. Security threats are categorized based on severity. The arrows and corresponding percentages define the trending performance over a 24-hour time period.

LANDesk publishes definitions to check for the local Windows system configuration errors and exposures.

Spyware detected

The **Spyware detected** widget shows the percentage of devices infected by one or more forms of spyware. Spyware is categorized based on severity. The arrows and corresponding percentages define the trending performance over a 24-hour time period.

Windows firewall

The **Windows firewall** widget shows the percentage of devices with Microsoft's second-generation firewall disabled or improperly configured. The data used to generate the values in the Windows firewall widget is based on the last security threat scan. If a device is modified (including turned off or on since the last scan), the data will not change and the widget will not show current information until you run the security threats scan again.

Note: If the state of some Windows XP* machines says "Disabled" or "Not Configured" in the widget, this could mean there was a problem installing ICFConfig, allowing the firewall to be opened for access by LDMS. It could also indicate the firewall has been turned off.

Latest Windows vulnerabilities

The **Latest Windows vulnerabilities** widget shows the number of devices that are vulnerable based on fixes released in conjunction with the monthly Microsoft security bulletins.

Antivirus

The Antivirus widget shows the number of devices that have real-time antivirus detection enabled and how many devices have antivirus definitions that have been updated within the last three days.

Installed OS base

This **Installed OS base** widget shows the operating systems being used on the network and the number of devices running them.

Unlicensed products

The **Unlicensed products** widget shows which applications are most commonly used on your network without a license.

Installed but not used

The **Installed but not used** widget shows the number of installed and licensed applications not being used.

Unused licenses

This **Unused licenses** widget shows the number of application licenses not being used.

Policies success rate

The **Policies success rate** widget shows the percentage of successfully deployed policies for required and optional policies.

This widget should not be used with a roll-up core server. Rolling up policy data isn't currently supported. If this widget is used with a roll-up core server, the message "No data available" will be given.

Devices scanned past week

The **devices scanned past week** widget shows the percentage of devices scanned in the past week for inventory and vulnerabilities.

The inventory meter takes into account all devices in the database as the total. Then the devices that have a scan date within the past week are counted.

The vulnerabilities meter only takes into account devices that have previously scanned for vulnerabilities. Then the devices that have a scan date within the past week are counted.

Top 5 viruses found, past 10 days

The **Top 5 viruses found, past 10 days** widget shows the five most common viruses that have been detected on the network during the past 10 days.

Top 5 viruses found, past 10 weeks

The **Top 5 viruses found, past 10 weeks** widget shows the five most common viruses that have been detected on the network during the past 10 weeks.

Computers infected with viruses, past 10 days

The **Computers infected with viruses, past 10 days** widget lists all devices on the network that have had a virus detected during the past 10 days.

Computers infected with viruses, past 10 weeks

The **Computers infected with viruses, past 10 weeks** widget lists all devices on the network that have had a virus detected during the past 10 weeks.

Configuring the executive dashboard

You control which widgets appear in the user interface and the order in which they appear. All of the widgets show by default. You can customize the view, so only information important to you is shown. This personalized view provides greater visibility over the areas you're responsible for or interested in.

The executive dashboard is arranged in a grid with three columns. You can configure which widgets appear in each column and the location they appear in.

To configure the executive dashboard

1. From the executive dashboard, click **Configure**.
2. In the **Dashboard Configuration** dialog, use the arrows between the columns to move widgets right and left to the desired columns. Change the ordering of a widget in a column by selecting it and clicking **Up** or **Down**. Hide a widget by selecting it in the column and clicking **Remove**. Add a widget to a column by selecting it the bottom box and clicking **Add**.
3. Click **OK**.

Managing local accounts

LANDesk provides an administrative tool that enables you to manage a local machine's users and groups from the console.

Read this chapter to learn about:

- "Local accounts overview" on page 285
- "Managing local users" on page 285
- "Managing local groups" on page 286
- "Assigning users to groups" on page 287
- "Changing passwords" on page 288
- "Resetting passwords" on page 288

Local accounts overview

Local accounts is an administrative tool used to manage the users and groups on local machines on your network. From the console, you can add and delete users and groups, add and remove users from groups, set and change passwords, edit user and group settings, and create tasks to reset passwords for multiple devices. If a device is turned off or not connected to the network, you won't be able to use local accounts to manage the device.

Note: When using local accounts, the core interacts with the other machines at near real-time.

Using the Core server's local account

Since your core server is a node on your network and has local accounts, you can use the local accounts tool to perform administrative tasks on the server, as well as the console itself. You can add LANDesk users to the console by creating local users and adding them to the Windows NT **LANDesk Management Suite** group. This enables you to perform administrative tasks from the console, without having to use the native local accounts management system, such as Computer Management on Windows NT.

If you prefer, you can still use the native local accounts management system to manage local accounts. You can access the devices directly, remote control the machines from the console, or use a third-party tool to access the devices and perform the administrative tasks.

For more information on using the console to perform local accounts management, see "Managing LANDesk users" on page 61.

Managing local users

You can add, delete, and edit users on a local machine from the console.

To add a user

1. In the console, from the **Network View**, click **Devices | All devices**.

2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Users** and then click **Add**.
4. In the **New User** dialog, enter a user name, a full name, and a description.
5. Enter a password, confirm the password, and specify the password settings.
6. Click **Save**.

To delete a user

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a user

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to edit and then click **Edit**.
5. Make your desired changes and then click **OK**.

Managing local groups

You can add, delete, and edit groups on a local machine from the console.

To add a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Groups** and then click **Add**.
4. In the **New Group** dialog, enter a group name and a description.
5. (Optional) Add users to the group by clicking **Add**.
6. Click **Save**.

To delete a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to edit and then click **Edit**.

5. Make your desired changes and then click **OK**.

Assigning users to groups

There are two methods for adding and removing users to and from groups on a local machine from the console. The first method allows you to add or remove multiple users to or from a group at one time. The second method allows you to add or remove the selected user to or from one or more groups.

To add users to a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to add users to and then click **Edit**.
5. In the **Edit group** dialog, click **Add**.
6. Select the users you want to add to the group and then click **Add>>**.
7. Click **OK**.
8. Click **OK** in the **Edit group** dialog.

To add a user to one or more groups

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to add to one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Click **Add**.
7. Select the groups you want the user to belong to and then click **Add>>**.
8. Click **OK**.
9. From the **Edit user** dialog, click **OK**.

To remove users from a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to remove users from and then click **Edit**.
5. Select the users you want to remove and then click **Remove>>**.
6. Click **OK**.

To remove a user from one or more groups

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to remove from one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Select the groups you want the user to be removed from and then click **Remove>>**.
7. Click **OK**.

Changing passwords

You can change a user's password on a local machine from the console.

To change a user's password

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to change the password for and then click **Set password**.
5. Enter a new password, confirm the password, and then click **OK**.
6. Click **OK** to verify the password has been changed successfully.

Resetting passwords

You can create a scheduled task to reset the password for a specific user name. Once the task has been scheduled, you are taken to the **Scheduled tasks** tool where you can specify the target devices and the start time. For example, from a local account you could create a task to reset the password for the **Administrator** user name. You would then designate the target devices and schedule when the task will occur. Once the task is run, all administrators wanting to authenticate to the target devices would have to use the new password.

To reset the password

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Click the **Schedule** icon.
5. In the **Schedule task** dialog, insert the user name that you want to reset the password for. You can select an existing user name from the drop-down list, or type a different one.
6. Enter a new password, confirm the password, and then click **Schedule**.
7. From the **Scheduled tasks** tool, right-click on the scheduled task and then click **Properties**.
8. From the **Scheduled tasks - properties** dialog, designate the target devices and enter the scheduling information.
9. Click **Save**.

File replicator

The LANDesk file replicator is a utility designed to replicate files from a remote Web server to the local system. It provides the following features:

- **File and directory support:** Replicate individual files or directories. Directory support can be recursive.
- **Multiple task support:** Multiple download tasks can be defined and run simultaneously. Each task can download resources located in different Web servers.
- **Bandwidth control:** A maximum bandwidth in percentage or actual transmission rate can be specified that will not be exceeded during the replication operation.
- **Restartable copying:** If a copy operation is interrupted because the connection is lost or time runs out, replication will resume from the point where it was interrupted when the job is relaunched.

Your Web server must be configured properly for the file replicator to work:

- The Web server's directory browsing option must be enabled.
- Some application extensions, such as .ASP and .ASPX, have special meanings in the Web server. You must remove the application extension for these kinds of files if you want to replicate them from a Web server.

Using the file replicator

The file replicator copies files from Web sites or Web shares to a folder you specify. You can create periodic repeating tasks or single tasks that run on a schedule you specify. The file replicator uses the same HTTP transfer technology that Management Suite uses for software distributions. You can limit the transfer bandwidth by kilobytes per second or by a percentage of available bandwidth.

Management Suite setup copies the file replicator to the \Program Files\LANDesk\ManagementSuite\Utilities\File Replicator folder. The replicator is a standalone Windows application and you can copy the File Replicator folder and subfolders to any server you want. If you want to access the online help, also copy Idms.chm to the same place. The default .NET Framework security configuration won't allow the file replicator to launch from a remote path. If you try to run the program remotely, nothing will happen.

To configure a replication task, you need to provide the following:

- Task parameters, such as the schedule, target folder, and bandwidth options
- Source URLs. If you specify multiple URLs, they are processed one at a time.

The file replicator caches files in the **Temporary folder** box. Once the copy finishes to the temporary directory, the replicator copies the file to the destination and deletes it from the temporary directory. This prevents partial copies from ending up on the destination if the file copy from the source is interrupted for some reason.

The file replicator stops whatever it's doing when it's opened. When you're done with the window, make sure you click **Start download**. This minimizes the replicator to the system tray and allows replication tasks to execute.

The file replicator configuration file, stored in XML format, needs to be created before you can do any replication tasks. There is no default XML configuration file. This XML configuration file can be the same or different on each server.

If the user logs off, the file replicator process in the system tray terminates. Usually with servers, file replicator must be launched when a user is not logged in. This can be done using Microsoft's Task Scheduler service or LANDesk's Local Scheduler service, as described in "Scheduling replication from the command-line" on page 291.

To create a replication task

1. Launch the file replicator.
2. From the **New** button's menu, click **New periodic task** or **New single task**.
3. Enter a task **Name**.
4. Enter or **Browse** for the **Destination folder**.
5. Enter or **Browse** for the **Temporary folder**.
6. Set the time you want the replication task to occur. If the task doesn't finish in the time allowed, it will resume from the point it left off the next time the task runs.
7. Select the bandwidth options you want. You can specify a value in kilobytes per second, a percentage of available bandwidth, or none.
8. Click Add to enter source URLs. The address must be in the form of http://server/path. If necessary, specify the credentials necessary to access the URL. When you're ready, click **Browse**. If the URL and credentials work, you'll see the destination in the lower half of the dialog. Check **Download recursively** if that's what you want. Click OK when you're done.
9. Repeat step 8 for each URL you want to replicate.
10. Click **Save** when you're done.
11. When you're done configuring tasks, click **Start download** to activate file replication on the schedule you specified. The file replicator minimizes to the system tray.

The file replicator stores a log of its actions.

To view the file replicator log

1. Launch the file replicator.
2. Click the **View log** toolbar button.

You can reschedule a single task. This resets the task so it will run again.

To reschedule a task

1. Launch the file replicator.
2. Select the single task you want to reschedule.
3. Click the **Reschedule task** toolbar button.

Understanding the bandwidth options

The file replicator uses bandwidth options to make sure replication doesn't saturate a device's available bandwidth. Any bandwidth options you specify apply to the device the replicator is copying files from, not the destination. There are two bandwidth options the replicator can use:

- **Value(KB):** The amount of bandwidth, in kilobytes/sec, that the job can use. Values must be in the range of 2 to 10000.
- **Percentage(%):** The amount of network bandwidth. Values must be in the range of 5 to 100.

Bandwidth options are set on a per-job basis. If you have multiple file replication jobs active at once, the job bandwidth settings can interact. For example, if you have one job that's allowed 100 KB/sec second, and another that's allowed 50 KB/sec, the total bandwidth used if the two jobs are active at the same time will be 150 KB/sec. With percentage of available bandwidth, it's slightly more complicated. If you have two jobs that are allowed 50% of available bandwidth, the total bandwidth used by both jobs won't exceed 50% of the total. Each job will end up with about 25% of the available bandwidth.

Scheduling replication from the command-line

Management Suite ships with two file replicator versions:

- The graphical version (LANDeskFileReplicator.exe), which only runs when a user is logged on.
- The command-line version (LANDeskFileReplicatorNoUI.exe), which you can run from Microsoft's Task Scheduler or the LANDesk local scheduler. Running the file replicator this way doesn't require a logged-on user.

The graphical and command-line file replicators use the same XML-format configuration file. Before using the command-line file replicator, you need to use the graphical file replicator to create an XML configuration file.

The following is the syntax for LANDeskFileReplicatorNoUI.exe:

```
LANDeskFileReplicatorNoUI.exe configfile [logfile]
```

Here is an example:

```
LANDeskFileReplicatorNoUI.exe LDHTTPCopyTaskConfig.xml replicator.log
```

The following sections describe to ways you can schedule LANDeskFileReplicatorNoUI.exe from the command-line.

- "Scheduling replication using LANDesk's Local Scheduler service" on page 292
- "Scheduling replication using the Microsoft Task Scheduler service" on page 292

The examples in the steps below assume that each package server has two hard drives: the C drive for the operating system; and the D drive for data storage. It also assumes that each server is configured to have a web share named Packages that has a local patch of D:\Packages.

Scheduling replication using LANDesk's Local Scheduler service

LANDesk's Local Scheduler service is installed with the LANDesk agent configuration. The file used is LocalSch.exe. If your server isn't managed by LANDesk, this service won't exist and you'll have to use the Microsoft task scheduler instead. For more information on the local scheduler, see "Using the local scheduler" on page 144.

Once you've copied the file replicator files and XML configuration file to your server, enter the following at a command prompt to schedule replication to occur every 20 minutes:

```
"%programfiles%\LANDesk\LDClient\LocalSch.exe" /taskid=1 /freq=1200
/exe="%ProgramFiles%\LANDesk\File
Replicator\LANDeskFileReplicatorNoUI.exe"
/cmd=" " "%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml" "
"%ProgramFiles%\LANDesk\File Replicator\replicator.log" " "
```

Note that the three quotes after /cmd= in the examples below is not a mistake. Three quotes are required to handle parameters that include quotes themselves.

To change the launch interval, change the /freq= parameter's value to the number of seconds you want. In the example above, 1200 seconds equals 20 minutes.

To verify that a task was created, run the following command:

```
"%programfiles%\LANDesk\LDClient\LocalSch.exe" /tasks |more
```

Scheduling replication using the Microsoft Task Scheduler service

You can also control Microsoft's task scheduler from the command-line with the SCHEDULE command. SCHEDULE can schedule LANDeskFileReplicatorNoUI.exe to run almost any time.

For more information on SCHEDULE, see:

<http://technet2.microsoft.com/windowsserver/en/library/1d284efa-9d11-46c2-a8ef-87b297c68d171033.mspx?mfr=true>

Once you've copied the file replicator files and XML configuration file to your server, do the following to schedule replication to occur at the interval you want (the example below uses every 20 minutes).

To schedule replication every 20 minutes with Microsoft's task scheduler

1. In the %ProgramFiles%\LANDesk\File Replicator directory, create a batch file called "File Replicator.cmd" that contains the following line.

```
"%ProgramFiles%\LANDesk\File  
Replicator\LANDeskFileReplicatorNoUI.exe "  
"%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml "  
"%ProgramFiles%\LANDesk\File Replicator\replicator.log"
```

2. Open a command prompt on the package server by clicking **Start | Run** and typing **CMD**.
3. Enter the following command.

```
schtasks /create /ru system /sc minute /mo 20 /tn "File Replicator  
every 20 minutes" /tr "%ProgramFiles%\LANDesk\File Replicator\File  
Replicator.cmd"
```

Note: The commands should be entered as a single command line.

4. To verify that the task was created, run SHTASKS with no parameters and the task details are displayed.

If you want to schedule hourly replication, change the schtasks command-line above to the following:

```
schtasks /create /ru system /sc hourly /tn "File Replicator hourly" /tr  
"%ProgramFiles%\LANDesk\File Replicator\File Replicator.cmd"
```

If you want to schedule daily replication, change the schtasks command-line above to the following:

```
schtasks /create /ru system /sc daily /tn "File Replicator daily" /tr  
"%ProgramFiles%\LANDesk\File Replicator\File Replicator.cmd"
```

Managing Macintosh devices

LANDesk provides the most complete system management for Apple Macintosh computers and devices. This enables IT professionals to automate systems management tasks throughout the enterprise. From the console, you can gather and analyze detailed hardware and software inventory data from each device. Use the data to select targets for software distributions and to establish policies for automated configuration management. Manage software licenses to save costs and monitor compliance with license agreements. Remote control devices to resolve problems or perform routine maintenance. Protect your devices from a variety of prevalent security risks and exposures. Keep track of your inventory and produce informative reports.

Read this chapter to learn more about:

- "LANDesk for Macintosh overview" on page 294
- "Agent Configuration for Macintosh devices" on page 295
- "Inventory for Macintosh devices" on page 300
- "Software Distribution for Macintosh devices" on page 302
- "Managed scripts for Macintosh devices" on page 305
- "Remote control for Macintosh devices" on page 306
- "Reporting for Macintosh devices" on page 307
- "Scheduled tasks for Macintosh devices" on page 307
- "Software license monitoring for Macintosh devices" on page 307
- "Security and Patch Manager for Macintosh devices" on page 308
- "Local scheduler for Macintosh devices" on page 309
- "Managing a Macintosh device" on page 309
- "Using the Mac remote control viewer" on page

Macintosh OS deployment support is included as of 8.7 SP3. For more information, download the operating system deployment for Macintosh white paper from <http://community.landesk.com/support/docs/DOC-1192>.

LANDesk for Macintosh overview

This chapter pertains to how LANDesk is used to manage Macintosh computers. It provides a central location for referencing specific information on Macintosh-related tasks, tools, features, and functionality. For broader information about using tools and features to manage your network, refer to the chapter pertaining to the tool of interest.

Mac OS X

You can use all supported features with Mac OS X devices, which are described below. LANDesk currently supports the following versions of Mac OS X:

- Leopard 10.5
- Tiger 10.4 (PowerPC and Intel)
- Panther 10.3
- Jaguar 10.2

Mac OS 9

You can use inventory and remote control with Mac OS 9 devices. This OS is in the process of being phased out, so only limited support is available. Few updates will be performed as needed.

Agent Configuration for Macintosh devices

LANDesk uses agent configurations to gain control of devices and manage them. Macintosh devices first need to have an agent manually loaded (via a pull). Then new configurations can be created and deployed via a push from the server. Agents are components provided by the server to the client devices that make them fully manageable from the console.

Loading the default Agent Configuration for Macintosh devices

The Default Mac Configuration package contains the required agents for controlling Macintosh devices. In order to gain control of your Macintosh devices, you need to:

1. Obtain the necessary package (agents).
2. Deploy the agents to the devices.
3. Install the agents on the machines.

After the default agents have been installed, your devices become managed devices. Then you can create custom configurations to have greater control of your Macintosh devices. Custom agents are easily implemented once your devices are managed.

Note: All devices must support TCP/IP.

Obtaining the package (agents) for Macintosh devices

You can obtain the default package from the LDLogon/Mac shared folder on your core server. The LDLogon/Mac folder is automatically created during the installation of LANDesk. Since the LDLogon folder is a Web share, it is available from the Internet at <http://<CoreServerName>/LDLogon/Mac>. The packages you need depend on the operating system version:

OS version	Package
Mac OS X	Default_Mac_Configuration.pkg.zip
Mac OS 9	Default_Mac_Configuration.ini LANDesk_Classic_Client.sit

Deploying agents to Macintosh devices

You need to decide on a deployment method to place the agents on the target Macintosh devices. Since there are no domain-level administrative accounts that give you access to Macintosh devices, there are no login scripts for Macintosh devices, and Apple ships with all services disabled for security reasons, the only way to natively deploy the agents is to perform the procedure manually. Due to these difficulties, in many organizations the only way to initially deploy the Mac OS X agents is to:

- Access the agent using a Web browser from LDLogon/Mac (see "Obtaining the package (agents) for Macintosh devices" on page 295). E-mail the configuration package to users.
- Put the configuration package on a CD or other removable media and take it to each Macintosh device.

There are third-party Macintosh software distribution applications you can use to deploy the agents to the devices. Otherwise, you'll have to deploy the agents manually as described above. The third-party software distribution applications for Macintosh are:

- Apple Remote Desktop
- Apple Network Administrator
- netOctopus
- Timbuktu
- FileWave
- FoolProof
- Secure Shell (SSH)

Use your deployment method to place the appropriate package with the corresponding agents on the target devices.

Installing agents on Macintosh devices

Once you have deployed the agents to the target devices, you need to install them on the machines. A full hardware and software scan is run at the end of every install, which synchronizes the devices with the core sever. You must have the LANDesk agents installed on your Macintosh devices and their inventory information sent to the core server before you can manage them. After you've installed the base agents, subsequent agent deployments and updates are easily handled through the existing agents.

Note: LANDesk agent cannot be installed if ZIP software is not present on Mac OS X 10.2.8

To install agents for Mac OS X

1. On the client machine, locate **Default Mac Configuration.pkg.zip** or access the package from the Web share (see "Obtaining the package (agents) for Macintosh devices" on page 295).
2. Unzip the file or copy the files to the target device.
3. Double-click **LDMSClient.pkg**.
4. Reboot the machine.

To install agents for Mac OS 9 devices

1. On the client machine, locate **LANDesk_Classic_Client.sit** and **Default_Mac_Configuration.ini** or access them from the Web share (see "Obtaining the package (agents) for Macintosh devices" on page 295).
2. Decompress **LANDesk_Classic_Client.sit**, if not already decompressed. This will create the **LANDesk Classic Client** folder.
3. From the core server's **ldlogon/Mac** directory, select the **Default Mac Configuration.ini** file and make a copy of it locally. Rename it **com.landesk.ldms.ini**.
4. Drag and drop the **com.landesk.ldms.ini** file from the core into the **LANDesk Classic Client** folder on the client and replace the old **com.landesk.ldms.ini** file with the new file you just created. If prompted, overwrite the file.
5. Launch the **Mac Client Install**.
6. Reboot the machine.

Creating agent configurations for Macintosh devices

Use the Agent configuration tool to create and update (replace) custom configurations for your Macintosh devices. You can create different configurations for your specific needs, such as changing inventory scanner settings, remote control permissions, or what network protocols the agents use.

In order to push a configuration to devices, you need to create or update an agent configuration and schedule the task to occur.

Creating or updating the agent configuration

Set up specific configurations for your devices. Don't use parentheses in your Macintosh agent configuration names. Parentheses in the name will cause the deployment task to fail.

To create an agent configuration for Macintosh devices

1. Click **Tools | Configuration | Agent configuration**.
2. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the Agent configuration dialog. For more information, see "Using the Agent configuration dialog (for Macintosh)" on page 298, or click **Help** in the dialog.
4. Click **Save**.

To update an agent configuration

1. Click **Tools | Configuration | Agent configuration**.
2. Right-click the agent configuration to be updated and select **Properties**.
3. Make the updates to the agent configuration.
4. Click **Save**.

Scheduling the agent configuration

You can push agent configurations to devices that have the standard LANDesk agent installed. Use the **Scheduled tasks** tool to run your new or updated agent configuration.

To schedule an agent configuration for Macintosh devices

1. Click **Tools | Configuration | Agent configuration**.
2. Right-click the agent configuration to be scheduled and select **Schedule**.
3. Target devices for the task and start the task.

Manually running agent configuration for Macintosh devices

You can manually run agent configurations for Macintosh devices once they have been created or updated. When an agent configuration is created (**Tools | Configuration | Agent configuration**), the following files are created in the LDLogon/Mac folder on your core server:

- **<agent configuration name>.pkg.zip** (for Mac OS X)
- **<agent configuration name>.ini** (for Mac OS 9 devices)

The LDLogon/Mac folder is a Web share and should be accessible from any browser. Follow the instructions for "Loading the default Agent Configuration for Macintosh devices" on page 295. Insert your agent configuration files instead of the default files.

Uninstalling Mac OS X

If you want to uninstall the Mac OS X agents, run the uninstall script, **lduninstall.command**, located on each device in the /Library/Application Support/LANDesk folder. You will need to provide an administrator password.

Uninstalling Mac OS 9

If you want to uninstall the Mac OS 9 agents, run the uninstall script from: **HD:System Folder:Application Support:LANDesk:Mac Client Uninstall**.

Using the Agent configuration dialog (for Macintosh)

This section describes the agent configuration dialog for Macintosh devices. The dialog consists of the following:

- Application policy management
- Inventory
- Remote control
- Standard LANDesk agent
- LANDesk Trust Agent

About the Application policy management page

Use this page to specify the port the policy-based distribution agent will use to communicate with the core server. The default port is 12175. You'll need to make sure this port is open on any firewalls between devices and the core server. If you change this port, you'll also need to change it on the core server. You can change the port the QIP server service uses by editing the following registry key:

- HKLM\Software\Intel\LANDesk\LDWM\QIPsrvr

About the Inventory page

Use this page to configure the inventory scanner.

- **Send scan to LDMS core server:** Enter the core server name or IP address. This is the server the agent sends scan information to. No scan information goes to the core database unless this server address is correct.
- **Save scan in directory:** The directory where the data from the scan is saved. If you select both the core server option and this option, the scan information will go to both location.
- **Choose scan components:** Select the components you want to scan. Not selecting all components may slightly increase scanning speed.
- **Force software scan:** Forces the device to do a software scan with each inventory scan, regardless of whether the core server indicates one is due.
- **Scan applications folder only:** For software scans, only scans for applications in the applications folder. This can increase scanning speed, though it will miss applications stored outside this folder.

About the Remote control page

Use this page to configure the remote control agent.

- **Permission required:** Prompts the user for permission to be remote-controlled whenever someone initiates a remote control session. If the user isn't at the keyboard or denies permission, the remote control session won't start.
- **Open applications and files:** Permits a remote user to open files on this device.
- **Copy items:** Permits a remote user to copy files to and from this device.
- **Delete and rename items:** Permits a remote user to delete or rename files that reside on this device.
- **Lock keyboard and mouse:** Permits a remote user to lock your keyboard and mouse during a remote control session. This option prevents you from interfering with remote actions.
- **Blank screen:** Permits a remote user to make your screen go blank during a remote control session. This option is useful if your device contains sensitive documents that an administrator may need to open remotely without letting others read if they happen to walk by your device monitor.
- **Restart and shut down:** Permits a remote user to restart or shut down your device.
- **Control and observe:** Permits a remote user to remote control and observe your actions on this device. The administrator can't do anything except watch your actions.

- **Alert when observing:** When a remote control session is active, display a visual cue in the menu bar.

About the Standard LANDesk agent page

Use this page to configure agent security and management scope. For more information on agent security, see "Agent security and trusted certificates" on page 90. For more information on scope, see "Role-based administration" on page 59.

- **Trusted certificates:** Lists the certificates on the core server. The client must have a certificate that matches the certificate on the core server for agent communication to be authorized. These certificates are used to authenticate agent communication. The remote control agent for Macintosh doesn't use a certificate.
- **Path:** Defines the device's computer location inventory attribute. Scopes are used by role-based administration to control user access to devices, and can be based on this custom directory path. The path is optional.
- **Fully qualified domain name support:** You can enter in a domain name or IP address for the client to use when communicating with the LANDesk core server.

About the LANDesk Trust Agent page

Use this page to configure the LANDesk Trust Agent (LTA). Once LTA is installed on a device, it can validate with the LANDesk DHCP server and posture validation server. For more information on LTA, see "Understanding the basic LANDesk NAC components" on page 372.

- **LANDesk Trust Agent:** Causes the LTA agent to be installed on the device when the agent is deployed.

Inventory for Macintosh devices

The inventory scanning utility is used to add Macintosh devices to the core database and to collect device hardware and software data. When you configure a device, the inventory scanner is one of the components of the LANDesk agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database.

The scanner executable for Mac OS X is called **ldscan** (UNIX; it is case sensitive). Inventory scan files are saved locally on the client and are compatible with the core. You can e-mail the file to the core administrator and then drag and drop it into the ldscan directory. You need to change the extension of the file to .SCN.

Macintosh devices can be configured to scan at boot-up, at log in, at wake from sleep, and at network change. You can also set up a cron job to schedule the inventory scan to occur at a regular interval.

The Macintosh inventory scanner encrypts scans. The inventory scanner also uses delta scans so that after the initial full inventory scan, subsequent scans send only the changed data to the core server, reducing network bandwidth consumption.

Note: The scanner executable for Mac OS 9 devices is named **LANDesk Inventory Agent**. These devices only scan at boot-up.

The Macintosh inventory scanner looks in the "Custom Data" folder under the agent installation folder for XML files that contain additional information you want the inventory scanner to pass to the core server. This additional information appears in the inventory tree under the Custom Data node.

With the inventory scanner, you can view summary or full inventory data. You can print and export the inventory data. You can also use it to define queries, group devices together, and generate specialized reports. For more information about the Inventory tool, see [Managing inventory](#).

Software scanning

Software scans inventory software on managed devices. These scans take longer to run than hardware scans. Software scans can take a few minutes to complete, depending on the number of files on the managed device. By default, the software scan runs once a day, regardless of how often the inventory scanner runs on the device. You can configure the software scan interval in the **Configure | Services | Inventory** tab.

All applications installed in the Applications folder are placed into the **Software | Application Suites** node in the inventory tree.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner's (ldscan) shortcut properties to control how it functions.

Option	Description
-F	Forces a software scan even when none of the software scanning options have been selected in the agent configuration. Example: [MACHINES_MACX] REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldscan -F
-C	Specifies which core the scan is sent to. Example: c spencercore2.landesk.com
-O	Specifies which directory you want the scan file to go to. Example: -o /Users/spencer

Editing the LDAPPL3.TEMPLATE file

The LDAPPL3.TEMPLATE file contains the scanner's inventory parameters. This template file works with the LDAPPL3 file to identify a device's software inventory.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in this directory on the core server:

- \Program Files\LANDesk\ManagementSuite\LDLogon

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
MacMode	<p>Determines how the scanner scans for Macintosh software on devices. The default is All. Here are the settings:</p> <ul style="list-style-type: none">• Listed: Records the files listed in LDAPPL3.• Unlisted: Records the names and dates of all files that have the extensions listed on the MacScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network.• All: Discovers files with extensions listed on the MacScanExtensions line.

You need click **Make available to the clients**, so they can download the MacModes. MacScanExtensions is turned on by default. This can create very large scan files (11 MB+), so you may want to change these defaults.

Note: The /Library or /System directories are not scanned in a MacScanExtensions scan by default. This reduces the size of the scan file. The directories can be placed in the Mac folder include section.

Software Distribution for Macintosh devices

Software distribution enables you to deploy software and file packages to Macintosh devices on your network running Mac OS X.

You can distribute single-file executable packages to Mac OS X devices. Each distributed package consists of only one file, and the agent will try to install the file once the device receives it. Any file can be downloaded. Install packages (.PKG) can also contain directories, but they must be compressed. If the file downloaded has a suffix of .DMG, .PKG, .MPKG, .SIT, .SITX, .ZIP, .TAR, .GZ, .SEA, .APP, .SH, .HGX, or Automator/workflow packages, LANDesk will decompress the file before returning (Automator packages will only work on versions 10.4.2 or later).

Note: Users should make sure that Stuffit Expander* has its "check for new versions" option disabled; otherwise a dialog may interrupt the software distribution execution.

Software distribution also provides the ability to distribute shell scripts as jobs. This enables IT to take even greater control over the Mac operating environment and perform nearly any configuration or information gathering task on a MacOS X computer.

You can schedule Mac OS X distributions in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as distribution targets (see [Scheduled tasks for Macintosh devices](#)).

Note: You must install LANDesk's Mac OS X agent on the target devices before you can distribute files to them.

A distribution package consists of the package files you want to send and distribution details, which describe the package components and behavior. You must create the package before it can be delivered and run. The following instructions explain how to perform software distribution. In order to execute it correctly, the software distribution package must exist on either a network or Web server and the recipient devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices:

1. Create a distribution package for the software you want to distribute
2. Create a delivery method
3. Schedule the script for distribution

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools | Distribution | Distribution Packages**.
3. Under **My distribution packages**, **Public distribution packages**, or **All distribution packages**, right-click **Macintosh** and select **New distribution package**.
4. In the **Distribution package** dialog, enter the package information and set the options. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your distribution appears under the tree item for the package type you selected.

To create a delivery method

1. If you've already configured a delivery method that you want to use, skip to the next procedure (To schedule a script for distribution).
2. Click **Tools | Distribution | Delivery Methods**.
3. Right-click the delivery method you want to use and then click **New delivery method**.
4. In the **Delivery method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method you selected.

To schedule a script for distribution

1. Click **Tools | Distribution | Scheduled Tasks**.
2. Click the **Create software distribution task** toolbar button.
3. On the **Schedule task** page, enter the task name and the task schedule.
4. On the **Delivery Methods** page, select the delivery method you want to use.
5. On the **Distribution package** page, select the package script you created.
6. On the **Target machines** page, add the devices you want to receive the package.
7. On the **Summary** page, confirm the task is configured correctly.
8. Click **OK** when you're done.

View the task progress in the Scheduled tasks window.

You can use queries to create a list of devices to deploy a package to. For information on creating queries, see "Database queries" on page 104.

Macintosh software distribution commands

Macintosh software distribution commands are download commands, as opposed to a shell command (see "Managed scripts for Macintosh devices" on page 305). Download commands begin with either "http://" or "ftp://". If it's not a download command, it's a shell command by definition. The following is an example of a download command:

```
REMEXEC0=http://...
```

A download command won't autorun any files. After downloading the file to devices, you can follow up with a shell command to execute the file. Files are downloaded to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in your shell commands.

Note: If you're hosting files on a Windows 2003 server, you need to create MIME types for the Macintosh file extensions, such as .SIT, otherwise the 2003 server won't let you access the files. The MIME type doesn't have to be valid, it just needs to exist.

Configuring policies for Macintosh devices

You can also create Macintosh device policies (Mac OS X only). Creating a Macintosh device policy is similar to creating a policy for a Windows-based device. Macintosh devices also have the same required, recommended, and optional policy types. Macintosh application packages must be a single-file format. Policy-based management will check for policy updates at an interval of four hours. For optional or recommended policies, the client user needs to launch the LANDesk preference pane and click **Check now** for policy-based distribution. When targeting policies, Macintosh devices don't support policy-based management by user name, only by device name.

Policy-based management does the following with Macintosh application policy packages:

1. Downloads files to /Library/Applications/LANDesk/sdcache (just like software distribution downloads) .
2. If the download is compressed, policy-based management will decompress it in place.
3. If the download is a disk image, policy-based management will mount it, look for the first Apple Package Installer file found on the mounted volume, run it silently, and then unmount it.
4. If the download is an Apple Package Installer file, policy-based management will run it silently.

Also, policy-based management does support .DMG files with EULAs.

Note: Some package types don't work well with software distribution.

Installer Vise and Installer Maker installers don't work well with policy-based management. They almost always require user interaction and can be canceled.

To add a Macintosh client policy

1. Click **Tools | Distribution | Delivery methods**.

2. Configure a Hybrid or Policy delivery method for the package you want to distribute.
3. Click **Tools | Distribution | Scheduled tasks**.
4. Click the **Create software distribution task** button.
5. Configure the task. Click **Help** on each page if you need more information.

To refresh the local client policies

1. In the Management Suite Preference Pane on the Macintosh device, click the **Overview** tab.
2. Click **Check now** for application policy management.

To view installed policies

- In the Management Suite Preference Pane on the Macintosh device, click the **APM** tab.

Exposing the UI to the client

You have the option of showing or hiding the UI to the client when distributing a software package. If the LANDesk administrator is pushing out a package that requires the user to select a license agreement, the package needs to be installed using a user-controlled type delivery method because the package will not install if the license agreement is not accepted by the end user. You can expose the UI for either a push- or policy-based delivery method.

To show the UI to the client during software distribution

1. Create a new software distribution delivery method or select an existing method to edit.
2. Select **Feedback** from the tree.
3. Select **Display progress to user** and then select **Display full package interface**.

Managed scripts for Macintosh devices

LANDesk uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools | Distribution | Manage scripts**). Macintosh scripts use shell commands to execute files. Shell commands run as root. The scripts are saved as text files, and you can edit them manually if you need to once they're created. The following is an example of a shell command:

```
REMEXEC0=...
```

The user can use the shell command "open" to launch files and applications, or "installer" to install .PKG files. It's also possible for the download file to be a shell script written in Perl, Ruby, Python, and so on.

When files are downloaded, they are saved to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in order to execute some of your shell commands.

You can schedule Mac OS X managed scripts in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as script targets (see "Scheduled tasks for Macintosh devices" on page 307).

Remote control for Macintosh devices

You can remote control a Macintosh device from the console the same way you would a Windows device. Before you can perform any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see the connection messages and status in the **Connection messages** pane (**View | Connection messages**). LANDesk's integrated security checks to see if the user initiating the remote control session has the appropriate rights and that the machine is part of the user's scope. The data is obfuscated as it is passed over the network.

Note: Integrated security is turned on by default. It is only supported for versions 10.3.9 and up. If integrated security is installed on a machine that was released before version 10.3.9, the client will automatically switch to local security.

Key mapping

Macintosh keyboards have some keys that PC keyboards don't have. When remote controlling a Macintosh device, the following keys are used on the PC keyboard to emulate a Macintosh keyboard:

- The Alt keys map to the Command key.
- The Window keys map to the Option key.

You need to have system key pass-through enabled in the remote control viewer window for the Alt and Windows keys to pass their Macintosh mappings.

Note: Clipboard sharing and draw features are not supported on Macintosh devices.

For more information, see [Using remote control](#).

Connecting to a device

You can connect to a Macintosh device and remote control it.

To connect to a device

1. In the **Network view**, right-click the device you want to remote control, and then click **Remote control**, **Chat**, **File transfer**, or **Remote execute**.
2. Once the viewer window appears and connects to the remote device, you can use any of the remote control tools available from the **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File | Stop connection**.

Command line remote control

You can remote control a Mac machine from the command line on a machine that has the remote control container installed. Use the following command:

`ircntr.exe /a[client name] /s[core name]`

Remote control features

The inactivity timeout specifies a period of time (10 minutes by default) that if the client hasn't received mouse or key moves, the session is terminated. Similar to a screen saver, it prevents others from using the remote computer if it is left unattended.

Note: Inactivity timeout is not supported on Jaguar (10.2.8) because one of the operating system APIs will hang forever.

Reporting for Macintosh devices

The reporting tool enables you to generate a wide variety of specialized reports that provide critical information about the Macintosh devices on your network. The reporting tool operates the same way for all operating systems. For more information, see "Reports" on page 123.

Scheduled tasks for Macintosh devices

The scheduled tasks tool actuates or starts many of the tasks you set up or configure in the application. These tasks can be run immediately, scheduled to occur at a later time, or configured to run on a regular basis. Both the core server and managed devices have services/agents that support scheduled tasks. For more information, see "Scripts and tasks" on page 136.

Note: Before you can schedule tasks for a device, it must have the standard LANDesk agent installed and be in the inventory database.

The following procedures require the use of the scheduled tasks tool:

- Agent configuration deployment
- Software distribution
- Managed scripts
- Operating system deployment
- Security and patch manager

Software license monitoring for Macintosh devices

Macintosh devices running Mac OS X support software license monitoring. With each inventory scan, the Macintosh software monitoring agent sends information to the core server about the applications that devices run. The Software license monitoring window shows Macintosh applications along with Windows applications. You can deny Macintosh application execution in the same manner by adding Macintosh applications to the **To be denied** list.

Macintosh applications don't come prebundled in the LDAPPL3.INI file. You will have to set the LDAPPL3 file mode to "all" or "unlisted" first so that Macintosh applications are in the database to be dispositioned. When you think that all of the Macintosh applications are included, you can then set the mode back to "listed." The "to be excluded" mode is also supported.

You can scan for files based on their extensions. The LDAPPL3.INI file contains the list of extensions to scan for. By default, .DMG and .PKG file types are scanned for. You can insert additional extensions into the LDAPPL3.INI file, which is located in the **/Library /Applications /System /User** folders by default. The file location can be changed as well. You can also use the LDAPPL3.INI file to scan for multimedia files.

Macintosh devices can use the LANDesk Client pane's Software license monitoring tab (from **System Preferences**) to show what applications are installed and how often they have been used. This tab also shows blocked applications that won't launch on the device.

Security and Patch Manager for Macintosh devices

Security and Patch Manager is a complete, integrated security solution that helps you protect your Macintosh devices from a wide range of prevalent security risks. The tool allows you to manage security and patch content, scan devices, use patches, and remediate devices.

Note: Security and patch manager only supports Mac OS X devices.

Configuring Macintosh devices for security scanning and remediation

Before Macintosh devices can be scanned for vulnerabilities and receive patch deployments or software updates, they must have the Security and Patch manager agent installed. The Security and Patch manager agent is part of the standard LANDesk agent for Macintosh devices. If vulnerabilities are detected, remediation can be performed on the affected device.

Launching the scanner for Macintosh devices

You can launch the scanner from the console or manually on the client machine.

To launch the security scanner

1. Open the Mac OS X **System Preferences** on the target device and select the **LANDesk Client** panel.
2. On the **Overview** tab, click **Check Now** in the Security and Patch Manager section.

Local scheduler for Macintosh devices

Local scheduler uses cron jobs to handle Management Suite tasks on Macintosh devices, such as running the inventory scanner periodically. In order to configure the time intervals, you need to unzip the Mac agent configuration package and modify the `ldcron.xml` file. You can modify the following configurations:

- Inventory scans are set by default to run once per day with a two-hour randomization interval.
- Patch scans are set by default to run once per week with a two-hour randomization interval.
- Policy scans are set by default to run once every four hours at a 30-min randomization period.
- Cleaning the `sdcache` directory is set by default to run once per week.

Managing a Macintosh device

From a Macintosh device, you can manage LANDesk services running on the device, as well as perform general administrative tasks like creating new users, locking/unlocking the device configuration, logging in as a different user, and uninstalling LANDesk agents.

System requirements

The device needs to meet or exceed the following system requirements:

- Power Macintosh, Power Mac, PowerBook, iMac, eMac, or iBook with a G3 processor or better, at 400 MHz or faster
- Mac OS X version 10.2 or later
- 128 megabytes (MB) of physical random-access memory (RAM)
- 12 megabytes (MB) of free hard disk space

Managing LANDesk services on a Macintosh device

The LANDesk Client dialog in System Preferences is used to manage the LANDesk services on Macintosh devices (**System Preferences | LANDesk Client**). Configuring the services defines how the server will interact with the device.

The dialog enables you to specify the LDMS core server address. You can lock the dialog to prevent other users from making changes to the device's configuration.

The LANDesk Client dialog consists of the following tabs:

- Overview
- Policy-based distribution
- Inventory scanner
- Remote control
- Software license monitoring

Overview

The Overview page provides status and usage information for services running on the device. From this page, you can also check policy-based distribution, start the inventory scanner, or check patch management.

Policy-based distribution

The Policy-based distribution page lists the policies that are installed on the device and the dates they were installed.

Inventory scanner

The Inventory scanner page enables you to configure how the device will interact with the server during an inventory scan.

The page consists of the following options:

- **LDMS server address:** Specifies the core server or IP address that you send scan files to.
- **Send scan to LDMS server:** Sends data collected from the scan to the core server.
- **Save scan in directory:** Sends data collected from the scan to the specified directory.
- **Choose scan components:** Specifies which components the inventory scanner will collect data on.
- **Force software scan:** Forces a software scan to be done whenever a hardware scan is conducted.
- **Scan applications folder only:** Scans the applications folder only for applications. When selected, the software scanning shouldn't scan for applications outside of the applications folder.

Remote control

The Remote control page enables the configuration of what users can do when they take control of the device.

The page consists of the following options:

- **Allow user to do the following to this computer:** Specifies what the user is able to do if they take control of the device, such as opening applications and files, copying items, deleting and renaming items, locking the keyboard and mouse, blanking the screen, restarting and shutting down the computer, and controlling and observing the device, including showing the device when it's being observed.
- **Permission required:** Requires the console user to receive permission from the device before any kind of remote access is granted.

Software license monitoring

The Software license monitoring page lists the applications that are running on the device, how many times each application has launched, how many times the applications have been denied, and the duration the applications have been running. It also contains a list of all applications to be denied.

Using the Mac remote control viewer

Use the remote control viewer to remotely access a device. You can only remote control Windows and Mac devices that have the LANDesk agent installed. During a remote control session, the remote device actually has two users--you and the end user. You can do anything at the remote device that the user sitting at it can do.

Once you've taken control of a remote device, its screen appears in the viewer window. Because the viewer window often isn't as big as the remote device's screen, you'll either need to use the scroll bars to scroll up, down, and side to side, or use the **Scale** feature to rescale the remote screen representation so it fits in the viewer window. Scaling reduces the image quality, and if the scaler has to reduce the screen size too much you may have a hard time reading text.

You can also increase the viewer window displayable area by disabling items in the **Session** menu, such as the chat and log panes or the toolbar. Use the **Session** menu's **Full screen** option to completely remove the viewer window's controls. If the remote screen's resolution exceeds yours, it will be scaled to fit your monitor.

If you want to speed up the viewing rate or change the viewer window settings, use the **LANDesk Remote Control** menu's **Preferences** option to display the **Options** dialog.

Read the following sections for more information:

- [Connecting to devices](#)
- [Chatting with remote devices](#)
- [Sending special key sequences](#)
- [Using remote control without viewing the remote screen](#)
- [Customizing remote control](#)

Connecting to devices

Before you can do any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see connection messages and status in the log pane, if that is visible. If it isn't, you can display it by clicking **Session | Show log**.

The easiest way to launch the viewer is to right-click a device in the Windows or Web console and click **Remote control**. If you launch the viewer manually, it will first prompt you to enter the client address for the device you want to remote control. After you provide that, you'll be prompted for the core server name and the username and password for a user in the LANDesk Management Suite group on the core server that has remote control rights. The viewer needs these credentials to authorize the remote control session.

If you want to start a new session, click **File | New**. To stop a session, click **File | Close**. If the **Session** menu options are dimmed, you aren't connected to a device.

Chatting with remote devices

You can use the remote control viewer to remotely chat with a user at a remote device. This feature is useful if you need to give instructions to a remote user whose dial-up connection is using the only available phone line. Users can respond back using the chat window that appears on their screen. You can only use chat on devices that have the LANDesk Agent for Mac installed. This feature works even if you're not viewing a remote device's screen.

If you want to save the messages from a chat session, you can. Any text appearing in the gray area of the chat session will be saved to a text file.

To chat with a user at a remote device

1. Once you're connected to a remote device, click **Session | Show chat**.
2. A chat frame appears on the right side of the viewing window. The top section shows sent and received messages. The bottom section is where you can type your message. Press enter to send a message you've typed.

Your message will appear on the remote device's screen. A user can respond by typing a message and clicking **Send**. The user also can click **Close** to exit out of a chat session.

To save messages from a chat session

1. In the chat area of the viewer window, click **Save messages**.
2. In the **Save as** dialog, type in a filename and click **Save**.

Sending special key sequences

You can send special key sequences such as Alt-Tab to remote devices. You need to use a menu item to send these key sequences to prevent your local OS from intercepting them.

Once you're connected to a remote device, click **Session** and click the special key sequence you want. The available special key sequences vary, depending on the operating system you're remote controlling.

- Send Alt-Tab
- Send Ctrl-Esc
- Send Ctrl-Alt-Del
- Send Command-Tab

Using remote control without viewing the remote screen

If you don't want to see the remote device's screen but you still want to be able to chat with a user at the remote device, you can stop observation.

To stop observing a remote device but still maintain a remote control connection

1. Once you've connected to a remote device, click Session | Don't observe. You can still use the chat feature with the device.
2. Click Session | Observe to restore the remote view.

Customizing remote control

You can customize these remote control options:

- [Change remote control settings](#)
- [Optimize remote control performance](#)
- [Customize the toolbar](#)

Changing remote control settings

Use the **Options** dialog's **Change settings** tab (**LANDesk Remote Control | Preferences**) to adjust the remote control settings.

- **Lock out the remote keyboard and mouse:** Locks the remote device's keyboard and mouse so that only the user running the viewer can control the remote device. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Blank the remote computer screen:** Blanks the remote device's screen so only the user running the viewer can see the user interface display on the remote device.
- **Write log entries to Remote.log:** If you want to save a log of remote control actions in a log file on the remote device, check this option. You can choose from three logging levels, with level 1 being the least detailed and level 3 being the most detailed. Level 1 is the default level.

Optimizing remote control performance

Use the **Options** dialog's **Optimize performance** tab (**LANDesk Remote Control | Preferences**) to optimize remote control performance.

Changing the optimization setting dynamically adjusts color reduction, wallpaper visibility, and remote windows appearance effects (the ones you can adjust in Windows **Display Properties | Appearance | Effects**), such as transition effects for menus and tooltips.

Remote control always uses a highly efficient compression algorithm for remote control data. However, even with compression, it requires a lot of data to send high color depth information. You can substantially reduce the amount of remote control data required by reducing the color depth displayed in the remote control viewer. When the viewer reduces the color depth, the viewer has to map the full color palette from the remote desktop to a reduced color palette in the viewer. As a result, you may notice colors in the remote control window that don't accurately reflect the remote desktop. If that's a problem, select a higher-quality compression setting.

Another way you can optimize performance is to **Suppress remote wallpaper**. When you do this, remote control doesn't have to send wallpaper updates as parts of the remote desktop are uncovered. Wallpaper often includes bandwidth-intensive images, such as photographs. These don't compress well and take time to transfer over slower connections.

Customizing the remote control toolbar

You can customize which buttons appear on the remote control toolbar.

To customize toolbar buttons

1. Click **Session | Customize toolbar**.
2. Drag buttons you want from the palette onto the viewer window.
3. Drag buttons you don't want from the viewer window to the palette.
4. To restore the default button layout, drag the default set at the bottom of the palette onto the viewer window.

You can change the button size by clicking **Use small size**. You can also use the **Show** option to show icons only, text only, or both icons and text.

Security and Patch Manager

LANDesk Security and Patch Manager is a complete, integrated security management solution that helps you protect your LANDesk managed devices from a variety of prevalent security risks and exposures.

Security and Patch Manager provides all the tools you need in order to: download the most common types of security content updates (such as vulnerabilities, spyware, configuration security threats, virus pattern files, and unauthorized applications) from LANDesk Security services; download associated patch files, and configure and run security assessment and remediation scans on your managed devices. You can also create your own custom definitions to scan for and remediate specific, potentially harmful conditions on devices. If any security risks are detected, Security and Patch Manager lets you remediate affected devices. Additionally, at any time you can view detailed security and patch information for scanned devices, and generate specialized security and patch reports.

All of these enterprise security management tasks can be performed from the convenience of a single console.

Additionally, Security and Patch Manager lets you scan managed devices, and core servers and console machines, for versions of installed LANDesk software and deploy the appropriate LANDesk software updates.

About LANDesk Security Suite

The Security and Patch Manager tool is the main security management component of LANDesk Security Suite. Security Suite is based on much of the primary LANDesk Management Suite functionality, supplemented with specialized security management tools such as the Security and Patch Manager, LANDesk Network Access Control, LANDesk Antivirus, and connection control manager. The Security and Patch Manager tool has the same features in Management Suite and Security Suite and is described in detail in this chapter. For more information on which basic LANDesk functionality is supported in Security Suite, see [Introduction to LANDesk Security Suite](#).

About LANDesk Network Access Control and endpoint compliance security

Endpoint compliance security can be enforced on your LANDesk network with the LANDesk Network Access Control (NAC) tool. LANDesk NAC, in conjunction with the custom policy, scanning, and remediation capabilities of Security and Patch Manager, enables you to control access to the corporate network by verifying the health of connecting devices, blocking and/or remediating infected devices, and protecting the network from malicious intrusion. LANDesk NAC adds another powerful layer of security to your LANDesk network. For more information on how to set up and use a LANDesk NAC solution, see "LANDesk Network Access Control (NAC)" on page 369.

About LANDesk Antivirus

LANDesk Antivirus lets you download the most up-to-date virus definition files, scan your managed devices for viruses, and clean any virus infections. You can automate scheduled virus pattern file downloads and custom antivirus scans; create and apply unique antivirus scanner settings that control scanner behavior and end user interaction; and evaluate virus definitions and antivirus scans in a limited, controlled pilot test environment before deploying them to your managed devices. For more information, see "LANDesk Antivirus" on page 474.

Read this chapter to learn about:

- "Looking ahead: What to do after configuring devices for LANDesk Security management" on page 316
- "Security and Patch Manager overview" on page 316
 - "Security content types and subscriptions" on page 318
 - "Supported device platforms" on page 319
 - "Role-based administration with Security and Patch Manager" on page 319
 - "Security and patch management task workflow" on page 321
- "Understanding and using the Security and Patch Manager tool window" on page 321
- "Configuring devices for security scanning and remediation" on page 330

Looking ahead: What to do after configuring devices for LANDesk Security management

Once you understand Security and Patch Manager concepts, how to navigate the user interface, and the general task workflow; and after you've configured devices to work with Security and Patch Manager, you can perform the following security management tasks:

- Downloading security content updates and patches
- Viewing security content definition and detection rule properties
- Creating custom vulnerability definitions
- Scanning managed devices for security risks
- Remediating affected devices
- Enabling security alerts
- Generating security reports

For detailed information on performing these tasks, see "Managing security content and patches" on page 334, and "Scanning and remediating devices" on page 346.

Security and Patch Manager overview

Security and Patch Manager provides all of the tools you need to establish system-wide security across your network. With Security and Patch Manager, you can automate the repetitive processes of maintaining security and patch content, and organizing and viewing that content.

Use security scan tasks and policies to assess managed devices for known platform-specific vulnerabilities. You can download and manage patch executable files. Finally, you can remediate detected vulnerabilities by deploying and installing the necessary patch files, and verify successful remediation.

Additionally, you can create your own custom vulnerability definitions in order to scan managed devices for specific OS and application conditions that might threaten the operation and security of your system. Custom definitions can be configured for detection only or to do both detection and remediation. For more information, see "Creating custom definitions and detection rules" on page 341.

New features

The latest version of Security and Patch Manager offers several new capabilities, such as:

- Use the change settings task to change/update only the device agent configuration settings you want to, including : 802.1X support settings, compliance security settings, configure Windows firewall settings, custom variable override settings, HIPS settings, LANDesk Antivirus settings, and security scan and repair settings. With the change settings task you can change desired settings without a full device agent configuration deployment.
- Configure global alert settings.
- Scan for the presence of spyware on your managed devices. If spyware is detected, you can schedule a repair job that removes the spyware from affected devices.
- Deny launch of unauthorized or prohibited applications on end user devices with blocked application definitions.
- Enable real-time spyware monitoring (detection and removal), and real-time application blocking.
- Scan managed devices for security threats (Windows system configuration errors and exposures) on the local hard drive. Once a security threat is identified, you can perform the necessary fix manually at the affected device.
- Use specific security threat definitions that detect the Windows firewall, turn it on or off, and configure the firewall settings.
- Use custom variables that are included with other security threat definitions in order to customize and change specific local system configurations, and to enforce enterprise-wide system configuration policies.
- Scan for third-party antivirus scanner engines, and enable/disable real-time virus scanning and ensure up-to-date virus pattern files for those specific antivirus products.
- Receive alerts when specified vulnerabilities are detected on managed devices by a security scan. You can configure alerting by definition severity.
- Implement frequent security scans for critical, time-sensitive security risks such as virus scanning.
- Enforce endpoint security and compliance security policies with the Compliance group and the LANDesk Network Access Control tool.
- Use vulnerability dependency relationships to identify which patches need to be installed before other vulnerabilities can adversely affect managed devices or before they can be remediated. Supercedence information describes patches that have been replaced by more recent versions and that don't need to be applied.
- Verify the latest LANDesk software is installed on your managed devices, as well as core servers and console machines, by scanning for LANDesk software updates. If an outdated version is detected on a device, you can schedule a repair job the deploys and installs the latest LANDesk software update.

Features

With Security and Patch Manager, you can:

- Provide patch security for international versions of the operating systems on your network, including current support for the following languages: Czech, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Simplified Chinese, Spanish, Swedish, and Traditional Chinese.

- Organize and group security definitions to perform customized security assessment scans and remediation (see "Security and Patch Manager tree view" on page 325).
- Assess vulnerabilities and other security risks on a variety of supported device platforms, including Windows, Sun Solaris, and Linux (see "Scanning devices for security risks" on page 347).
- View security and patch information for scanned devices (see "Viewing security and patch content" on page 337).
- Schedule automatic patch management tasks, including content updates, device scans, and patch downloads.
- Perform remediation as a scheduled task, a policy, or automatically with the Auto Fix feature (see "Remediating devices with detected security risks" on page 355).
- Download, deploy, and install patches that have been researched and verified (see "Downloading patches" on page 339).
- Track the status of patch deployments and installation on scanned devices.
- Use LANDesk's Targeted Multicast, peer download, and checkpoint restart features for fast and efficient patch deployment.
- Generate and view detected an extensive variety of security and patch management-specific reports (see "Using security reports" on page 368).

Security content types and subscriptions

When you install LANDesk Management Suite, the Security and Patch Manager tool is now included by default (previously, it was a separate add-on). However, without a Security Suite content subscription, you can only scan for LANDesk software updates and custom definitions. A Security Suite content subscription enables you to take full advantage of the Security and Patch Manager tool by providing access to additional security and patch content (definition types).

LANDesk Security Suite content types include:

- Antivirus updates (for third-party scanners, includes antivirus scanner detection content only; for LANDesk Antivirus, includes both scanner detection content AND virus definition files)
- Blocked applications (see the "Legal disclaimer for the blocked applications type" on page 333)
- Custom vulnerability definitions
- Driver updates
- LANDesk software updates
- Security threats (system configuration exposures; includes firewall detection and configuration)
- Software updates
- Spyware
- Vulnerabilities (known platform- and application-specific vulnerabilities)

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Scanning and remediation functions are not the same between these content types. For more information, see the appropriate sections below.

Supported device platforms

Security and Patch Manager supports most of the standard LANDesk-managed device platforms, including the following operating systems:

- Windows 98 SE
- Windows NT 4.0 (SP6a and higher)
- Windows 2000 Professional (SP4)
- Windows XP Professional (SP1/SP2)
- Windows 2003 Servers
- Mac OS X (10.2.x, 10.3.x, and 10.4.x)
- Red Hat Linux 9 (scanning from the console; manual remediation)
- SUSE Linux (scanning from the console; manual remediation)
- Sun Solaris (scanning from the console; manual remediation)

For information on configuring managed devices for security and patch scanning, see "Configuring devices for security scanning and remediation" on page 330 later in this chapter.

Scanning core servers and consoles for LANDesk software updates is supported

You can also scan LANDesk core servers and consoles for LANDesk software updates, but those machines must first have the standard LANDesk agent deployed, which includes the Security and patch scanner agent required for security scanning tasks.

Role-based administration with Security and Patch Manager

Security and Patch Manager uses LANDesk's role-based administration to allow users access to the Security and Patch Manager features. Role-based administration is LANDesk's access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each LANDesk user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see "Role-based administration" on page 59

A LANDesk Administrator assigns these rights to other users with the Users tool in the console. Security and Patch Manager introduces one new role and corresponding right to role-based administration. The right is called Security and Patch Manager, and it appears in the User Properties dialog. In order to see and use this tool, a LANDesk user must be assigned the necessary Security and Patch Manager right.

Security and Patch Manager rights

Security and Patch Manager features are controlled by role-based administration rights, as described below:

Security and Patch Manager

The Security and Patch Manager right provides users the ability to:

- See and access the Security and Patch Manager tool in the Tools menu and Toolbox
- Configure managed devices for security assessment and remediation scanning
- Configure devices for real-time spyware and blocked application scanning
- Configure devices for high frequency scanning for critical security risks
- Download security updates and associated patches for the security types for which you have a Security Suite content subscription
- Create scheduled tasks that automatically download definitions and/or patch updates
- Create custom vulnerability definitions and custom detection rules
- Import, export, and delete custom definitions
- View downloaded security and patch content by type (including: all types, blocked applications, custom definitions, LANDesk updates, security threats, spyware, vulnerabilities, driver updates, and software updates)
- Customize selected security threats with custom variables
- Configure and run security scans on managed devices as a scheduled task or as a policy
- Divide a scheduled task scan into a staging phase and a deployment phase
- Create and configure scan and repair settings that determine the scan options, such as: content type to be scanned for, scanner information and progress display, device reboot behavior, and the amount of end user interaction. Then, apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks
- View detailed scan results by: detected group, specific definition, individual device, or a group of selected devices
- Perform remediation as a scheduled task or as a policy
- Use Auto Fix to automatically remediate the following security types if they are detected: vulnerabilities, spyware, LANDesk software updates, and custom definitions (must also be a LANDesk Administrator)
- Track and verify the status of patch deployment and installation (repair history on scanned devices)
- Purge unused security type definitions (must be a LANDesk Administrator)
- Uninstall patches from scanned devices
- Remove patches from the core database
- Configure vulnerability alerts
- Generate a variety of security specific reports (also requires the Reports right)

Security and Patch Compliance

The Security and Patch Compliance right provides users the ability to:

- Add and remove security definitions from the Compliance group
- Change the status of definitions contained in the Compliance group
- **Note:** Even with this right a user can't configure LANDesk NAC services, such as adding posture validation servers or remediation servers, or configuring and publishing compliance rules. A user must be a LANDesk Administrator to be able to configure LANDesk NAC.

Antivirus

For information on the Antivirus right and using LANDesk Antivirus, see "Role-based administration with LANDesk Antivirus" on page 477.

Edit Custom Variables

The Edit Custom Variables right provides users the ability to:

- Edit custom variable values (for security content types with custom variables, such as security threats)
- Enable a custom variable's override option in order to ignore the modified value and scan for the original value
- Create and deploy a change settings task that includes custom variable override settings

Security and patch management task workflow

The following steps provide a quick summary outline of the typical processes involved in implementing security and patch management on your LANDesk network. Each of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using security and patch management:

1. Configuring managed devices for security scans and remediation.
2. Collecting updated security and patch information (i.e., vulnerability definitions) from industry/vendor data sources. Also, creating custom definitions.
3. Organizing and viewing security and patch information.
4. Creating and configuring scan tasks and security policies. Scan for vulnerabilities, spyware, security threats, blocked applications, etc.
5. Viewing scan results for scanned devices.
6. Downloading patches for detected vulnerabilities
7. Repairing detected vulnerabilities by deploying and installing patches to affected devices
8. Repairing other detected security risks and exposures.
9. Viewing patch installation status and repair history information.

Understanding and using the Security and Patch Manager tool window

The Security and Patch Manager window, like all other LANDesk tool windows, is opened from either the Tools menu or the Toolbox and can be docked, floated, and tabbed with other open tool windows (see "Dockable tool windows" on page 34). Note that with LANDesk's role-based administration, a LANDesk user must have either the LANDesk Administrator right (implying full rights), or the specific Security and Patch Manager right, to be able to see and access the Security and Patch Manager tool. For more information on user rights and scope, see "Role-based administration" on page 59."

The Security and Patch Manager window contains a toolbar and two panes. The left-hand pane shows a hierarchical tree view of security type definition and detection rule groups. You can expand or collapse the objects as needed.

The right-hand pane displays a column list of the selected group's definition details or detection rule details, depending upon which group you've selected in the left-hand pane, plus a Find feature for searching in long item lists.

Characters not allowed when searching a list

In the **Find** box, the following extended characters are not supported: <, >, ', ", !

The Security and Patch Manager window includes a toolbar with the following buttons:

Toolbar buttons

- **Download updates:** Opens a dialog where you can specify the platforms and languages for the content types you want to update, as well as which LANDesk Security content server to access. You can also configure whether to place definitions in the Unassigned group, whether to download associated patches concurrently, the location where patches are downloaded, and proxy server settings.
- **Create a task:** Includes a drop-down list where you can select which type of task you want to create:
 - **Security scan** lets you create a security scan task, specify whether the scan is a scheduled task or a policy, and select a scan and repair setting that determines whether the security scanner displays, reboot and interaction behavior, and the content types scanned for.
 - **Compliance scan** lets you create a security scan task that specifically checks target devices for compliance with your current security policy as defined in LANDesk Network Access Control settings and by the contents of the Compliance group. You can also specify whether the compliance security scan runs as a scheduled task (including which devices to scan and whether to scan immediately) or as a policy.
 - **Reboot** lets you create a device reboot task, specify whether the reboot is a scheduled task or a policy, and select a scan and repair setting that determines display and interaction behavior. Note that only the options on the reboot tab of the dialog apply to this task.
 - **Repair** lets you create a security repair task that remediates detected security exposures on scanned devices. You can configure the repair as a scheduled task or as a policy or both, divide the repair task into separate staging and repairing phases, select a scan and repair settings, and download patches. Note that one or more repairable security definitions must first be selected in order to create a repair task.
 - **Gather historical information** lets you create a task that gathers the current scanned and detected counts (for a specified number of days) that can be used for reporting. You can also create and configure a scheduled task that performs the same action.
 - **Change settings** lets you create a task that changes the default settings on a managed device by writing the specified setting ID to the local registry. With a change settings task you can change one or more of these settings: 802.1X support settings, compliance security settings, configure Windows firewall settings, custom variable override settings, HIPS settings, LANDesk Antivirus settings, and security scan and repair settings. You can use this task as a quick and convenient way to change only the settings you want to without having to redeploy a full device agent configuration.
 - **LANDesk Antivirus scan** lets you create an antivirus scan task, specify whether the antivirus scan is a scheduled task or a policy, and select an antivirus setting that determines how and when the scanner runs on target devices and the options available to the end user.

- **Install/Update LANDesk Antivirus** lets you create a task that installs the LANDesk Antivirus agent on target devices that don't yet have it installed, or updates the existing version of the LANDesk Antivirus agent on target devices that already have it installed. You can also select whether to remove existing antivirus products from target devices. This task allows you to conveniently deploy and update a managed device's LANDesk Antivirus agent (and associated antivirus settings) without having to redeploy a full agent configuration.
- **Remove LANDesk Antivirus** lets you create a task that removes the LANDesk Antivirus agent from target devices.
- **Configure settings:** Includes a drop-down list where you can select which type of settings you want to configure, change, or update:
 - **Scan and repair settings** lets you create, edit, copy, and delete scan and repair settings. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, user interaction, and the content types scanned.
 - **Compliance settings** lets you create, edit, copy, and delete compliance settings. Compliance settings determine when and how a compliance security scan takes places, whether remediation occurs automatically, and what to do when LANDesk Antivirus detects a virus infection on target devices.
 - **LANDesk Antivirus settings** lets you create, edit, apply, and delete scan and repair settings. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.
 - **HIPS settings** lets you create, edit, copy, and delete HIPS settings. HIPS settings determine whether the LANDesk HIPS client is password protected, WinTrust signed code handling, action on programs added to system startup, buffer overflow protection, operating mode, whitelists, file certifications, and file protection rules
 - **Windows firewall settings** lets you create, edit, copy, and delete Windows firewall settings. You can use Windows firewall settings associated with a change settings task to enable\disable and configure the firewall on target devices running the following Windows platforms: Windows 2003/XP; Windows Vista.
 - **Custom variable override settings** lets you create, edit, apply, and delete scan and repair settings. Custom variables overrides lets you configure exceptions to custom variable values. In other words, with custom variable override settings you can ignore or bypass a specific custom variable condition so that a scanned device is not determined to be vulnerable.
 - **Definition group settings** lets you create, edit, copy, and delete Definition group settings to automate security content downloads.
 - **Alert settings** lets you configure global security alerts.
 - **Rollup core settings** lets you enable automatic immediate forwarding of vulnerability scan results to a rollup core that you specify. Sending vulnerability scan results to a rollup core server can enhance real-time access to critical vulnerability data for all managed devices across a distributed enterprise network.
- **Create custom definition:** Opens a blank Definition properties dialog with editable fields where you can specify whether the custom definition is detection only or also allows remediation, enter specific vulnerability information, create detection rules, and identify the appropriate patch file for remediation.
- **Import custom definitions:** Allows you to import an XML file containing custom definitions.

- **Export selected custom definitions:** Allows you to export a custom definition as an XML file.
- **Computers out of compliance:** Lists devices that have been scanned to check for compliance with the predefined compliance security policy (based on the content of the Compliance group, and the definition of healthy found on the Configure Network Access Control dialog), and are determined to be unhealthy or out of compliance.
- **Antivirus activity:** Lets you view detailed antivirus activity and status information for all of your managed devices with the LANDesk Antivirus agent.
- **Refresh:** Updates the contents of the selected group.
- **Delete selected custom definitions:** Removes the selected custom definitions from the core database.
- **Purge security and patch definitions:** Lets you specify the platforms and languages whose definitions you want to remove from the core database. Note that only a LANDesk Administrator user can perform this operation.
- **Publish LANDesk NAC settings:** Lets you specify which content you want to publish to posture validation servers and remediation servers. Any time you change the LANDesk NAC settings, you must republish the new settings to the posture validation servers. (**Note:** Publishing NAC content sends network access control settings and compliance rules to posture validation servers or LANDesk DHCP servers, AND sends any associated patches to remediation servers; while publishing Infrastructure files sends setup and support files, including the security client scanner and trust agents as well as the HTML template pages, to remediation servers.)
- **Help:** Opens the online help to the Security and Patch Manager section.

Type drop-down list

Use the **Type** drop-down list to determine which downloaded definitions display in the tree view. Definition types are designated by the publisher of the content. Filtering the display can be helpful if you want to see only one specific type of security content, or if you want to narrow down an extremely long comprehensive list.

The **Type** drop-down list includes the following options:

- All types (comprehensive list of all downloaded security definitions)
- Antivirus updates (lists downloaded scanner detection definitions only; does not list specific LANDesk Antivirus virus definition files)
- Blocked applications (lists downloaded blocked application definitions only)
- Custom definitions (lists user-defined vulnerability definitions only)
- Driver updates (lists downloaded driver update definitions only)
- LANDesk software updates (lists downloaded LANDesk software updates only)
- Security threats (lists downloaded security threat definitions only)
- Software updates (lists downloaded software updates only)
- Spyware (lists downloaded spyware definitions only)
- Vulnerabilities (lists all downloaded vulnerability definitions for any of the available platforms)

The left pane of the Security and Patch Manager window shows the following items:

Security and Patch Manager tree view

Security and Patch Manager is the root object of the Security and Patch Manager tree view, containing all of the security types such as vulnerabilities, spyware, security threats, blocked applications, and custom definitions groups (and associated detection rule groups, if applicable). The root object can be expanded and collapsed as needed.

Type name (or All Types)

The type groups contain the following subgroups:

- **Detected:** Lists all of the definitions detected by security scans, for all of the devices included in the scans. The contents of this group are cumulative based on all the security scans run on your network. Definitions are removed from this group only by: being successfully remediated, being removed from the Scan group and running the scan again, or by actually removing the affected device from the database.

The Detected list is a composite of all detected security definitions found by the most recent scan. The Scanned and Detected columns are useful in showing how many devices were scanned, and on how many of those devices the definition was detected. To see specifically which devices have a detected definition, right-click the item and click **Affected computers**.

Note that you can also view device-specific information by right-clicking a device in the network view, and then clicking **Security and Patch Information**.

You can only move definitions from the Detected group into either the Unassigned or Don't Scan groups.

- **Scan:** (For the Blocked Applications type, this group is called **Block**.) Lists all of the security definitions that are searched for when the security scanner runs on managed devices. In other words, if a definition is included in this group, it will be part of the next scan operation; otherwise, it won't be part of the scan.

By default, collected definitions are added to the Scan group during a content update. (**Important:** Except for blocked applications, which are added to the Unassigned group by default.)

Scan can be considered one of three possible states for a security definition, along with Don't Scan and Unassigned. As such, a definition can reside in only one of these three groups at a time. A definition is either a Scan, Don't Scan, or Unassigned and is identified by a unique icon for each state (question mark (?) icon for Unassigned, red X icon for Don't Scan, and the regular vulnerability icon for Scan). Moving a definition from one group to another automatically changes its state.

By moving definitions into the Scan group (click-and-drag one or more definitions from another group, except the Detected group), you can control the specific nature and size of the next security scan on target devices.

Caution about moving definitions from the Scan group

When you move definitions from the Scan to the Don't Scan group, the current information in the core database about which scanned devices detected those definitions is removed from the core database and is no longer available in either an item's Properties dialog or in a device's Security and Patch Information dialog. To restore that security assessment information, you would have to move the definitions back into the Scan group and run the same security scan again.

- **Don't Scan:** (For Blocked Applications, this group is called **Don't Block**.) Lists all of the definitions that aren't searched for the next time the security scanner runs on devices. As mentioned above, if a definition is in this group, it can't be in the Scan or Unassigned group. You can move definitions into this group in order to temporarily remove them from a security scan.
- **Unassigned:** Lists all of the definitions that do not belong to either the Scan or Don't Scan groups. The Unassigned group is essentially a holding area for collected definitions until you decide whether you want to scan for them or not.

To move definitions, click-and-drag one or more from the Unassigned group into either the Scan or Don't Scan groups.

New definitions can also be automatically added to the Unassigned group during a content update by checking the **Put new definitions in the Unassigned group** option on the **Download updates** dialog.

- **All Items:** Lists all of the selected type's definitions in a flat list, even if you've moved a definition into either the Unassigned, Scan, or Don't Scan group.
- **View by Product:** Lists all of the definitions organized into specific product subgroups. These subgroups help you identify definitions by their relevant product category.

You can use these product subgroups to copy definitions into the Scan group for product-specific scanning, or copy them into a custom group (see below in order to perform remediation for groups of products at once).

Definitions can be copied from a product group into the Scan, Don't Scan, or Unassigned group, or any of the user-defined custom groups. They can reside in platform, product, and multiple custom groups simultaneously.

Groups

Contains the following subgroups:

- **Custom Groups:** Lists all of the subgroups you've created and the definitions they contain. My Groups provide a way for you to organize security definitions however you want. Use a group's contents to copy several definitions into the Scan group for customized scanning, or to create a repair job for several definitions at once.

You can also use a custom group to define the contents of a security scan. Copy the definitions you want to scan for into a custom group and select that group in the Scan for option of the Scan and repair settings dialog.

To create a custom group, right-click **Custom Groups** (or a subgroup) and then click **New Group**.

To add definitions to a custom group, click-and-drag one or more of them from any of the other definition groups. Or, you can right-click a custom group, and then click **Add Definition**.

- **Alert:** Lists all of the definitions that will generate an alert message the next time the security scanner run and devices. For more information, see Using vulnerability alerts.
- **Compliance:** Lists all of the definitions that are used to determine whether a managed (or mobile/guest device) is Healthy or Unhealthy. This group is used by LANDesk Network Access Control (NAC) to deny or allow access to the main network. The definitions and associated patch files contained in the Compliance group are copied to a special remediation server that scans devices, determines compliance or non-compliance (according to compliance rules published to a posture server), and can remediate non-compliant devices so that they can be granted full access to the corporate network.
- **SANS Top 20:** Lists the top 20 vulnerability definitions as identified and published by Microsoft. These definitions are typically a subset of the Microsoft Windows Vulnerabilities that are downloaded with the **Download updates** dialog.

Detection Rules

The Detection Rules group displays only for certain security content types.

Detection rules define the specific operating system, application, file, or registry conditions that a definition checks for in order to detect the applicable security risk (vulnerabilities, custom definitions, and security threats on scanned devices). Spyware and blocked applications do not apply.

The Detection Rules group contains the following subgroups:

- **Scan:** Lists all of the detection rules that are enabled for security scanning on devices.

By default, detection rules associated with a definition of any security content type are added to the Detection Rules Scan group during a content update. Likewise, custom detection rules associated with a custom definitions are added to the Scan group when you create the custom definition.

Note that in addition to having a definition's detection rules enabled, its corresponding patch executable file must also be downloaded to a local patch repository on your network (typically the core server) before remediation can take place. The Downloaded attribute (one of the detail columns in the tool window's right-hand pane) indicates whether the patch associated with that rule has been downloaded.

- **Don't Scan:** Lists all of the detection rules that are disabled for security scanning on devices. Some definitions have more than one detection rule. By disabling a detection rule, you can ensure that it won't be used to scan for the conditions indicating that definition is present on devices. This can allow you to simplify a security scan without redefining the definition.
- **View by Product:** Lists all of the detection rules for collected definitions, organized into specific product subgroups. These subgroups help you identify detection rules by their relevant product category.

You can use these product subgroups to perform group operations.

Settings

The Settings group lets you view the various settings you've created for security scanning tasks. You can right-click any of the Settings groups to create a new setting and view the settings information in a report format.

The Settings group contains the following subgroups:

- **Scan and Repair:** Lists all of the scan and repair settings you've created that are used to determine the operation of the security scanner. Each scan and repair setting has a unique ID number. The right-hand pane shows useful information for the listed scan and repair settings.
- **Compliance:** Lists all of the compliance settings you've created that are used to determine the operation of the security scanner when performing a specific compliance scan. Each setting has a unique ID number. The right-hand pane shows useful information for the listed scan and repair settings.
- **LANDesk Antivirus:** Lists all of the antivirus settings you've created that are used to determine the operation of the antivirus scanner. Each setting has a unique ID number.
- **Windows Firewall:** Lists all of the Windows firewall settings you've created that are used to determine the behavior of either the Windows XP/2003 or Windows Vista firewall on devices configured with the specific setting.
- **Custom variables to override:** Lists all of the custom variable override settings you've created that are used to determine which modified custom variable values to ignore when the security scanner runs. Each setting has a unique ID number. The right-hand pane shows useful information for the listed settings.
- **Network Access Control:** Lists LANDesk Network Access Control (NAC) services. You can right-click the LANDesk DHCP/NAC object in order to access a shortcut menu with options to: configure network access control settings such as LANDesk DHCP servers or posture validation servers, the logging level, and audit-only posturing; configure remediation servers; configure user credentials; publish network access control settings; and add unmanaged devices. Expand the object to access posture validation server logs that can be double-clicked to download the server's log file data.

Definition details

The right pane of the Security and Patch Manager window displays detailed information listed in sortable columns for definition and detection rule items, as described below:

- **ID:** Identifies the definition with a unique, vendor-defined alphanumeric code.
- **Severity:** Indicates the severity level of the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown.
- **Title:** Describes the nature or target of the definition in a brief text string.
- **Language:** Indicates the language of the OS or application affected by the definition.
- **Date Published:** Indicates the date the definition was published by the vendor.
- **Repairable:** Indicates whether the definition can be repaired through patch file deployment and installation. Possible values are: Yes, No, Some (for a definition that includes multiple detection rules and not all detected definitions can be fixed), and No rules (for a custom definition that doesn't include any detection rules).

- **Silent Install:** Indicates whether the definition's associated patch (or patches) installs silently, meaning without user interaction. Some definitions may have more than one patch. If any of a definition's patches don't install silently, the Silent Install attribute says No. To see how individual patches install, right-click the definition and click **Properties | Patches**.
- **Detected:** Displays the number of scanned devices that detected the definition.
- **Scanned:** Displays the number of devices scanned for the definition.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the definition.
- **CVE ID:** (Applies only to vulnerabilities) Identifies a vulnerability by its unique CVE (Common Vulnerabilities and Exposures) name. For more information, see [Using CVE names](#).

Using a definition shortcut menu

You can right-click an item to view more details with the **Properties** option.

A definition's shortcut menu also lets you do the following tasks (depending on the security type):

- View affected computers
- Download associated patches
- Enable/disable autofix
- Add the definition to the Compliance and Alert groups
- Clear the definition's scan information and repair status
- Create a repair job.

Detection Rule details

- **Name:** Displays the name of the detection rule (can be the file name of the patch executable).
- **ID:** Displays the ID of the definition associated with the rule.
- **Repairable:** Indicates whether the associated definition can be repaired through patch file deployment and installation.
- **Silent Install:** Indicates whether the rule's associated patch installs silently on devices without user interaction.
- **Reboot:** Indicates whether the associated patch file requires a system reboot in order to complete a successful remediation.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the associated definition.
- **Downloaded:** Indicates whether the rule's associated patch executable file has been downloaded to the local repository.

Right-click a detection rule to view more details with the **Properties** option. The shortcut menu also lets you enable/disable the rule and download the associated patch.

Configuring devices for security scanning and remediation

Before managed devices can be scanned for vulnerabilities, spyware, security threats, and other security types, and receive patch deployments or software updates, they must have the Security and patch scanner agent installed (this agent is installed by default with the standard LANDesk agent).

This section includes information about configuring Windows devices as well as Linux, UNIX and Mac devices.

Scanning core servers and consoles for LANDesk software updates is supported

You can also scan LANDesk core servers and consoles for LANDesk software updates, but they must first have the standard LANDesk agent deployed, which includes the Security and patch scanner agent required for security scanning tasks.

Configuring Windows devices for security scanning

With previous versions, for Windows devices, the vulnerability scanner agent had to be installed as a separate add-on component to an existing device agent configuration.

However, now the security and patch scanner agent is included by default with the standard LANDesk agent and is installed on devices with even the most basic agent configuration. In other words, any Windows device configured with the new Agent configuration tool will be ready for security and patch scanning and remediation.

Configuring scan and repair options for Windows devices during agent configuration

When creating or editing an agent configuration, you can specify some of the security and patch scanner's options, such as when and how often the scanner runs automatically on managed devices, whether the scanner displays progress and prompts on the end user device, as well as global settings for remediation operations such as device reboot and autofix. For more information on customizing the behavior of the security and patch scanner agent as part of creating and deploying agent configurations to managed Windows devices, see "Deploying and configuring the LANDesk security and patch scanner" on page 686.

Note: WinSock2 is required on Windows 9x devices in order for the Vulnerability Scanner agent to run.

After agent configuration occurs, a program icon for the security and patch scanner is added to the device's LANDesk Management program group, that can be used to run the scanner directly from the device as opposed to any runkey launch, recurring local scheduler launch, or scheduled task using the console .

Additional security settings in agent configurations

When defining a device agent configuration (for Windows devices), you can also enable and configure the following the security scanner settings:

- Frequent security scanning for critical security risks
- Real-time application blocker and spyware monitoring

See the sections below for more information.

About the Agent configuration dialog's Frequent security scan page

Use this page to enable and configure high frequency scanning for critical, time-sensitive security risks such as recently discovered and malignant viruses, and firewall configuration risks.

- **Use the frequent security scanner:** Enables high frequency scanning with the security and patch scanner, based on the time and group content specified below. If this option is not selected, managed devices configured with this agent configuration will still be able to be scanned with the security and patch scanner, according to the settings specified on the Security and patch scan page because the security and patch agent is part of the standard LANDesk agent .
- **Scan only when a user is logged in, every:** Specifies how often the frequent security scan runs when a user is logged in to a managed device. The minimum frequency is 30 minutes.
- **Choose a scan and repair setting:** Determines the security type's definitions that are scanned by the high frequency scan, based on the contents of the custom group selected here. The high frequency scan can only be defined by the contents of a custom group, not the Scan, Alerts, or Compliance groups. Any type of security content type can be added to a custom group, such as spyware, vulnerabilities, custom definitions, security threats, etc. The custom group is selected on the scan and repair settings dialog. Chose a scan and repair setting from the drop-down list. Only scan and repair settings that are configured to scan for a custom group (as opposed to a specific type or types appear in this list).
- **Configure:** Opens the scan and repair settings dialog where you can select a scan and repair setting that has a custom group scan specified.

About the Agent configuration dialog's Spyware/Application blocker page

Use this page to enable and configure real-time application blocking and spyware detection and removal on managed devices configured with this agent configuration. (See the "Legal disclaimer for the blocked applications type" on page 333.)

- **Allow application blocking monitoring:** Enables real-time application blocking, based on the list of unauthorized applications definitions contained in the Scan group (or custom group).
 - **Notify user when and application has been blocked:** Displays a message on the end user device notifying them that the application they attempted to launch has been denied or blocked.
- **Allow real-time spyware monitoring:** Enables real-time spyware detection and removal, based on the list of spyware definitions contained in the Scan group (or custom group).

Important: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

- **Notify user when spyware has been blocked:** Displays a message on the end user device notifying them that known spyware has been detected and removed from their system.
- **Prompt user when an unknown application is being installed:** Displays a message on the end user device notifying them that an unknown application is being installed on their system.

Configuring Linux and UNIX devices for security scanning

Security and Patch Manager also supports vulnerability scanning on:

- Red Hat Linux
- SUSE Linux
- Sun Sparc (Solaris 8)

Each of these platform's security and patch content can be downloaded with Security and Patch Manager just as with Windows vulnerabilities.

Linux and UNIX devices can't be configured with the security and patch scanner agent via the console's agent configuration tool. Linux and UNIX device configuration is a manual process. For more information on setting up Linux and UNIX devices, see the *Installation and Deployment Guide*, as well as the README file contained in the respective platform's tar file located in the platforms folder under ManagementSuite\LDLogon on the core server.

Once configured, these Linux and UNIX platforms can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed manually at the affected device.

Configuring Mac OS X devices for security scanning

On Macintosh OS X devices, Security and Patch Manager now supports both security scanning and remediation. Macintosh security and patch content can be downloaded with Security and Patch Manager.

Additionally, you can create and configure agent configuration for your Macintosh devices with the Agent configuration tool. As with Windows agent configuration, the security and patch scanner agent is part of the default standard LANDesk agent for Macintosh devices. To create and deploy a Macintosh agent configuration with security and patch scanner support, see "Managing Macintosh devices" on page 294 in the *Users Guide*.

Once configured, Macintosh devices can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed at the affected device.

To launch the security scanner manually on Mac devices

1. Open the Mac OS X **System Preferences** and select the **LANDesk Client** panel.
2. On the **Overview** tab, click **Check Now** in the Security and Patch Manager section.

Legal disclaimer for the blocked applications type

As a convenience to its end users, LANDesk provides access to a database containing certain information regarding executable files that an end user may utilize in connection with the application blocker functionality of the LANDesk® Security Suite. THIS INFORMATION IS PROVIDED AS-IS WITHOUT ANY EXPRESS, IMPLIED, OR OTHER WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. As such, LANDesk does not guarantee the accuracy, completeness or currency of this information and the end user is responsible to review and confirm this information before use. Any use of this information is at the end users own risk.

Some of the Summary information in the blocked applications definitions are provided from: <http://www.sysinfo.org>, and is copyrighted as follows: "Presentation, format and comments Copyright © 2001 - 2005 Paul Collins; Portions Copyright © Peter Forrest, Denny Denham, Sylvain Prevost, Tony Klein; Database creation and support by Patrick Kolla; Software support by John Mayer; All rights reserved."

Managing security content and patches

This section provides information on updating and viewing security content, creating and using custom definitions, and downloading and working with patches.

For information on actually scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports, see "Scanning and remediating devices" on page 346.

Read this chapter to learn about:

Managing security content and patches

- "Downloading security content and patch updates" on page 334
- "Viewing security and patch content" on page 337
- "Searching for vulnerabilities by CVE names" on page 337
- "Using filters to customize item lists" on page 338
- "Purging unused definitions" on page 737

Working with patches

- "Downloading patches" on page 339
- "Uninstalling patches" on page 340
- "Removing patches from the core database" on page 340

Using custom definitions

- "Creating custom definitions and detection rules" on page 341
- "Importing and exporting custom definitions" on page 344
- "Deleting custom definitions" on page 345

Downloading security content and patch updates

Your network and devices are continuously vulnerable to security risks and exposures from many harmful sources: worms, viruses, spyware, as well as ordinary maintenance issues like software updates and bug fixes. Patches are released regularly to repair inevitable operating system and application vulnerabilities. Security and Patch Manager makes the process of gathering the latest security type's definitions and patches quick and easy by letting you download content via a LANDesk-hosted database. This LANDesk Security service consolidates known definitions from trusted, industry/vendor sources and sends reliable information directly to you.

Security and Patch Manager also supports custom vulnerability definitions

In addition to known vulnerabilities, you can also create your own custom vulnerability definitions and associated detection rules. For more information, see "Creating custom definitions and detection rules" on page 341.

By establishing and maintaining up-to-date security and patch content, you can better understand the nature and extent of the security risks for each platform and application you support, determine which vulnerabilities and other types of risks are relevant to your environment, and customize security scanning and remediation tasks. The first step in this security management strategy is to download a current listing of the latest known security and patch content.

With Security and Patch Manager, you can configure and perform security and patch content updates at once, or create a scheduled update task to occur at a set time or as a recurring task (see "Scheduling automatic security and patch content update downloads" on page 336).

Only one LANDesk user on a specific core server (including additional consoles) can update security and patch content at a time. If a user attempts to update content while the process is already running, a message prompt appears indicating there is a conflict.

To update security and patch content

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Download updates** toolbar button.
3. Select the update source site from the list of available content servers.
4. Select the definition types whose security and patch content you want to update. You can select one or more types in the list depending on your LANDesk Security Suite content subscription. The more types you select, the longer the update will take.
5. Select the languages whose content you want to update for the types you've specified.

Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

When downloading content for any platform (with the appropriate subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.

6. If you want new content (content that does not already reside in any groups in the Security and Patch Manager tree) to automatically be placed in the Unassigned group instead of the default location, which is the Scan group, check the **Put new definitions in the Unassigned group** check box.
7. If you want to automatically download associated patch executable files, click the **Download patches** check box, and then click one of the download options:
 - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).

- **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerability, security threats, and LANDesk updates currently residing in the Scan group.

Patches are downloaded to the location specified on the **Patch Location** tab of the Download updates dialog.

8. If you have a proxy server on your network that is used for external Internet transmissions (that is required to update security and patch content and download patches), click the **Proxy Settings** tab and specify the server's address, port number, and authentication credentials if a login is required to access the proxy server.
9. Click **Apply** from any of the tabs at any time to save your settings.
10. Click **Update Now** to run the security and patch content update. The **Updating Definitions** dialog displays the current operation and status. (To create a scheduled task, click **Schedule Update**.)
11. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the security and patch security content that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining security and patch content.

Note: Do not close the console while an update security and patch process is running or the process will be terminated. However, this rule does not apply to a Download Security and Patch Content scheduled task, which will finish processing even if the console is closed while it is running.

To configure the patch download location

1. On the **Download updates** dialog, click the **Patch Location** tab.
2. Enter a UNC path where you want the patch files copied. The default location is the core server's \LDLogon\Patch directory.
3. If the UNC path entered above is to a location other than the core server, enter a valid username and password to authenticate to that location.
4. Enter a Web URL where devices can access the downloaded patches for deployment. This Web URL should match the UNC path above.
5. You can click **Test Settings** to check to see if a connection can be made to the Web address specified above.
6. If you want to restore the UNC path and Web URL to their default locations, click **Restore to Default**. Again, the default storage location is the core server's \LDLogon\Patch directory.

Scheduling automatic security and patch content update downloads

You can also configure security and patch content updates as a scheduled task to occur at a set time or as a recurring task. To do this, simply click the **Schedule download** toolbar button. The **Scheduled update information** dialog shows task-specific settings for the task. Click **OK** to create a Download Security and Patch Content task in the Scheduled Tasks window, where you can specify the scheduling options.

Task-specific settings and global settings Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other tabs of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global setting it is effective for all security content download tasks from that point on.

Viewing security and patch content

After security and patch content has been updated with the LANDesk Security service, you can view the definitions and detection rules (for vulnerabilities and custom definitions) only in their respective groups in the Security and Patch Manager window.

Use the **Type** drop-down list to view content for a specific definition type or for all definition types. You can also use the **Filter** control to further customize the content you want to display.

Once security and patch content has been downloaded, you can move items into different status groups, or copy them into your own custom groups. For information on how to use the different groups in the Security and Patch Manager view, see "Understanding and using the Security and Patch Manager tool window" on page 321.

You can also view property details for each of the updated definitions and detection rules by right-clicking an item and selecting **Properties**. This information can help you determine which definitions are relevant to your network's supported platforms and applications, how detection rules check for the presence of definitions, what patches are available, and how you want to configure and perform remediation for affected devices.

Custom definitions can be modified

If you select a downloaded industry definition, its properties dialog is primarily for information viewing purposes only. However, if you select a custom definition, or are creating a new custom definition, the pages and fields in the properties dialog are editable, allowing you to define the definition and its detection rules.

Searching for vulnerabilities by CVE names

LANDesk supports the CVE (Common Vulnerabilities and Exposures) naming standard. With Security and Patch Manager you can search for vulnerabilities by their CVE names, and view CVE information for downloaded vulnerability definitions.

For more information about the CVE naming convention, LANDesk compatibility with the CVE standard, and how to use CVE identification to find individual security vulnerability definitions in Security and Patch Manager, see [Using CVE names](#).

Using filters to customize item lists

The **Filter** drop-down list lets you create and apply custom display filters to control the items that display in the right-hand frame of the Security and Patch Manager window. Filters can help you streamline a large amount of security and patch content. You can filter content by operating system and severity.

The **Filter** control can be used in conjunction with the **Type** control to display exactly the security and patch content you're interested in viewing.

To create a new display filter

1. In Security and Patch Manager, click the **Filter** drop-down list, and then click **Manage filters**.
2. Click **New**.
3. Enter a name for the new filter.
4. If you want to filter content by operating system, click the check box, and then select the operating systems you want to display.
5. If you want to filter by the severity of the definition, click the check box, and then select the severities you want to display. Click **OK**

To apply a filter to a content group's display

1. Click the content group in the left-hand pane of the Security and Patch Manager window.
2. Click the **Filter** drop-down list, and then select a filter from the list.

Viewing security information for a scanned device

You can also view information specific to scanned devices directly from the network view by right-clicking one or more selected devices, and then clicking **Security and Patch Information**.

This dialog lets you view detection, installation, and repair history, and perform patch management tasks.

Purging unused definitions

You can purge unused definitions from the Security and Patch Manager window and the core database if you determine that it isn't relevant to your environment or if a successful remediation makes the information obsolete.

When you purge definitions, associated detection rule information is also removed from the Detection Rules groups in the tree view. However, the actual associated patch files aren't removed by this process. Patch files must be removed manually from the local repository, which is typically on the core server.

To purge unused definitions

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Purge unused definitions** toolbar button.
3. Select the platforms whose definitions you want to remove. You can select one or more platforms in the list. If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition to be removed.
4. Select the languages whose definition you want to remove (associated with the platform selected above). If you select a Windows or Macintosh platform above, you should specify the languages whose definition you want to remove. If you select a UNIX or Linux platform above, you must specify the Language neutral option in order to remove their language independent definitions.
5. Click **Remove**.

Working with patches

Downloading patches

In order to deploy security patches to affected devices, the patch executable file **MUST** first be downloaded to a local patch repository on your network. The default location for patch file downloads is the core server's /LDLogon/Patches directory. You can change this location on the Patch Location tab of the Download updates dialog.

Patch download location and proxy server settings

Patch downloads always use the download location settings currently found on the Patch Location tab of the Download updates dialog. Also note that if your network uses a proxy server for Internet access, you must first configure the proxy server's settings on the Proxy Settings tab before you can download patch files.

Security and Patch Manager first attempts to download a patch file from the URL (shown on the Patch Properties dialog). If a connection can't be made, or if the patch is unavailable for some reason, then the patch is downloaded from the LANDesk Security content service, which is a LANDesk-hosted database containing patches from trusted industry sources.

You can download one patch at a time, or a set of patches together at the same time.

To download patches

1. From any Detection Rules group, right-click a detection rule, and then click **Download Patch**. You can also download patches for custom definitions from the detection rule dialog when creating or editing a custom definition.
2. Or, to download a set of patches, select any number of rules in any Detection Rules group, right-click the selection, and then click **Download Patch**.
3. The download operation and status displays in the Downloading Patches dialog. You can click **Cancel** at any time to stop the entire download process.
4. When the download is finished, click the **Close** button.

Downloading associated patches only

You can also just download those patches associated with a specific vulnerability (or other security content type) definition that requires patches for remediation or a group of selected vulnerabilities. To do this, right-click the definition(s), click **Download associated patches**, select whether to all associated patches or only current patches, and then click **Download**.

For more information on patch file download status, see "Understanding and using the Security and Patch Manager tool window" on page 321.

Uninstalling patches

You can uninstall patches that have been deployed to managed devices.

For example, you may want to uninstall a patch that has caused an unexpected conflict with an existing configuration.. By uninstalling the patch, you can restore the device to its original state.

To uninstall a patch

1. From any detection rule listing, right-click one or more rules, and then click **Uninstall Patch**.
2. Enter a name for the uninstall task.
3. Specify whether the uninstall is a scheduled task or a policy-based scan, or both.
4. If you selected scheduled task, specify which devices from which you want to uninstall the patch.
5. If the patch can't be uninstalled without accessing its original executable file (i.e., to use command-line parameters), and you want to deploy the executable using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. For more information, see "About the Multicast options dialog" on page 748.
6. If you selected policy, and you want to create a new query based on this uninstall task that can be used later, click the **Add a query** check box.
7. Select a scan and repair setting from the available list (or create a custom setting for this scan, to determine how the scanner operates on end user devices).
8. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Removing patches from the core database

To remove patch files permanently, you must delete them from the patch repository, which is typically on the core server.

Using custom definitions

Creating custom definitions and detection rules

In addition to the known vulnerabilities that you update via the LANDesk Security and Patch Manager service, you can also create your own custom (or user-defined) definitions—; complete with custom detection rules, associated patch files, and special additional commands to ensure successful remediation.

Vulnerability definitions consist of a unique ID, title, publish date, language, and other identifying information, as well as the detection rules that tell the security scanner what to look for on target devices. Detection rules define the specific platform, application, file, or registry conditions that the security scanner checks for in order to detect a vulnerability (or practically ANY system condition or status) on scanned devices.

Security and Patch Manager's custom vulnerability definitions is a powerful, flexible feature that lets you implement an additional, proprietary level of patch security on your LANDesk system. In addition to enhancing patch security, custom vulnerabilities can be used to assess system configurations, check for specific file and registry settings, and deploy application updates, among other innovative uses that take advantage of the scanning capabilities of the vulnerability scanner.

Creating custom blocked application definitions

You can also create your own custom definitions for the blocked application type. From the **Type** drop-down list, select **Blocked Applications**, enter an executable filename and a descriptive title for the definition, and then click **OK**.

Custom definitions don't necessarily have to perform remediation actions (deploying and installing patch files). If the custom definition is defined with a Detect Only detection rule or rules that can only be detected by Security and Patch Manager, the security scanner looks at target devices and simply reports back the devices where the rule's prescribed condition (i.e., vulnerability is found). For example, you can write a custom Detect Only rule for the security scanner to check managed devices for the following:

- Application existence
- File existence
- File version
- File location
- File date
- Registry setting
- And more...

You can create as many custom vulnerability definitions as you need to establish and maintain the optimal level of patch security for your environment.

Creating custom definitions

To create custom definitions

1. Click **Tools | Security | Security and Patch Manager**.
2. From the **Type** drop-down list, select **All Types** or **Custom Definitions**. (The **Create custom definition** toolbar button is available only with one of these two types selected; or with the **Blocked Applications** type selected, if you want to create a custom blocked application definition.)
3. Click the **Create custom definition** toolbar button. An editable version of the properties dialog opens, allowing you to configure vulnerability settings.
4. Enter a unique ID for the vulnerability. (The system-generated ID code can be edited.)
5. The type is a Custom Definition and can't be modified.
6. The publish date is today's date and can't be modified.
7. Enter a descriptive title for the vulnerability. This title displays in vulnerability lists.
8. Specify the severity level. Available options include: Unknown, Service Pack, Critical, High, Medium, Low, and Not Applicable.
9. Specify the status for the vulnerability. Available options include: Don't Scan, Scan, and Unassigned. When you specify a status, the vulnerability is placed in the corresponding group in the Security and Patch Manager tree view (see "Security and Patch Manager tree view" on page 325).
10. The language setting for user-defined vulnerabilities is automatically set to INTL (International or Language neutral, which means the vulnerability can be applied to any language version of operating systems and/or applications).
11. The Detection Rules list displays all the rules used by this vulnerability. If you are creating a new custom vulnerability, you should configure at least one detection rule that is used by the security scanner to scan devices for the vulnerability. To add detection rules, click **Add**. (See the procedure below for step-by-step instructions.)
12. If you want to provide additional information about this vulnerability, click the **Description** tab and type your comments in the text box and/or enter a valid Web address where more information is posted.

As with known vendor vulnerabilities, custom vulnerabilities should include one or more detection rules that tell the security scanner what conditions to look for when scanning managed devices. Follow the steps below to create a detection rule for a custom vulnerability.

Creating custom detection rules

To create custom detection rules

1. Right-click a custom definition, and then click **Properties**. (Or double-click the vulnerability definition.)
2. Click the **Add** button located under the Detection Rules list. An editable version of the Rules Properties dialog opens at the dialog's General Information page, allowing you to configure a detection rule.
3. At the General Information page, enter a unique name for the rule. The rule's status cannot be modified here. To change the status of a detection rule, right-click the rule in any list view, and then click **Enable** or **Disable**, depending on the current state. The rule's definition information cannot be modified here either. However, you can enter any information you want in the Comments box.

4. Use the various pages of the Rules Properties dialog to define the detection rule, as described in the rest of this procedure.
5. Open the Detection Logic pages.
6. At the Affected Platforms page, select the platforms you want the security scanner to run on to check for this detection rule's definition. The list of available platforms is determined by the vulnerabilities you've updated via the LANDesk Security and Patch Manager service. Click **Load default platform list** to add the available platforms to the list. You must select at least one platform.
7. At the Affected Products page, associate the rule with one or more specific software applications. First, click **Edit** to open the Selected Affected Products dialog where you can add and remove products in the Affected Products list (this list can be shortened if you like, by clicking the check box at the bottom of the dialog). The list of available products is determined by the content you've updated via the LANDesk Security and Patch Manager service. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If the specified associated product is found on the device, the scan quits. However, if the product is found, or if no products are specified, the scan continues to the files check.
8. At the Files page, configure specific file conditions that you want the rule to scan for. Click **Add** to make the fields on this page editable. The first step in configuring a file condition is to specify the verification method. The fields on this tab depend on the verification method you select. To save a file condition, click **Update**. You can add as many file conditions as you like. For a detailed description of this option, see "About the Detection logic: Files used for detection page" on page 731.
9. At the Registry Settings page, configure specific registry conditions that you want the rule to scan for. Click **Add** to make the fields editable. To save a registry condition, click **Update**. You can add as many registry conditions as you like. For a detailed description of this option, see "About the Detection logic: Registry settings used for detection page" on page 732.
10. At the Custom Script page, you can create a custom VB script to assist with detection for this detection rule. The security scanner agent's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.
Note: You can click the **Use editor** button to open your default script editing tool, associated with this file type. When you close the tool you're prompted to save your changes in the Custom Script page. If you want to use a different tool you have to change the file type association.
11. At the Patch Information page, specify whether the vulnerability associated with this detection rule can be repaired or can only be detected on your managed devices. If you select the repair option, the Patch Download Information and Repair Information fields become editable.
12. If you can repair by deploying a patch, enter the URL to that patch file and specify whether it can be downloaded automatically. (You can attempt to download the associated patch file at this time by clicking **Download**, or you can download it at another time.)
13. Also, if you can repair by deploying a patch, enter a unique filename for the patch file and specify whether the patch requires a reboot in order to complete remediation and if the patch requires user input during remediation. (For a detection rule that includes remediation, we strongly recommend you create a hash for the patch file by clicking **Generate MD5 Hash**. The actual patch file must be downloaded before you can create a hash. For more information on the hash, see "About the Detection rule: General information page" on page 730.)

14. For a rule that allows remediation of the associated vulnerability, you can configure additional commands that are run during the remediation process on affected devices. To configure additional remediation commands, click the Patch Install Commands page, and then click **Add** to select a command type and to make the command's argument fields editable. Additional patch install commands are NOT required. If you don't configure special commands, the patch file executes as it normally would by itself. For a detailed description of this option, see "About the Patch install commands page" on page 735.

Now that you've created a custom vulnerability definition, you can do the same things with it as you would with a known vulnerability from an industry source. You can set the vulnerability's status to Scan or place it in the Scan group to be included in the next security scan, place it in the Don't Scan or Unassigned group, view affected computers, enable Auto Fix, create a repair job, or clear scan/repair status. To choose an option, right-click a custom vulnerability definition to access its shortcut menu.

Two operations that are unique to user-defined definitions are importing and exporting, and deleting.

Importing and exporting custom definitions

Security and Patch Manager provides a way for you to import and export custom definitions and their detection rules. You can't import and export known industry vulnerability definitions.

Custom definitions are exported and imported as an XML-formatted file.

Import and export is useful if you want to share custom definitions with other core servers. Exporting makes it possible for you to save a backup copy for a definition that you want to remove temporarily from the core database.

You can also use the export/import feature to export a definition, manually edit the exported file as a template and save multiple variations of the definition, and then import the new definitions. If the definition is complex, this procedure can be faster and easier than creating multiple definitions in the console.

To export custom definitions

1. From a Custom Definitions list, select one or more custom definitions.
2. Click the **Export** toolbar button. (Or, right-click the selected definitions, and then click **Export**.)
3. Enter the path to the folder where you want to export the definitions as an individual XML file.
4. If you've exported the definitions before to the specified location and you want to replace it, click the **Overwrite existing definitions**.
5. Click **Export**. Check the Export Status window to see whether the definitions are successfully exported.
Note: An exported definition continues to exist in the core database, and therefore still appears in the Custom Definitions group that corresponds to its status: Unassigned, Scan, or Don't Scan.
6. Click **Close**.

To import custom definitions

1. In the Security and Patch Manager window, click the **Import Custom Definitions** toolbar button.
2. Locate and select one or more definitions (in the XML file you want to import), and then click **Open**. If the definition already exists in the core database, you're prompted whether you want to overwrite it. Check the status window to see whether the definition is successfully imported.
3. Click **Close**. Imported definitions (new and updated) are placed in the Custom Definitions Unassigned group.

Deleting custom definitions

If you no longer need a custom definition, you can delete it. Deleting a custom definition removes its information and its associated detection rules from the core database, and from the Security and Patch Manager window. (Exporting does not remove the definition information.)

As with purging known vulnerability information, deleting custom definitions does not remove any downloaded associated patch files. Patch files must be removed manually from the patch repository.

To delete custom definitions, select one or more custom definitions, and then click the **Delete selected custom definitions** button in the toolbar.

Restoring exported custom definitions

If you delete a custom definition that had previously been exported as an XML file, you can restore that definition by importing it back into Security and Patch Manager.

Scanning and remediating devices

This section provides information on scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports.

For information on updating and viewing security content, creating and using custom definitions, and downloading and working with patches, see "Managing security content and patches" on page 334.

Read this chapter to learn about:

Scanning devices

- "Scanning devices for security risks" on page 347
- "How Security and Patch Manager scans for different content types" on page 348
- "Creating security (and compliance) scan tasks" on page 350
- "Configuring scan options with scan and repair settings" on page 351
- "Using custom variables and custom variable override settings" on page 352
- "Viewing detected security data" on page 353
- "Forwarding security scan results to a rollup core" on page 353

Remediating devices

- "Remediating devices with detected security risks" on page 355
- "How Security and Patch Manager remediates different content types" on page 359
- "Remediation methods" on page 361
 - "Using a scheduled repair task" on page 361
 - "Using a repair policy (Windows only)" on page 362
 - "Using an autofix repair" on page 363
- "What happens on a device during remediation" on page 364
- "Viewing security and patch information for scanned devices" on page 364
 - "Verifying remediation status" on page 365
 - "Clearing vulnerability scan and repair status by vulnerability" on page 365

Other security management tasks

- "Creating a scheduled reboot task" on page 367
- "Using security alerts" on page 367
- "Using security reports" on page 368

Scanning devices for security risks

Traditionally, security scanning meant checking the currently installed versions of operating system and application specific files and registry keys on a device against the most current known vulnerabilities in order to identify and resolve security risks. LANDesk Security services offers expanded security content types, enabling you to scan for and remediate even more of today's prevalent security risks and exposures.

Depending on your Security Suite content subscription, you can scan for:

- Known vulnerabilities (for Windows, Mac, Linux, and UNIX)
- Custom vulnerabilities (defined by a LANDesk Administrator)
- Spyware
- Antivirus scanner status (third-party scanner engines, as well as the LANDesk Antivirus tool)
- Viruses (using the integrated LANDesk Antivirus tool, you can: download the latest virus definition files, create and deploy antivirus scans, configure antivirus scanner settings and the antivirus scan options available to end users, enable real-time file and email protection, and more. For more information, see "LANDesk Antivirus" on page 474.)
- Security threats (local system or platform configuration errors; includes firewall detection and configuration)
- Blocked applications
- LANDesk software updates
- Driver updates
- Software updates

Security Suite content subscriptions

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

How Security and Patch Manager scans for different content types

The table below describes how the security scanner works for each content type:

When scanning for...	Security and Patch Manager scans by...
LANDesk software updates	Using software update definitions published by LANDesk to check for the latest LANDesk software versions.
Windows vulnerabilities	Using vulnerability definitions published by LANDesk (based on official vendor security bulletins to check for known operating system and/or application vulnerabilities).
Macintosh vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins to check for known vulnerabilities).
Linux/UNIX vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins to check for known vulnerabilities).
Custom definitions	Using custom vulnerability definitions created by a LANDesk Administrators to check for a user-defined platform, application, file, or registry setting conditions.
Security threats	Using security threat definitions published by LANDesk to check for local Windows system configuration errors and exposures. You can modify security threat definitions that use editable custom variables to check for specific conditions.
Spyware	Using spyware detection definitions that check for instances of spyware programs on scanned devices. Security and Patch Manager uses the LANDesk Software license monitoring tool's softmon.exe program to monitor for spyware. You can also enable real-time spyware monitoring and blocking with a device's agent configuration.

When scanning for...	Security and Patch Manager scans by...
Driver updates	Using third-party driver update definitions that check for driver versions.
Software updates	Using third-party software update definitions that check for software versions.
Antivirus updates	Using antivirus scanner detection definitions (NOT actual virus definition/pattern files) that check for: <ul style="list-style-type: none"> - installation of common antivirus scanner engines (including the LANDesk Antivirus tool) - real-time scanning status (enabled or disabled) - scanner-specific pattern file versions (up to date or old) - last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)
Blocked applications	Using application definitions published by LANDesk (or user-defined application definitions) to immediately deny end user access to the application by editing the local registry. Remediation is NOT a separate procedure. Security and Patch Manager uses the LANDesk Software license monitoring tool's softmon.exe program to deny access to specified application executables, even if the executable file name has been modified, by reading the file header information. (See the legal disclaimer for the blocked application type.)

To understand how Security and Patch Manager remediates these different content types, see the "How Security and Patch Manager remediates different content types" on page 359.

Configuring the content of a security scan

After reviewing downloaded definitions and deciding which items you want to scan for, you can perform customized security assessment on managed devices by moving definitions into their respective Scan groups. When the security scanner runs, it always reads the contents of the Scan group and scans for those specific definitions (**Important:** if that type is selected in the task's scan and repair settings). Before scanning devices, you should always make sure the appropriate definitions are in the Scan group. You can move definitions into and out of the Scan group manually at any time.

You can also update security and patch content which, by default, automatically adds new definitions into the Scan group.

Blocked applications are placed in the Unassigned group by default

Keep in mind that the blocked application type is handled differently than the other types. By default, blocked application definitions are placed in the Unassigned group, not in the Scan group.

Security scans add security and patch information to a device's inventory in the core database. This information can be used to generate specific queries, policies, and reports. To view this information, right-click the device and then click **Security and Patch Information**.

Caution about moving definitions from the Scan group

When you move definitions from the Scan to the Don't Scan group, the current definition assessment information (information located in the core database about which scanned devices detected those definitions) is removed from the core database and is no longer available in either the definition Properties dialogs or in the device Security and Patch Information dialogs. To restore that information, you would have to move the definitions back into the Scan group and run the scan again.

Creating security (and compliance) scan tasks

The security and patch scanner can be run directly at a device (Click **Start | All Programs | LANDesk Management | Security and Patch Scanner**), or it can be run as a scheduled task or a policy from the core server.

Scheduled tasks can be thought of as a push distribution because the task is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

Compliance security scans

With Security and Patch Manager you can also create and configure a compliance-specific security scan, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task, a policy, and even initiated by LANDesk Antivirus when a virus is detected that can't be removed or quarantined (see the options on the **Compliance** tab of a **Scan and repair settings** dialog).

On-demand security and compliance scans

You can also run an immediate security and/or compliance scans on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), click **LANDesk Security/Compliance scan now**, select a scan and repair setting, choose the type of scan, and then click **OK**.

To create a security scan task

1. Click **Tools | Security | Security and Patch Manager**.
2. Make sure security and patch content has been updated recently.
3. Make sure the **Scan** group contains only those definitions you want to scan for.
4. Click the **Create a task** toolbar button, and then click **Security scan**. The Create security scan task dialog displays.
5. Enter a name for the scan.
6. Specify whether the scan is a scheduled task or a policy-based scan, or both.

7. Select a scan and repair setting from the available list (or create a custom setting for this scan), to determine how the scanner operates on end user devices.
8. Click **OK**. For a scheduled task scan, you can now add target devices and configure the scheduling options in the Scheduled tasks tool.

About the security scan log file

The security and patch scanner writes a log file for the most recent scan on the device called **vulscan.log**, and also saves the last five log files in chronological order by number. These log files record useful information about the time of the scan, language, platform, and the processes run by the scan.

Viewing the most recent security scan dates in the device Inventory

To see when the last security scan was run on a device, right-click the device, click **Inventory**, and then scroll down to the **Last Scan Dates** in the right-hand pane of the Inventory view.

Configuring scan options with scan and repair settings

Security and Patch Manager gives you complete control over what the end user sees, device reboot behavior, and the level of interaction the end user is allowed when the security and patch scanner runs on devices. For example, depending on the purpose or scheduled time of a scan you may want to show the end user scanner progress and give them the opportunity to cancel or defer an assessment scan or patch deployment remediation. You can do this by creating and applying scan and repair settings.

Scan and repair settings is also where you determine the content of a security scan, by selecting specific definition types.

You can create and apply scan and repair settings (a saved set of configured options) to scan tasks. You can create as many scan and repair settings as you like. Some scan and repair settings might be well suited for a variety of scanning or remediation tasks, while others might be specifically designed for a single task.

All of the scan and repair settings you create are stored in the **Scan and Repair** group located under **Settings** in the Security and Patch Manager tree view.

To create scan and repair settings

1. In the Security and Patch Manager window, click the **Configure settings** toolbar button, and then click **Scan and repair settings**.
2. Click **New**. Or, you can click **Edit** or **Configure** on any of the task dialogs that let you apply an scan and repair setting.
3. Enter a name for the scan and repair setting.
4. Specify the settings on the tabs as desired for the particular task (scan, repair, reboot). For more information about an option, click **Help**.

Note that the **Compliance** tab applies only to compliance security scan tasks.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, reboot tasks, and change settings tasks.

Changing a device's default scan and repair settings

A device's default scan and repair settings are deployed as part of the initial agent configuration. When a task has a different scan and repair settings associated or assigned to it, the default settings are overridden. You can also choose to use the device's default settings by selecting it when you create a task.

At some point you may want to change these default scan and repair settings on certain devices. Security and Patch Manager provides a way to do this without having to redeploy an entirely new and complete agent configuration. To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button.

The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing scan and repair settings as the default or use the **Edit** button to create a new scan and repair settings as the default for target devices.

Using custom variables and custom variable override settings

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected). Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

Edit Custom Variables right required

In order to edit custom variable settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Every security definition with customizable variables has a unique set of specific values that can be modified. In each case however, the **Custom Variables** tab will show the following common information:

- **Name:** Identifies the custom variable. The name can't be modified.
- **Value:** Indicates the current value of the custom variable. Unless the variable is read-only, you can double-click this field to change the value.
- **Description:** Provides additional useful information about the custom variable from the definition publisher.
- **Default value:** Provides the default value if you've changed the setting and want to restore it to its original value.

To change a custom variable, double-click the **Value** field, and either select a value if there's an available drop-down list, or manually edit the value, and then click **Apply**. Note that some variables are read-only and can't be edited (this is usually indicated in the description).

Custom variable override settings

In some situations you may want to ignore a custom variable setting, or in other words create an exception to the rule. You can do this with a feature called custom variable override settings. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules. A user must have the Edit Custom Variables right in order to create or edit a custom variable override setting. You can create as many custom variable override settings as you like, and apply them to devices using a **Change settings** task. For more information, see "About the Custom variable override settings dialog" on page 751.

Viewing detected security data

If the security scanner discovers any of the selected definitions, this information is reported to the core server. You can use any of the following methods to view detected security data after running a scan:

By the Detected group

Select the **Detected** group in the Security and Patch Manager window to view a complete listing of all definitions detected by the most recent scan. The Scanned column indicates how many devices were scanned for a definition, and the Detected column shows how many of those devices are affected by that definition.

By a definition

Right-click a definition, and then click **Affected computers** to view a list of devices on which the definition was detected by the most recent scan.

By an individual device

Right-click a specific device in the network view, and then click **Security and Patch Information** to view detailed security assessment information and patch deployment status for the device. For more information, see "About the Security and patch information dialog" on page 745.

By a group of selected devices

Select multiple devices in the network view, right-click the group, and then click **Security and Patch Information** to view a list of definitions discovered on one or more of those devices. When you select a definition in the list, the devices on which the definition was detected by the most recent scan display in the bottom pane.

Forwarding security scan results to a rollup core

If you're working in a large, distributed enterprise network, you may want to forward the latest security scan results to a rollup core server located in a specific region in order to facilitate access to real-time vulnerability information for all of your managed devices. You can enable automatic and immediate security (vulnerability) scan results forwarding by defining the rollup core settings in the Security and Patch Manager tool.

Every time the security scanner runs it writes a scan results file to a folder called VulscanResults on the core server and notifies the LANDesk Security web service, which adds the file to the core database. If the rollup core settings are enabled and a valid rollup core is identified, the rollup core reads the scan results file into its own database, providing faster access to critical vulnerability information.

To enable the immediate forwarding of security scan results to a rollup core

1. In the Security and Patch Manager window, click the **Configure settings** toolbar button, and then click **Rollup core settings**.
2. Check the **Send scan results to rollup core immediately** checkbox.
3. Enter the name of the rollup core you want to receive the latest security scan results.
4. If you want to use the default URL (location on the rollup core) where the scan results file is written, check the **Use default rollup URL** checkbox. Otherwise, you can clear the checkbox and enter a preferred address.

Remediating devices with detected security risks

Once you've updated security and patch content for the content types you've have a license or subscription for, scanned devices, determined which detected security exposures require attention, and downloaded patches, the next step in implementing security and patch management is to remediate (or repair the security problem).

Remediation solutions and actions are different depending on the type of security risk. Furthermore, some remediation can be done remotely with the Security and Patch Manager tool, while other remediation tasks must be done manually. For example, vulnerabilities are remediated by deploying and installing the necessary security patches on affected devices, while spyware is remediated by removing the infecting spyware itself, and a system configuration security threat is typically remediated by editing the registry or changing some other platform-specific setting.

Remediation by security content (definition) types

Remediation for each security content type is described below:

Known vulnerabilities

For known vulnerabilities, remediation entails deploying and installing the appropriate security patch. Windows and Macintosh vulnerability remediation can be performed via the console, as a scheduled task, or policy-based remediation, or as an autofix scan. However, Linux and UNIX vulnerability remediation must be done manually at the affected device.

Custom definitions

For custom definitions, remediation can consist of deploying a custom patch or script that addresses the exposure. Like known vulnerability remediation, custom vulnerability repair tasks can be done via the console.

LANDesk software updates

For LANDesk software updates, remediation means the proper version upgrade is installed. You can do this via the console.

Security threats

For security threats (local Windows system or platform configuration errors and exposures), remediation means applying the configuration settings specified by the security threat definition. You can do this via the console. You can also modify security threat definitions that use editable custom variables to apply customized settings.

Some security threats must be remediated manually at the affected device. To find out whether a security threat can be remediated from the console, view its Repairable column value (Yes or No) in the item list view.

Firewall detection and configuration (using Windows firewall settings and security threat definitions)

For Windows firewall configurations, remediation means applying configuration settings specified by Windows firewall settings or predefined security threat definitions.

Windows firewall settings are associated with a change settings task to enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs) on target devices running the following Windows platforms:

- Windows 2003/XP
- Windows Vista

Additionally, LANDesk Security provides predefined security threat definitions that let you scan for, detect, and configure firewall settings on managed devices running specific Windows platforms. The following security threat definitions let you scan for and modify firewall configurations:

- **ST000102:** Security threat definition for the Windows firewall on Windows 2003 SP1; Windows XP SP.
- **ST000015:** Security threat definition for the Internet Connection Firewall on Windows 2003 SP1; Windows XP SP2.

The Windows firewall security threat properties includes custom variables that let you configure Windows firewall settings. You can use these security threat definitions to scan for your specified settings and return a vulnerability condition if those settings are not matched. You can then use the customized definition in a repair task in order to turn on or off the firewall as well as change or reconfigure the firewall settings on the scanned device.

Windows GPO could change firewall settings

You should be aware that it is possible for a Windows Group Policy Object (GPO) to interfere with firewall settings configured with the security scanner. For example, the firewall settings you define in the Configure the Windows Firewall security threat's custom variables dialog and that are then implemented by a security scanner repair task could be changed back to their original value according to how the settings are defined in an active Group Policy Object.

Spyware

For spyware, remediation consists of removing the violating spyware application. This can be done remotely from the console with a repair task.

You can also configure a device for real-time spyware monitoring (scanning, detection, and removal). In order to use real-time spyware monitoring, you must enable the settings in the device's agent configuration. On the **Spyware** page of the **Agent configuration** dialog, check the appropriate spyware monitoring options to enable real-time spyware monitoring and end user notification. Real-time spyware monitoring uses the LANDesk Software license monitoring tool's softmon.exe program to monitor for spyware and to create log files that are read by the security and patch scanner when it scans for spyware definitions on target devices.

Autofix must be enabled for real-time spyware monitoring

In order for real-time spyware scanning and detection to work, downloaded spyware definitions must have the autofix option enabled. You can manually enable the autofix option for spyware definitions in item lists in the Security and Patch Manager tool window. Or you can configure spyware definition updates so that the autofix option is turned on by default when spyware definitions are downloaded.

Blocked applications

For blocked applications, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to any unauthorized applications.

Security and Patch Manager uses the LANDesk Software license monitoring tool's softmon.exe program to deny access to specified application executables, even if the executable file name has been modified, by reading the file header information.

Antivirus updates

Antivirus updates are available for several common antivirus products, including LANDesk Antivirus. See the **Definition types** list in the **Download updates** dialog to see the antivirus scanner engines that are supported, meaning the antivirus scanners you can download detection definitions for.

Antivirus scanner detection content versus virus definition content

Antivirus updates does not imply actual virus definition (or pattern) files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download LANDesk Antivirus updates, both the scanner detection content AND the LANDesk Antivirus-specific virus definition files are downloaded. LANDesk Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the `\\LDLogon\Antivirus\Bases` folder.

Antivirus updates are scanner definitions that detect:

- Installation of common antivirus scanner engines (including the LANDesk Antivirus tool)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

When you deploy a security scan with antivirus scanner detection definitions, the security scanner checks whether an antivirus scanner engine is installed on managed devices, whether real-time scanning is enabled or disabled, whether the scanner's pattern files is up to date, and when the latest scan was run on the device. You can remotely enable real-time scanning if it's turned off.

Remediating Linux and UNIX devices manually

Supported Windows and Macintosh devices can be remediated remotely from the console, but other platforms such as Linux and UNIX Sun Solaris can only be scanned from the console, not remediated.

You must manually install the appropriate patches on both Linux and UNIX devices in order to remediate them.

How Security and Patch Manager remediates different content types

The table below describes how Security and Patch Manager remediates the various security content types:

When remediating...	Security and Patch Manager remediates by...
LANDesk software updates	Deploying and installing the appropriate LANDesk software update.
Windows vulnerabilities	Deploying and installing the required patch files (patch files must already be downloaded to the local patch repository).
Macintosh vulnerabilities	Deploying and installing the required patch files
Linux/UNIX vulnerabilities	Remediation is performed manually at the affected device.
Custom definitions	Deploying and installing patch files, if the associated detection rule allows remediation, and if the specified patch files are available.
Security threats	Applying configuration settings specified by the security threat definition. You can do this via the console. You can also modify security threat definitions that use editable custom variables to apply customized settings. Some security threats must be remediated manually at the affected device. To find out whether a security threat can be remediated from the console, view its Repairable column value (Yes or No) in the item list view.
Spyware	Removing the detected spyware instance. See the spyware section above for more information on real-time spyware detection and removal.
Driver updates	Deploying and installing the appropriate third-party driver update.

When remediating...	Security and Patch Manager remediates by...
Software updates	Deploying and installing the appropriate third-party software update.
Antivirus updates	Allowing you to re-enable real-time scanning if it's been turned off. The other antivirus scanner detection definitions return status information about specific antivirus scanner engine installations, pattern file versions, and last scan dates (related issues can't be remediated remotely from the console).
Blocked applications (published and custom)	Denying access to the application, even if the program's executable file name has been changed, by reading the file header information. Remediation in this case is NOT a separate procedure. Application blocking is done during the security scan process. The security scan immediately denies end user access to the application by editing the registry. (See the "Legal disclaimer for the blocked applications type" on page 333.)

To understand how Security and Patch Manager scans for these different content types, see the "How Security and Patch Manager scans for different content types" on page 348.

Remediating from the console

As stated above, Windows and Macintosh vulnerabilities, custom definitions, LANDesk software updates, and blocked applications can be remediated from the console. The sections below describe these different methods.

Intelligent patch deployment remediation

Security and Patch Manager performs an intelligent remediation by installing only those patches that are needed on each individual device, not all of the patches referenced by all of the vulnerabilities included in the repair job. The tool also takes advantage of LANDesk's enhanced package deployment capabilities for fast and efficient patch deployment, such as: Targeted Multicast, peer download, and checkpoint restart. For more detailed information about these software distribution features, see "Software distribution" on page 162.

Remediating one or more definitions at a time

You can remediate a single detected definition or a set of them with any of the three remediation methods described below.

To remediate one definition at a time, right-click the item and then click **Repair**.

To remediate a set of definitions together, copy definitions from any of the content groups into a custom group (see "Understanding and using the Security and Patch Manager tool window" on page 321, right-click the group, and then click **Repair**). The Auto Fix method isn't available for custom groups; however, you can multi-select definitions in a listing, right-click and select **Auto Fix**.

Remediation methods

Security and Patch Manager provides the following methods to remediate from the console:

- "Using a scheduled repair task" on page 361
- "Using a repair policy (Windows only)" on page 362
- "Using an autofix repair" on page 363

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

Using a scheduled repair task

Scheduling a remediation or repair task is useful if you want to set up the task to run at a specific time in the future, or as a recurring task. Security and Patch Manager uses the Scheduled Tasks tool to configure and process a scheduled repair task.

Supported platforms for scheduled task remediation

Scheduled task remediation is supported on both Windows and Macintosh devices.

To create a scheduled repair task

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Schedule repair dialog displays.
3. Edit the **Task name** if you want to change the name of the repair task.
4. Click the **Repair as a scheduled task** check box.
5. (Optional) If you want this repair task to be divided into two parts: a staging task that deploys the necessary patches to affected devices, and the actual repair task that installs the patch, click the **Split into staging task and repair task**.
6. Specify which devices you want to repair. If you want the current affected devices automatically added to the target list in the Scheduled Tasks window, click the **Add all affected devices** check box. The vulnerable devices are those devices where the vulnerability was detected by the last scan. You can also add more targets once the task is created in the Scheduled Tasks window.
7. If you want patches to be deployed using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. See "About the Multicast options dialog" on page 748 below for details.

8. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
9. Specify whether to only download the patch and not deploy and install it on affected devices.
10. Select a scan and repair setting for this repair task. The scan and repair setting determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
11. Click **OK**.
12. The task appears in the Scheduled Tasks window with the job name specified above, where you can further customize the target device list and configure scheduling options.

Using a repair policy (Windows only)

Policy-based remediation offers flexibility by letting you dynamically target devices based on the results of a custom LDAP or core database query. For example, you can configure a remediation policy so that it runs only on devices in a particular directory container, or only on devices running a specific OS (or any other inventory attribute that can be queried). Security and Patch Manager uses policies in the Scheduled tasks/Software distribution tool to configure and process remediation policies.

Supported platforms for policy-based remediation

Policy-based remediation is supported on Windows devices only. Macintosh devices can't be remediated via the application policy method.

In order to be remediated by a policy, a device must have the Software distribution agent installed. When the agent runs, it checks the core database for policies that might apply to it. If such policies exist, a dialog appears at the device showing recommended and optional policies (required policies are automatically applied).

Remediation (repair) policies operate in much the same way as application policies do, except you're distributing patch files instead of application files. Policy management prerequisites, task flow, policy types, and static and dynamic targeting are essentially identical between repair policies and application policies. For more information on policies, see the software distribution chapter.

To create a policy-based remediation

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Schedule repair dialog displays.
3. Edit the **Task Name** if you want to change the name of the repair task.
4. Check the **Repair as a Policy** check box.
5. If you want to create a new query, based on this vulnerability definition, that can be used later to scan other managed devices, check the **Add a query** check box.

6. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
7. Specify whether to only download the patch and not deploy and install it on affected devices.
8. Select a scan and repair setting for this repair policy. The scan and repair setting determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
9. Click **OK**.
10. The new policy appears in the Policies group in the Scheduled Tasks window with the name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using an autofix repair

Auto Fix is a convenient, integrated method for quick remediation in cases where you don't want to create a scheduled task or policy-based repair task. For example, if there is a new known vulnerability that you want to scan for and repair in a single process, you can use the Auto Fix feature.

Auto fix is available for the following content types: vulnerabilities, spyware, LANDesk software updates, and custom definitions.

Requirements for using Auto Fix

Only Administrators or users with the Patch Manager right AND the Default All Machines scope can enable the Auto Fix feature for applicable definitions. LANDesk users without either the LANDesk Administrator or Patch Manager right won't even see this option on a definition's shortcut (right-click) menu. For more information on rights and scope, see "Role-based administration" on page 59.

Auto fix has to be enabled in two places in order to work properly. The first setting is on the and the second setting is the scan and repair setting applied to the scheduled scan task. If either one of these two item's autofix option is NOT enabled, autofix will not happen.

When Auto Fix is enabled in both places mentioned above, the next time the security scanner runs (either manually or via a scan task), Security and Patch Manager automatically deploys and installs the required patch on any affected device. With Auto Fix, if a patch requires a reboot, the target device always automatically reboots.

You can enable Auto Fix for an individual definition, or a multi-selected group of definitions at once.

To configure Auto Fix remediation

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click one or more selected definitions from one of the content groups. You can't enable autofix on a custom group.
3. Click **Autofix when scanning**.

4. Now run the security scanner on the devices you want to scan and automatically remediate using a scheduled security scan task with a scan and repair setting where the autofix option is enabled.

What happens on a device during remediation

Automated remediation entails deploying and installing patches on managed devices, by any of the three methods described in the sections above.

It is important to remember that a repair job can include remediation for one or more detected security definitions. Furthermore, a single detected definition can require the installation of one or more patches to fix. Because of these factors, remediation might imply the installation of just one patch file on the device, or the installation of several patch files on the device, depending on the number and type of detections.

Almost all patch files install silently, meaning transparently, requiring no user interaction at the end user device itself. Some Windows 9.x patches and non-English patches do not install silently. You can tell whether a patch installs silently or not by checking the Silent Install column in a patch listing. For more information, see "Understanding and using the Security and Patch Manager tool window" on page 321 earlier in this chapter.

Configuring security scanner display and interaction on end user devices

However, whether a patch file can install silently or not, you can now configure how much you want the security scanner to display and prompt for input on the end user device with the scan and repair setting feature.

Consolidated reboot

If a patch file installation requires a reboot (AND the **Never reboot** option isn't selected on the Reboot tab of the scan and repair setting applied to the task in question), Security and Patch Manager first installs ALL of the specified task's patches on the device, and then reboots the device once.

Additional commands (for custom definitions only)

Custom definition remediation can include special additional commands that are defined when you create a custom detection rule. Additional commands run in the order specified on that rule's Commands tab, and according to the arguments for each command. Additional commands can run before, during, or after the patch file itself executes.

Viewing security and patch information for scanned devices

As mentioned above, one way to view scanned security data is by device. To do this, right-click a single device or a group of selected devices, and then click **Security and Patch Information**.

This page provides many useful functions. With one or more devices selected, you can:

- View detected definition lists
- View detailed information about when and why the detection occurred
- View installed patch and software update lists
- View detailed information about when the patch was installed or uninstalled
- Clear patch install status
- View repair history data
- Clear repair history data

You can also right-click definitions and detection rules in their respective item lists to run common tasks for one or more affected devices.

Viewing the most recent security scan dates in the device Inventory

To see when the last security scan was run on a device, right-click the device, click **Inventory**, and then scroll down to the various **Last Scan Dates** in the right-hand pane of the Inventory view.

Verifying remediation status

After performing remediation on affected devices, Security and Patch Manager reports the status of each patch installation. You can check the status of patch installation per vulnerability/definition and per target device.

To verify patch installation on a device

1. Run the security scanner on the device.
2. Right-click a remediated device in the network view, and then click **Security and Patch Information**.
3. Click the **Installed Patches** object in the left-hand pane.
4. Check the **Patch Information** fields at the bottom of the dialog.

The **Install status** field indicates whether the installation was successful. Possible states include: Succeeded, Failed, and Failed to Download.

Clearing vulnerability scan and repair status by vulnerability

If a patch installation failed, you must first clear the install status information before attempting to install the patch again. You can clear the install (repair) status for the selected device by clicking **Clear** on this dialog. You can also clear the patch install status by vulnerability.

You can clear vulnerability scan and repair status information for all devices affected by a vulnerability (or vulnerabilities with the **Clear scan/repair status dialog**. As stated above, if a patch installation fails, you must first clear the install (repair) status before attempting to install the patch again.

You can also use this dialog to remove vulnerability scan information from the database for one or more vulnerabilities.

To clear vulnerability scan and repair status, right-click the vulnerability and select **Clear scan/repair status**, select the desired options, and then click **Clear**.

Other security management tasks

Creating a scheduled reboot task

Security and Patch Manager provides a tool that lets you create a device reboot task. A reboot task can be useful when you want to install patches, without rebooting, as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

To create a reboot task

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Create a task** toolbar button, and then click **Reboot**.
3. Specify whether the reboot is a scheduled task or a policy-based scan, or both.
4. Select a scan and repair setting from the available list (or create a custom setting just for this scan task), to determine how the scanner operates on end user devices. (**Note:** Only the reboot settings in the scan and repair setting are used by a reboot task.)
5. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above, where you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using security alerts

You can configure vulnerability alerting so that you can be notified when specific vulnerabilities are detected on managed devices in your system. Security and Patch Manager's vulnerability alerting uses the standard LANDesk alerting tool.

A vulnerability must be copied to the Alert group in order to generate an alert when detected. A vulnerability in the Alert group is a copy, and also resides in the Scan group. After placing the desired vulnerability definitions in the Alert group (either manually, or by specifying the severity level vulnerabilities to automatically be placed during downloads), you can configure the alert interval in the Configure alerts dialog.

To configure vulnerability alerting

1. Specify which vulnerabilities will generate an alert by manually placing downloaded vulnerability definitions into the Alert group.
2. Or click the **Configure settings** toolbar button, and then click **Alert settings**.
3. Specify a minimum alert interval for alerting.
4. To configure security and patch alerting, select the definitions (by severity level) you want to be automatically placed in the **Alert** group during a download process. You can select more than one vulnerability severity level. These vulnerability definitions will also automatically be placed in the Scan group.
5. To configure antivirus alerting, select the antivirus events you want to generate alerts.
6. Click **OK**.

Using security reports

Security and Patch Manager is represented by several security-related reports in the Reports tool. These reports provide a variety of useful definition assessment, patch deployment, and remediation status information for managed devices on your network, for all of the content types.

In order to access the Reports tool, and generate and view reports, a LANDesk user must have either the LANDesk Administrator right (implying full rights) or the specific Reports right.

Security and Patch Manager reports follow the same rules as reports in the Software License Monitoring group, including their ability to be copied, removed, exported, and so on from the **My Reports** and **User Reports** groups.

Running and publishing reports

You can run any report from the Reports window. From the Reports window, right-click the report you want to run, and then click **Run** (or, click the **Run** toolbar button). The report data displays in the Report View.

You can also publish reports to a secure file share where they can viewed by any user you've given the proper access credentials.

For more information about using the Reports tool, and a complete listing of the Security and Patch Manager reports with descriptions, see "Reports" on page 123.

LANDesk Network Access Control (NAC)

LANDesk® Network Access Control (NAC) is an important component of LANDesk Security Suite's comprehensive security management solution. LANDesk NAC lets you protect your network from unauthorized access, malicious intrusions, and external security exposures introduced by vulnerable or corrupted devices that can infect and damage your network.

LANDesk Network Access Control provides flexibility in implementing network access control functionality on your network by supporting common industry standards and methodologies, such as Cisco NAC, IP security, and IEEE 802.1X, as well as offering its own proprietary DHCP standards based solution.

With LANDesk NAC, you can define custom baseline security policies, scan devices (both managed and unmanaged) for security policy compliance, verify the health status (posture) of connecting devices, and deny or allow access to your critical network resources based on the device's compliance to your security policy. Healthy devices are granted full network access. If a device is determined to be unhealthy, it is blocked from accessing the network and remains in a virtual quarantine area where it can either be repaired with LANDesk Security and Patch Manager's remediation capabilities or be allowed limited network access.

LANDesk NAC solutions

LANDesk NAC enforces endpoint perimeter security by using industry standard security technologies and systems. LANDesk offers two solutions to implement LANDesk NAC services:

- **Proprietary LANDesk DHCP solution**
- **Integrated Cisco NAC solution**

This guide provides detailed information on how to set up, configure, enable, and use these network access control solutions.

This introductory chapter gives a basic overview of LANDesk NAC technology and services; describes relevant Security Suite prerequisites and tools; compares the two original LANDesk NAC solutions; and includes links to the relevant sections on setting up and using each solution.

Additional LANDesk NAC solutions

LANDesk NAC now supports two more implementations of network access control as part of LANDesk Security Suite's comprehensive compliance security solution. The two new solutions are:

- **LANDesk IP Security**
- **LANDesk 802.1X**

For information on how to set up these new LANDesk NAC solutions on your LANDesk network, see "Using the LANDesk IP Security solution" on page 452, and "Using the LANDesk 802.1X solution" on page 461.

Important: Technical knowledge and expertise required for setting up LANDesk Network Access Control

This guide adequately describes all the concepts and procedures necessary to install, configure, and use LANDesk NAC services for both the LANDesk DHCP and Cisco NAC solutions.

Note that LANDesk NAC requires additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with either Cisco Network Access Control (NAC) and Cisco Secure Access Control Server (ACS) configuration and operation, and/or DHCP server management and DHCP protocols, as well as advanced networking infrastructure design principles and administration.

You should recognize that in order to set up LANDesk NAC you may need to consult with LANDesk technical support representatives and/or affiliated LANDesk system engineers. However, you can be confident that once configured and implemented properly, LANDesk NAC will significantly increase the overall security and protection of your corporate network.

Read this chapter to learn about:

LANDesk Network Access Control overview

- "LANDesk Network Access Control overview" on page 370
 - "Compliance security policies" on page 371
 - "Understanding the basic LANDesk NAC components" on page 372
 - "Security Suite prerequisites" on page 374
 - "Supported device platforms for compliance scanning" on page 374
 - "Role-based administration with LANDesk NAC" on page 533
- "Understanding and selecting a LANDesk NAC solution" on page 376
 - "Evaluating the LANDesk DHCP solution" on page 376
 - "LANDesk NAC solution matrix" on page 377
 - The links below open separate help topics:
 - "Using the LANDesk DHCP solution" on page 379
 - "Quickstart task list for setting up LANDesk DHCP" on page 390
 - "Using the Cisco NAC solution" on page 413
 - "Quickstart task list for setting up LANDesk integrated Cisco NAC" on page 425
 - "Using the LANDesk IP Security solution" on page 452
 - "Using the LANDesk 802.1X solution" on page 461

LANDesk Network Access Control overview

LANDesk Network Access Control (NAC) adds an extra layer of protection to your network by letting you prevent vulnerable or corrupted devices from gaining network access, as well as protect critical network resources from connected system that become corrupted.

LANDesk NAC provides flexibility in implementing network access control functionality on your network by supporting common industry standards and methodologies, such as Cisco NAC, IP security, and IEEE 802.1X, as well as offering its own proprietary DHCP standards based solution.

With network access control, you can evaluate the security credentials of any device as soon as it attempts to connect to your network by comparing it to custom security policies, monitor the security state of devices that are already connected, allow or deny network access, quarantine devices that fail to meet the security policy requirements, and remediate vulnerable devices so they can be rescanned for security policy compliance and allowed network access once they are deemed healthy.

Summary of LANDesk NAC benefits and features

With LANDesk NAC, you can:

- Create and enforce customized compliance security policies
- Implement stronger, around-the-clock, enterprise security
- Assess the security credentials (health status) of connecting devices
- Prevent infected or corrupted systems from accessing the network
- Quarantine non-compliant devices in a secure area
- Remediate infected devices to bring them into compliance
- Reduce downtime due to infections from malicious intrusions
- Protect your network, systems, applications, and data from external threats
- Extend existing security technologies and standards

Compliance security policies

Compliance security policies are comprised of rules that verify the health state of a device by checking for: vulnerabilities (in the form of missing or obsolete OS and application patches), software updates, antivirus engine and signature files, firewall presence and settings, and spyware.

For more information on defining a compliance security policy in the Security and Patch Manager tool in the console, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Understanding the basic LANDesk NAC components

The sections below describe the basic components of a LANDesk NAC implementation and the role of each component and how they interact. More detailed diagrams and process flows are shown in the topic covering each specific solution, respectively. For more information, see:

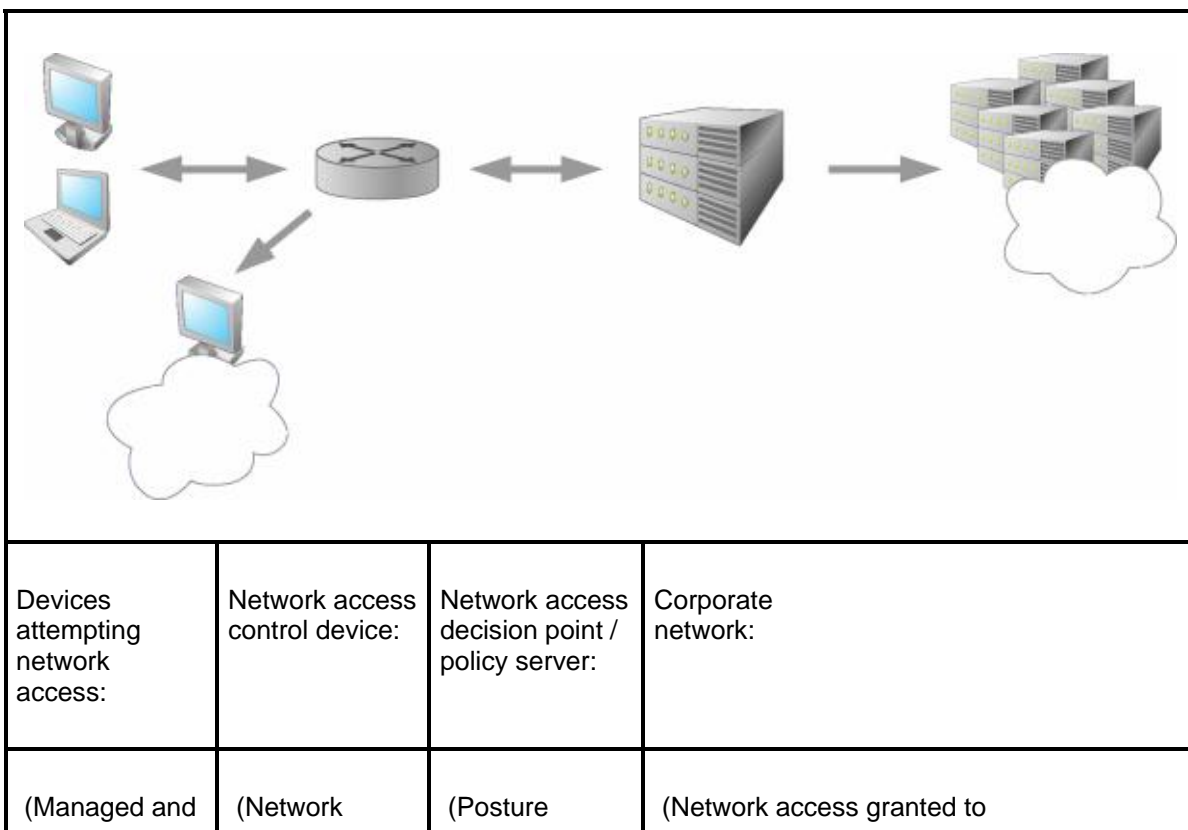
- "Using the LANDesk DHCP solution" on page 379
- "Using the Cisco NAC solution" on page 413

Basic LANDesk NAC components descriptions

Component	Description
Devices attempting to access the network	<p>Includes occasionally connecting or mobile laptops, visiting contractors and guest users, as well as regular network users that attempt to access the corporate network.</p> <p>Devices with a trust agent installed (LANDesk Trust Agent or LTA for LANDesk DHCP; Cisco Trust Agent or CTA for Cisco NAC) can communicate with the policy server or posture validation server in order to send and receive health credential information, and can be repaired by the remediation server if vulnerabilities are detected during the security scan.</p> <p>Without a trust agent, a device can't communicate with the posture validation server and can't be remediated. When a device without a trust agent is scanned for the first time, the device should be directed to a Web page with links to install the appropriate trust agent. For more information, see Using the HTML template pages. Note: The Cisco NAC solution doesn't redirect to a Web page. Instead, the device displays a message box configured by the network administrator which could specify a web page if the administrator sets it up that way.</p>
Network access control device	<p>The Cisco router, working in conjunction with the Cisco Secure ACS in a Cisco NAC environment.</p> <p>The LANDesk DHCP server, configured with "scopes" representing virtual routers with both a quarantine subnet and a primary subnet, in a LANDesk DHCP environment.</p> <p>The network access control device functions as the "first hop" network device from the supplicant/requesting device perspective and begins the posture validation and authentication process.</p>
Policy server / posture validation server	<p>A dedicated back-end server also known as the posture validation server that evaluates the posture credentials (state of devices requesting access) based on the compliance rules (security policy published to it from the LANDesk core</p>

Component	Description
(network access decision point)	server). Sends a validation response (healthy, unhealthy, etc.) via the network access control device. Note: A dedicated posture validation server is required only by the Cisco NAC implementation. With the LANDesk DHCP implementation, posture validation functionality is built into the LANDesk DHCP server.
Corporate network	Critical network area and resources that LANDesk NAC protects from unhealthy, infected, or otherwise vulnerable devices.
Quarantine VLAN	Virtual safe network area where non-compliant devices can be secured and either remediated, rescanned, and then granted full access to the corporate network, or retained with restricted access to network resources such as the Internet.

Basic LANDesk NAC components and process flow



unmanaged network user devices and/or visitor devices)	router or switch)	validation service, that evaluates and enforces compliance security policies)	compliant, healthy devices)
<p>Quarantine VLAN: (Virtual safe network area to secure and/or remediate non-compliant, unhealthy devices)</p>			

Security Suite prerequisites

In order to use the LANDesk NAC feature, you must have a valid Security Suite license (core server activation). LANDesk NAC requires not only the scanning and remediation capabilities of the Security and Patch Manager tool, but Security Suite content subscriptions in order to download the vulnerability, system configuration threat, and spyware definitions, and virus pattern files, that are used to create custom compliance security policies.

A group named Compliance has been added to the Security and Patch Manager's tree view. Users with the Security and Patch Compliance right can add and remove security type definitions into and from the Compliance group. Security definitions contained in the Compliance group comprise the compliance security policy, and are scanned for on connecting devices in order to determine their health status.

For more information on Security Suite content subscriptions, see "Security content types and subscriptions" on page 318.

Supported device platforms for compliance scanning

As with its underlying Security and Patch Manager tool, LANDesk NAC services supports most of the standard LANDesk Management Suite device platforms, including the following operating systems:

- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP4 / 2003 / XP SP1
- Macintosh (10.2 and higher)

For information on configuring managed devices for compliance scanning (installing the appropriate trust agent to allow communication with routing devices and posture validation servers), see the appropriate section for LANDesk DHCP and Cisco NAC:

- "Installing the LANDesk Trust Agent on devices to enable compliance scanning" on page 454
- "Installing the Cisco Trust Agent on devices to enable compliance scanning" on page 422

Role-based administration with LANDesk NAC

LANDesk NAC relies on the following two Security and Patch Manager rights and the LANDesk Administrator right.

Security and Patch Manager right

This right is required to see and access the Security and Patch Manager tool, and download security content updates need to define compliance rules.

Security and Patch Compliance right

This right is required to add or remove security definitions from the Compliance group.

LANDesk Administrator right

This right is required to configure devices with trust agents for compliance scanning, and to configure LANDesk NAC services in the console.

Note: The LANDesk Administrator right implies all other rights, including the two security-related rights mentioned above.

Understanding and selecting a LANDesk NAC solution

The following section describes the pros and cons for both the LANDesk DHCP solution and the Cisco NAC solution.

Evaluating the LANDesk DHCP solution

Pros:

- Uses standard DHCP filtering
- No proprietary hardware requirements
- Dedicated posture validation server not required
- Less expensive

Cons:

- Moderately less secure than Cisco NAC
- Requires dedicated machine for LANDesk DHCP server
- Requires some network infrastructure changes

Evaluating the Cisco NAC solution

Pros:

- Strong security
- Includes Cisco support

Cons:

- More expensive (especially if you don't already have Cisco hardware in place)
- Vendor specific hardware
- Windows only trust agent
- Potentially significant network configuration changes
- May not be suitable for small businesses

Evaluating the LANDesk IP Security solution

The LANDesk IP Security solution leverages IP security certificates that are built into most operating systems to provide network access control at a base level. This solution works by providing certificates signed by the LANDesk core certificate authority to managed devices that have passed an initial posture check by the LANDesk core server. If the initial posture check fails then the device is assigned a unique certificate that isolates it from communicating with any other device on the network. If a device is denied access, a prompt instructs the end user how to comply with the security policies outlined by the core server. Once the device is found to be in compliance with the security policy it is assigned a healthy certificate and is granted access to the network and is able to communicate with other healthy devices.

Evaluating the LANDesk 802.1X solution

The LANDesk 802.1X Radius proxy solution works with all major switching vendors supporting the 802.1X standard. A LANDesk 802.1X Radius proxy can participate with an existing AAA (authentication, authorization, and accounting) identity-management architecture authenticating users and endpoints, or act as an independent Radius for environments only requiring endpoint compliance validation. LANDesk Radius Proxy provisions switch port access dependant upon authentication results for connected endpoints.

LANDesk NAC solution matrix

The following matrix can help you choose the right LANDesk NAC solution for your network environment.

Solution	Core technology	Description	Use case
LANDesk Cisco NAC	Cisco NAC architecture	The LANDesk posture validation server provides the network health policies to the Cisco ACS server. The Cisco ACS server in turn enforces network admission based on the clients adherence to these policies. The LANDesk remediation and core servers provide remediation for clients who do not meet the predefined security policies.	Networks with existing (or planned) Cisco infrastructure.
LANDesk DHCP	LANDesk proprietary DHCP architecture	The LANDesk DHCP server enforces the security policies defined by the administrator. Controls both managed and unmanaged Windows and Mac devices.	Networks preferring a solution that is hardware independent, easy to implement, and affordable.
LANDesk IP Security	LANDesk certificate authority	LANDesk IP Security enforces security policies utilizing a certificate based enforcement methodology. Only clients with healthy certificates will be able to communicate on the network. Those clients who fail to meet policy criteria are given a unique unhealthy certificate with rights to communicate only with either the LANDesk remediation server or core server. (Does not currently support VPN.)	Networks utilizing static IP addresses, or have limited network infrastructure flexibility.

Solution	Core technology	Description	Use case
LANDesk 802.1X	LANDesk proprietary 802.1X	LANDesk 802.1X provides network access control by requiring the proper authentication credentials as well as an active standard LANDesk agent on the device. You can also validate device health compliance with your custom security policy, and quarantine and remediate unhealthy devices.	Networks utilizing radius servers (Microsoft IAS and other major vendors) to control access.

Choose a LANDesk NAC solution

Click on the links below to learn how to set up, configure, and use each of the LANDesk NAC solutions:

- ["Using the LANDesk DHCP solution" on page 379](#)
- ["Quickstart task list for setting up LANDesk DHCP" on page 390](#)
- ["Using the Cisco NAC solution" on page 413](#)
- ["Quickstart task list for setting up LANDesk integrated Cisco NAC" on page 425](#)
- ["Using the LANDesk IP Security solution" on page 452](#)
- ["Using the LANDesk 802.1X solution" on page 461](#)

Using the LANDesk DHCP solution

This section describes how to plan, set up, configure, and enable the LANDesk DHCP implementation of LANDesk Network Access Control (NAC).

With the LANDesk DHCP solution, a DHCP server is used for IP address filtering and routing. The LANDesk DHCP server works in conjunction with your primary DHCP server to assign IP addresses to devices attempting to access the network, and communicates with the server's built-in posture validation service to verify the health (or posture) of devices attempting to access the network. Diagrams below show the components and process workflow of a LANDesk DHCP implementation. Essentially, in a LANDesk DHCP implementation, the LANDesk DHCP server acts as the network access device that allows or denies access to the network based on device health credentials.

Also, with the LANDesk DHCP solution, you can add specified devices identified by their machine or MAC address to an exclusion list if you want to allow them to bypass the posture validation process altogether and gain immediate access to your corporate network.

In addition to the specific LANDesk DHCP server component, you must also set up a remediation server in order to implement LANDesk NAC.

Important: Technical knowledge and expertise required for setting up LANDesk NAC

Note that all of the LANDesk NAC implementations require additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with one or more of the following security technologies: Cisco NAC and Cisco Secure Access Control Server (ACS) configuration and operation; DHCP server management and DHCP protocols; TCP/IP and IPSec protocols and certificate-based authentication; 802.1X Radius server configuration and 802.1X authentication and health posture validation; as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

Setting up a LANDesk DHCP implementation of LANDesk NAC

- "Quickstart task list for setting up LANDesk DHCP" on page 380
- "Understanding the LANDesk DHCP components and process" on page 381
- "Network topology and design considerations for a LANDesk DHCP implementation" on page 387
- "Installing the LANDesk Trust Agent on devices to enable compliance scanning" on page 454
- "Setting up and configuring a remediation server" on page 459
- "Setting up a LANDesk DHCP server" on page 389

What you should do after setting up a LANDesk DHCP implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk NAC is to: define your compliance security policy, publish LANDesk NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. These tasks are generally the same and apply to the LANDesk DHCP, Cisco NAC, and LANDesk 802.1X solutions. For information on performing these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Additionally, to learn more about other ongoing LANDesk NAC management tasks such as: ensuring LANDesk NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing LANDesk NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Quickstart task list for setting up LANDesk DHCP

Use this task checklist to help keep track of the steps required to set up the LANDesk DHCP solution. Use this "Quickstart task list for setting up LANDesk DHCP" on page 390.

Understanding the LANDesk DHCP components and process

This section describes the components that comprise a LANDesk DHCP solution. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when LANDesk NAC is enabled. Scenarios with and without a LANDesk Trust Agent (LTA) installed on the device are covered in the diagrams and process workflows below.

The following components are required for a LANDesk DHCP implementation.

Required components

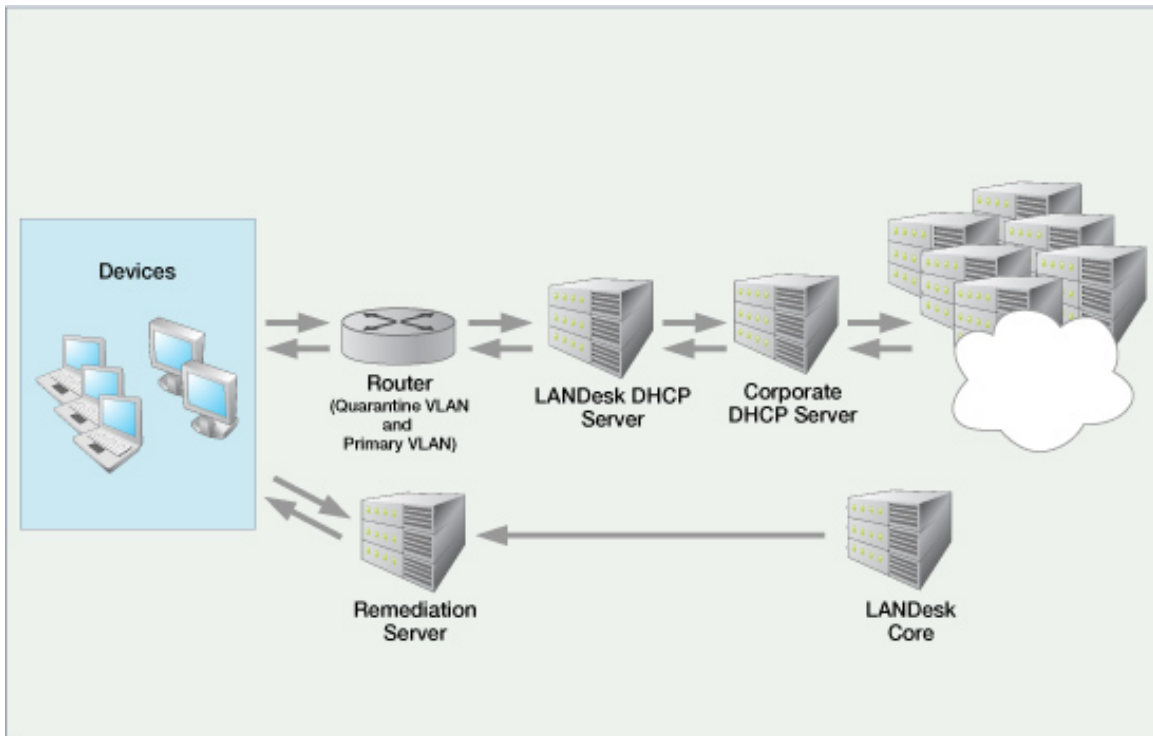
Component	Description
LANDesk core server	Provides the Security and Patch Manager tool used to: download security content (such as OS and application vulnerability definitions, spyware definitions, system configuration security threats, antivirus and firewall configuration definitions, etc.), define compliance criteria, configure posture validation servers and remediation servers, and configure and publish LANDesk NAC settings (including compliance security rules or policies and remediation resources) for scanning and repairing devices .
Corporate DHCP server	Provides permanent IP addresses to devices whose posture is validated as being healthy.
LANDesk DHCP server	<p>Acts as a network access device that enforces the compliance security policy. Communicates with the connecting device in order to evaluate the posture credentials of that endpoint device. Assigns temporary IP addresses to devices seeking network access, until the device meets compliance security criteria and can be given a permanent IP address from the primary corporate DHCP server. In other words, in a LANDesk DHCP environment, the DHCP server is the policy enforcement point on the network and grants or denies access privileges.</p> <p>The LANDesk DHCP server has posture validation functionality built in so you don't need a dedicated posture validation server. This service determines whether the connecting device has a healthy or unhealthy posture based on two factors: your compliance security policy (the contents of the Compliance group in the Security and Patch Manager tool AND the number of hours since a healthy scan as specified in the Definition of healthy setting in the Configure LANDesk NAC dialog).</p>
Remediation server	Contains the necessary setup and support files (security client, security type definitions and required patches), as well as the HTML template pages used to scan devices for vulnerabilities identified by your security policy and remediate

Component	Description
	(repair any detected vulnerabilities so that the device can be scanned as healthy or compliant and access the network).
Router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the LANDesk DHCP server to evaluate the posture credentials of the endpoint device. In a LANDesk DHCP server environment, the router/switch needs to be configured to support BOOTP/DHCP forwarding.
Devices	Mobile or guest user devices, as well as regular network user devices, attempting to access your corporate network. Typical endpoint devices include desktop computers and laptops but may also be "clientless" devices such as printers, etc. LANDesk NAC allows you to evaluate the health status of these connecting devices and control network access based on their posture credentials.

The following diagrams show a typical configuration of the components described above, as well as the posture validation process or workflow between those components.

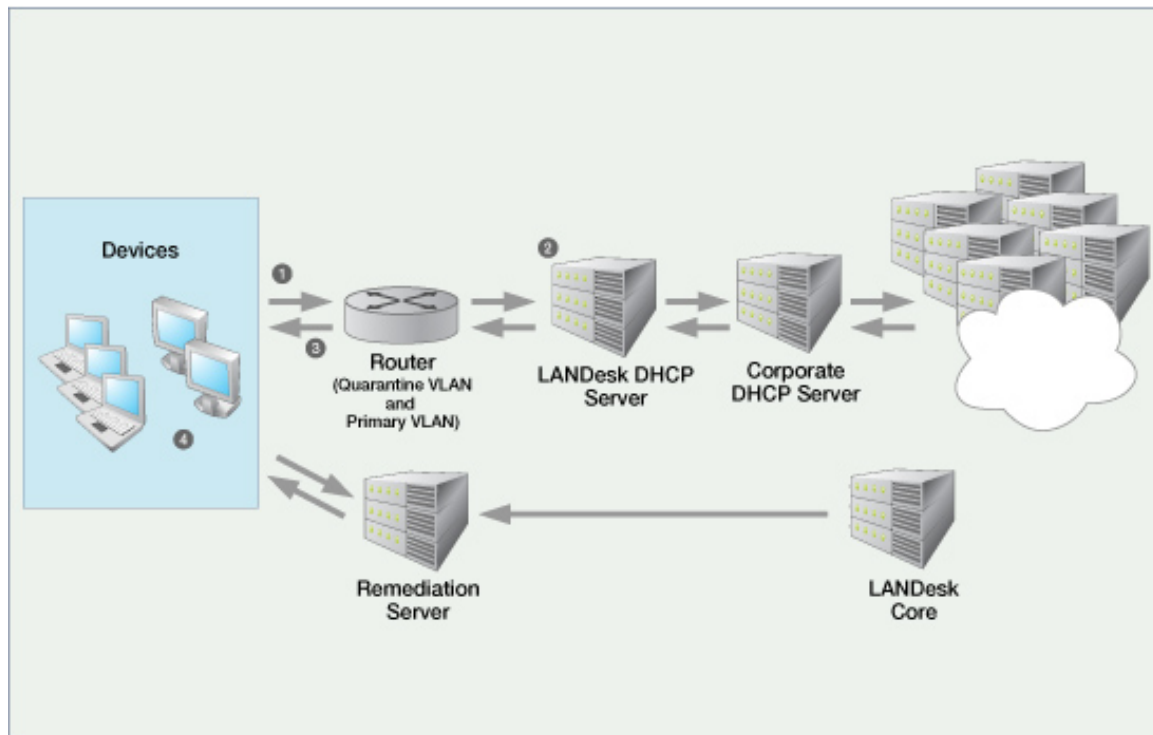
LANDesk DHCP components

The diagram below shows the specific LANDesk DHCP components:



Posture validation process for a device without the LTA installed

The diagram below shows the workflow or communication flow between the various components in a LANDesk DHCP environment when the device attempting to access the network does not have the LANDesk Trust Agent (LTA) installed. The callout numbers represent each stage of the process and are explained in the steplist below.



Process workflow:

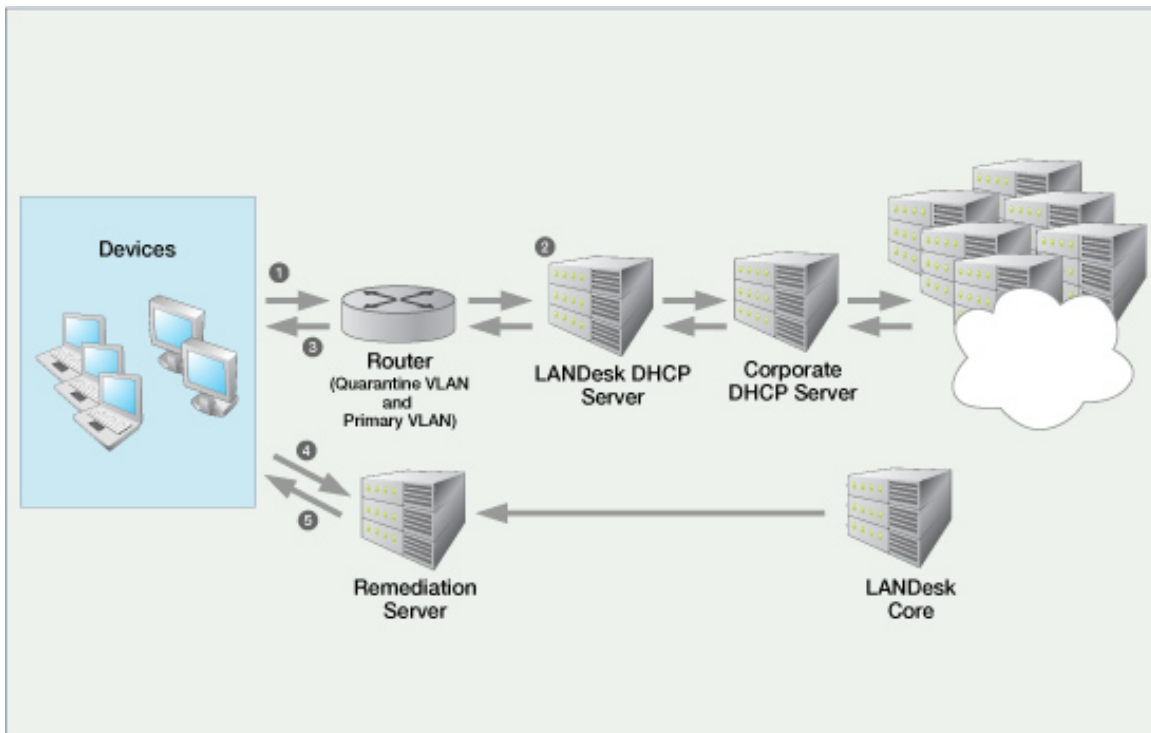
1. A device that is NOT configured with the LANDesk Trust Agent (LTA) makes an initial attempt to access the corporate network via the LANDesk DHCP server and requests an IP address.
2. The LANDesk DHCP server determines if this platform should be scanned, and its posture evaluated, by looking at Option 55 and Option 60. If the platform is to be scanned, the LANDesk DHCP server determines whether the health status of the device is known/cached, or if the device is included in the Exception List.
3. The LANDesk DHCP server returns a Quarantine VLAN IP address to the device (from the IP address pool). If the device is to be allowed, or if it is included in the Exception list, then the request is forwarded to the primary corporate DHCP server.
4. At this point, the device can either install the LANDesk Trust Agent and run the security client (from the Visitor.html page) in order to scan for and remediate any existing vulnerabilities, and become healthy or compliant with the corporate security policy, and granted access to the network. Or, the device can simply remain on the Quarantine VLAN with restricted network access, depending on the access control list rules (ACLs) defined on the router by the network administrator.

Posture validation process for a device with the LTA installed

The diagrams below show the workflow or communication flow between the various components in a LANDesk DHCP environment when the device attempting to access the network has the LANDesk Trust Agent (LTA) installed. The callout numbers represent each stage of the process and are explained below.

The LANDesk DHCP posture validation process has been divided into three phases.

Phase 1: Initial access attempt (temporary/quarantine IP address assigned; remediation offered)

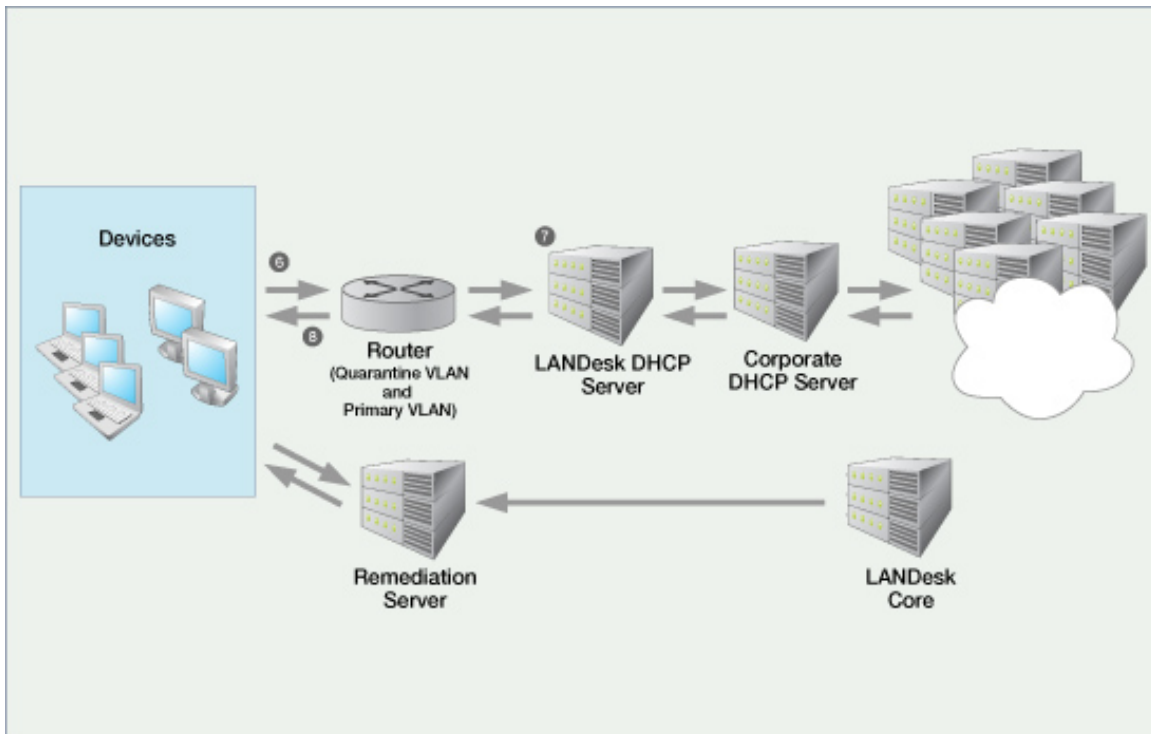


Process workflow for the initial access attempt:

1. A device that is configured with the LANDesk Trust Agent (LTA) makes an initial attempt to access the corporate network via the LANDesk DHCP server and requests an IP address.
2. The LANDesk DHCP server determines if this platform should be scanned, and its posture evaluated, by looking at Option 55 and Option 60. If the platform is to be scanned, the LANDesk DHCP server determines whether the health status of the device is known/cached, or if the device is included in the Exception List.
3. The LANDesk DHCP server returns a Quarantine VLAN IP address to the device (from the IP address pool). If the device is to be allowed, or if it is included in the Exception list, then the request is forwarded to the primary corporate DHCP server.

4. Because the trust agent is installed on the device, its browser can launch and be redirected to the Install page on the remediation server that should have already been published from the core server. This page has links that let you install agents and run the security scanner to scan for compliance and perform necessary remediation.
5. Run the security client (scanner) in order to scan for and remediate any existing vulnerabilities and other security risks defined in your compliance security policy. Successful remediation makes the device compliant or healthy so that it can proceed to the next steps in the LANDesk DHCP posture validation process.

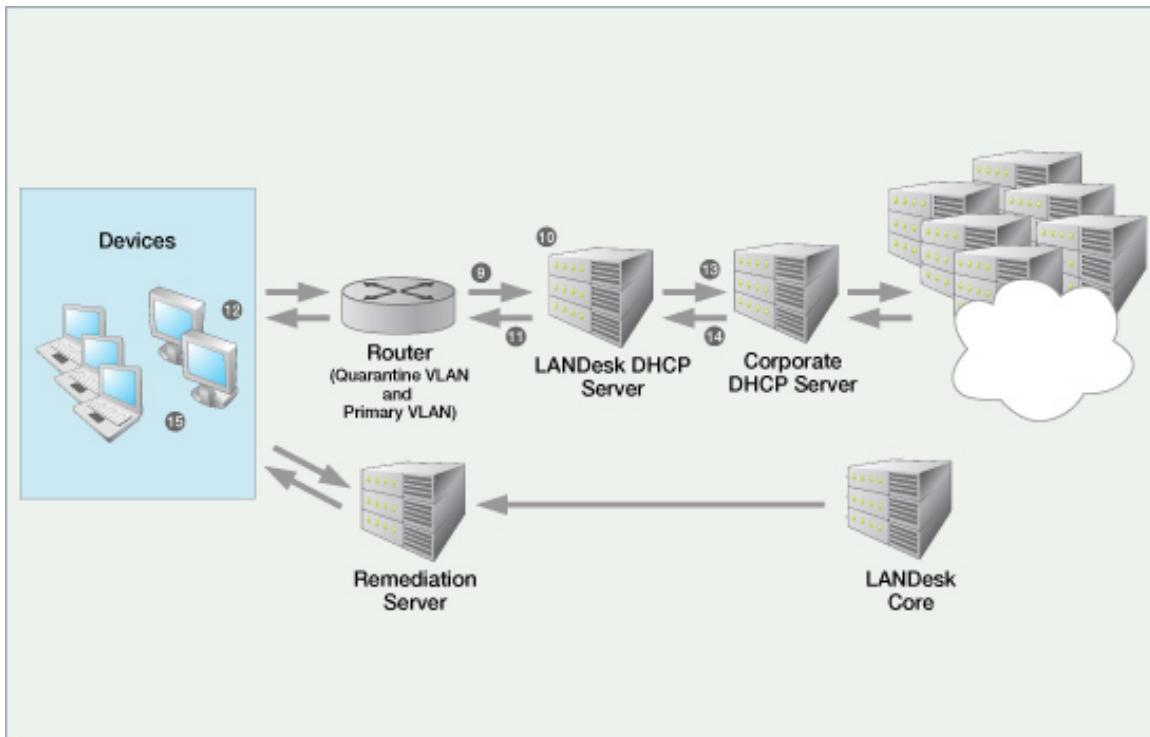
Phase 2: Remediated device access attempt (IP address reassigned; posture statement requested)



Process workflow for the second access attempt:

6. The remediated device attempts to access the network again via the LANDesk DHCP server and requests an IP address.
7. The LANDesk DHCP server considers the device to still be in a quarantined state, and...
8. The LANDesk DHCP server returns the same Quarantine VLAN IP address to the device.

Phase 3: Device posture validation (permanent IP address reassigned to healthy device; network access granted)



Process workflow for posture validation and network access:

9. The device sends its posture statement (health status) back to the LANDesk DHCP server.
10. The LANDesk DHCP server evaluates the device posture statement. (Note that it is the LANDesk DHCP server that acts as the decision point in the network access control process, meaning it determines the posture or health status of the device seeking network access.)
11. The LANDesk DHCP server communicates the posture reply to the device.
12. If the device is considered unhealthy (or non-compliant), it remains in the quarantine VLAN. If the device is considered healthy (or compliant), the device again requests an IP address from the LANDesk DHCP server.
13. Now, the LANDesk DHCP server recognized the device as being healthy and passes the IP address request on to the primary corporate DHCP server.
14. The primary corporate DHCP server notifies the LANDesk DHCP server about a permanent IP address being assigned to the healthy device, and...
15. The primary DHCP server returns the permanent IP address to the healthy device, and the device is granted access to the corporate network.

Network topology and design considerations for a LANDesk DHCP implementation

You should keep the following issues in mind when designing your LANDesk DHCP implementation:

- The LANDesk core server should not be visible to the quarantine network.
- The LANDesk DHCP server needs to be on the opposite side of the router/switch from the clients.
- The router needs to support a primary and secondary subnet for the client side of the router.
- The router needs to be configured to forward broadcasted BOOTP/DHCP requests to the LANDesk DHCP server (relay agent or IP helper).
- The primary DHCP server should be on the same side of the router as the LANDesk DHCP server.
- The LANDesk DHCP server can service many quarantined subnets, so potentially only one LANDesk DHCP server is required.
- Do not put the LANDesk DHCP server on the same machine as the primary DHCP server; they cannot share the same ports.
- The remediation server can be installed on the same machine as the LANDesk DHCP server machine, but if performance or scalability issues arise they can be installed on separate dedicated machines.
- The router must be configured with the real subnet as the primary subnet and the quarantined subnet as the secondary subnet.
- The secondary subnet should be restricted to only be able to see the remediation server.

Installing the LANDesk Trust Agent on devices to enable compliance scanning

In order to communicate with the LANDesk DHCP server, and to have its health posture evaluated, a device must have the LANDesk Trust Agent (LTA) installed.

The LANDesk Trust Agent (LTA) is used by both the LANDesk DHCP solution, and the LANDesk IP Security solution.

Note: Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.

To install the LANDesk Trust Agent on managed employee devices

- If they already have the standard LANDesk agent, install the LTA with a new device agent configuration
- Or, if they don't have the standard LANDesk agent, install the LTA with the initial agent configuration
- Or, install the LTA with an agent configuration to devices in UDD

To install the LANDesk Trust Agent on unmanaged employee devices

- Install the LTA by pulling with the standard LANDesk agent (wscfg32.exe)
- Or, by using a self-contained Agent Configuration

To install the LANDesk Trust Agent on new end user devices (employee or visitor)

- Install the LTA manually using a UNC or URL path (with the Visitor.html page located on the remediation Web share)

Setting up and configuring a remediation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC solutions.

For more information and step-by-step instructions, see "Setting up and configuring a remediation server" on page 396.

Setting up a LANDesk DHCP server

This is a unique procedure for the LANDesk DHCP solution. For detailed information including configuring your router/switch for a LANDesk DHCP solution, see "Setting up a LANDesk DHCP server" on page 400.

What you should do after setting up a LANDesk DHCP implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk NAC is to: define your compliance security policy, publish LANDesk NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. These tasks are generally the same and apply to the LANDesk DHCP, Cisco NAC, and LANDesk 802.1X solutions. For information on performing these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Additionally, to learn more about other ongoing LANDesk NAC management tasks such as: ensuring LANDesk NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing LANDesk NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Quickstart task list for setting up LANDesk DHCP

Use this task list to complete the planning, setup, and configuration tasks required to implement the LANDesk DHCP solution on your LANDesk network.

You can print out this task list and refer to it to keep track of each step during the implementation process. If you're viewing this task list online, you can click the **For more information** link to view detailed information and instructions about that particular task.

Setup a single LANDesk NAC server

For the purposes of this quickstart task list, the remediation server and the LANDesk DHCP server (which includes posture validation functionality) are both installed and configured on the same machine referred to here as the LANDesk NAC server. While this configuration is technically feasible and will create a functional LANDesk DHCP environment, keep in mind that it might not be the most suitable arrangement for your corporate network.

Quickstart task list for setting up a LANDesk DHCP implementation

Done	Task	For more information, go to
	<p>Prerequisite: A LANDesk Management Suite core server must be installed and running on your network, activated with a LANDesk Security Suite license and security content subscriptions:</p> <ul style="list-style-type: none"> • Install the core server • Activate the core with a Security Suite license • Log in as an Administrator user or as a user with both the Security and Patch Management and Security and Patch Compliance rights (allows downloading security and patch content and copying it to the Compliance group) 	<p>"Security and Patch Manager" on page 315</p> <p>For information on LANDesk DHCP components and process workflow (including diagrams), see "Understanding the LANDesk DHCP components and process" on page 381.</p> <p>For information on network topology and design considerations for a LANDesk DHCP implementation, see "Network topology and design considerations for a LANDesk DHCP implementation" on page 387.</p>
	<p>Install the LANDesk Trust Agent (LTA) on devices to enable compliance scanning:</p> <ul style="list-style-type: none"> • For managed employee devices: If they already have the standard LANDesk agent, install the LTA with a new device agent configuration 	<p>"Installing the LANDesk Trust Agent on devices to enable compliance scanning" on page 454</p>

Done	Task	For more information, go to
	<p>Or, if they don't have the standard LANDesk agent, install the LTA with the initial agent configuration Or, install the LTA with an agent configuration to devices in UDD</p> <ul style="list-style-type: none"> • For unmanaged employee devices: Install the LTA by pulling with the standard LANDesk agent (wscfg32.exe) Or, by using a self-contained Agent Configuration • For new end user devices (visitor): Install the LTA manually using a UNC or URL path (with the Visitor.html page located on the remediation Web share) 	
	<p>Identify and configure a single LANDesk NAC server that meets the following system requirements:</p> <ul style="list-style-type: none"> • Windows 2000 or above, with .NET Framework 1.1 • Web server installed and running (IIS) • Static IP address • The server must be on the opposite side of the router/switch from connecting devices • Can't be a current DHCP server • Can't be a PXE representative machine • Can't be the core server 	
	<p>Set up a remediation server:</p> <ul style="list-style-type: none"> • On the LANDesk NAC server, • Run the CONFIGURE.REMEDIATION.SERVER.VBS setup script located in: <coreserver>\LDMain\Install\TrustedAccess\RemediationServer • Note: This script automatically configures the server to perform remediation by: <ul style="list-style-type: none"> • creating a Web share named LDLogon (typically) at: c:\inetpub\wwwroot\LDLogon • enabling anonymous access to the LDLogon share with Read and Browse rights • adding a new MIME type for .lrd files, and setting it to application/octet-stream 	<p>"Setting up and configuring a remediation server" on page 396</p>

Done	Task	For more information, go to
	<p>Set up and configure a LANDesk DHCP server:</p> <ul style="list-style-type: none"> • On the LANDesk NAC server, • Run the LDDHCP.EXE setup program located in: <coreserver>\LDMain\Install\TrustedAccess\LDDHCP (copy the setup program to a disk if the core can't be accessed) • Copy keys and certificate files (*.key, *.crt) from the core server's Program Files\LANDesk\Shared Files\Keys folder to the same file path on the LANDesk DHCP server • Configure LANDesk DHCP server settings with the LDDHCP Configuration tool that can be accessed by the shortcut icon located on the desktop • Specify remediation server properties • Create VLAN address pool scopes for each subnet (make sure to define at least the scope option 003 for the router gateway) • (Optional) Configure OS filter options, exclusion lists, and the LANDesk DHCP Watcher • Exit the Configuration tool to start the LANDesk DHCP service • Note: The LANDesk DHCP solution does NOT require a dedicated posture validation server because this functionality is included in the LANDesk DHCP server 	<p>"Setting up a LANDesk DHCP server" on page 400</p>
	<p>Define compliance security criteria and enable LANDesk NAC with the Security and Patch Manager tool:</p> <ul style="list-style-type: none"> • In the console's Security and Patch Manager tool, • Download security content definitions and patches • Add security definitions to the Compliance group in order to define your compliance security policy • Make sure associated patches are downloaded and available for deployment • In Security and Patch Manager, open 	<p>"Defining compliance security criteria in the Security and Patch Manager tool" on page 433</p>

Done	Task	For more information, go to
	<p>the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Configure LANDesk DHCP/NAC, first make sure the Enable LANDesk NAC option is checked, and then define healthy and unhealthy postures</p>	
	<p>Configuring (adding) the single LANDesk NAC server in the console:</p> <ul style="list-style-type: none"> • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, and then click Configure LANDesk DHCP/NAC • Enter the LANDesk NAC server name in the LANDesk DHCP or posture validation server name field, click Add to add it to the list, and then click OK • Again, in Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Configure remediation servers, and then click Add • Enter the remediation server IP address, the UNC path to the LDLogon Web share, and user access credentials, and then click OK 	<p>"Setting up a LANDesk DHCP server" on page 400, and "Setting up and configuring a remediation server" on page 396</p>
	<p>Publish LANDesk NAC settings to appropriate servers:</p> <ul style="list-style-type: none"> • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Publish LANDesk NAC settings, select All, and then click OK • Note: The initial publishing process must include ALL of the LANDesk NAC settings; subsequent publishing can include compliance content only 	<p>"Publishing LANDesk NAC settings" on page 437</p>
	<p>Configure your network router for LANDesk DHCP:</p> <ul style="list-style-type: none"> • The network router must be located 	<p>"LANDesk DHCP server prerequisites" on page 401</p>

Done	Task	For more information, go to
	<p>between the LANDesk DHCP server and connecting devices</p> <ul style="list-style-type: none"> • The router must have DHCP forwarding turned on • Add a VLAN subnet to the client interface on the router (the quarantine subnet) • Change the IP address helper (relay agent) on the client interface to point to the LANDesk DHCP server • Add ACL (access control list) rules on the router to restrict traffic from the VLAN so that devices can only reach the remediation server. For example, an access control list might include the following access-list: <pre>101 permit ip 10.1.1.0 0.0.0.255 any access-list 101 permit ip any host 192.168.1.10 access-list 101 permit udp any eq bootpc any eq bootps</pre> <p>(Where 10.1.1.0 is the primary subnet gateway; and 192.168.1.10 is the LANDesk DHCP/remediation server.)</p>	
	<p>Ensure the posture validation process is working properly:</p> <ul style="list-style-type: none"> • Try a simple test of LANDesk DHCP by releasing and renewing a managed device's IP address 	
	<p>Perform ongoing compliance security management tasks:</p> <ul style="list-style-type: none"> • Ensuring LANDesk NAC is enabled • Using the allow/restrict access to everyone option • Understanding what happens when connecting devices are postured • Viewing affected (non-compliant) devices • Modifying and updating compliance security policies • Adding unmanaged devices • Configuring and viewing compliance logging • Generating compliance reports 	<p>"Managing LANDesk NAC compliance security" on page 445</p>

To return to the main help topic for the LANDesk DHCP, see [Using the LANDesk DHCP solution](#).

Setting up and configuring a remediation server

LANDesk Network Access Control (NAC) requires a remediation server to repair vulnerable or infected devices. The remediation server is where a device whose posture is determined to be unhealthy is sent to be remediated (repaired) so that it can meet the compliance rules you've configured for a healthy status.

The remediation server is where you publish remediation resources, such as: the security clients that scan for vulnerabilities and other security risks on devices, patch files, and the HTML pages that appear on devices providing options for remediation or limited network access.

To understand how the remediation server interacts with the other LANDesk NAC components and connecting devices, see the relevant component and process diagrams in "Using the LANDesk DHCP solution" on page 379, and "Using the Cisco NAC solution" on page 413.

Read this chapter to learn about:

Setting up and configuring a remediation server

- "Remediation server prerequisites" on page 396
- "Determining server location on the network" on page 429
- "Creating and configuring a Web share on the remediation server" on page 397
- "Configuring (adding) a remediation server in the console" on page 398
- "Next steps: Publishing remediation infrastructure files to remediation servers" on page 431

Remediation server prerequisites

The machine you want to set up as a remediation server must meet the following system requirements:

- The remediation server can be any type of Web server. For example: IIS on Windows, or Apache on Linux.
- You must create a Web share on the remediation server that has anonymous access with read and browse rights enabled. For detailed instructions, see "Creating and configuring a Web share on the remediation server" on page 397.

Note: If you're using an Apache Web server on Linux, the share you create must be a Samba share.

Determining server location on the network

You should comply with the following guidelines when deciding the location of the remediation server on your network.

- The remediation server can be placed on either side of the router.

- If you choose to have it on the client side of the router, then it will be more secure because you don't have to make any exceptions in your router rules, but you will have to manually walk all the remediation files to the machine each time you change them.
- If you put it on the opposite side of the router, then you have a potential security risk since quarantine machines are accessing a machine on your network, but you can push remediation files to the machine without having to walk them there.
- The remediation server must be visible from the remediation VLAN.
- You can have more than one remediation server on your network.

You can see diagrams showing component location and process workflow for each LANDesk NAC solution in their respective overview sections. See, "Using the LANDesk DHCP solution" on page 379, and "Using the Cisco NAC solution" on page 413.

Creating and configuring a Web share on the remediation server

This procedure has been automated for you with a script located on the core server that you run from the machine you want to set up as a remediation server.

The Web share that is created on the remediation server acts as a storage area for the patch executable files that are used to remediate vulnerabilities on affected devices. When you publish Infrastructure files or remediation resources (i.e., security client, patch files, and HTML files from the core server), those files are copied to this Web share.

Note: The name of the Web share must be LDLogon. You can create this share anywhere on the Web server. A typical path would be: C:\inetpub\wwwroot\LDLogon. However, you can create the share at any path as long as the URL redirect is configured to go to: <http://servername/LDLogon>.

After running the script to create and configure the Web share, you must then add the remediation server in the console and specify the path to the share (for detailed instructions, see "Configuring (adding) a remediation server in the console" on page 398). This ensures the core server publishes remediation resources to the correct location on the remediation server.

To run the remediation server configuration script

1. From the machine you want to set up as the remediation server, map a drive to your core server's LDMain\Install\TrustedAccess\RemediationServer folder.
2. Double-click the CONFIGURE.REMEDIATION.SERVER.VBS setup script.

The remediation server configuration script automatically configures the server to perform remediation by:

- Creating a Web share named LDLogon (typically) at: c:\inetpub\wwwroot\LDLogon .
- Enabling anonymous access to the LDLogon share with Read, Write, and Browse rights.
- Adding a new MIME type for .Ird files, and setting it to application/octet-stream (application/binary).

Note: You can also use the Microsoft IIS tool to manually configure the LDLogon share's access permissions and MIME types.

The remediation server is now ready to be added in the console.

Configuring (adding) a remediation server in the console

Once a remediation server is set up, you must configure and add it to the list of valid remediation servers in the **Configure remediation servers** dialog in the console. By doing this, the remediation server is recognized on the network and can communicate properly with the other LANDesk NAC components.

To configure and add remediation servers in the console

1. From the Security and Patch Manager tool in the console (**Tools | Security | Security and Patch Manager**), right-click the **Network Access Control** group, click **Configure remediation servers**, and then click **Add**. The **Remediation server name and credentials** dialog displays.
2. Enter the IP address of the remediation server.
3. Enter the path to the Web share (on the Web server you're setting up as a remediation server) where you want to publish compliance files. The Web share must be named LDLogon. Compliance files are the security definition files that define your compliance security policy (i.e., the contents of the **Compliance** group in Security and Patch Manager, as well as the required patch files that remediate detected vulnerabilities).

You can enter a UNC path or a mapped drive path. A UNC path is the most reliable method because drive mappings may change (see note below). You can click the Browse button to navigate to the share you want to publish compliance files to on the remediation server.

Important: If you enter a local path or a mapped drive in the Location to copy compliance files field, the files are published either to the local machine or to the specified mapped drive on the machine where the publish action is initiated. To ensure that compliance files are published to the same location on each remediation server on the network, we recommend using a UNC path to a network share.

4. Enter a valid user name and password to access the remediation server.
5. Click **OK** to add this remediation server to the list.

You can now publish remediation infrastructure files to the server (as long as you've also configured a posture validation server and user credentials).

About the Remediation server name and credentials dialog

Use this dialog to identify the remediation server and the path to Web share on the remediation server where remediation resources (security clients, patch files, and HTML pages are published).

- **Remediation server name:** Identifies the remediation server by its IP address or hostname.

- **Location to copy compliance files:** Specifies the full path to the Web share located on the remediation server where compliance files are published from the core. The name of the Web share should be LDLogon. The path can be either a UNC path or mapped drive path (or local path). A UNC path is recommended (see the **Important** note above).
- **Browse:** Opens the local Windows Explorer window where you can navigate to the remediation server's LDLogon share.
- **User name:** Identifies a valid user with access credentials to the Web share on the remediation server.
- **Password:** Identifies the user password.
- **Confirm password:** Verifies the user password.
- **OK:** Saves the remediation server settings and adds it to the list in the Configure remediation servers dialog.
- **Cancel:** Closes the dialog without saving the settings and without adding it to the list of remediation server.

Next steps: Publishing remediation infrastructure files to remediation servers

The next step in setting up and configuring a remediation server is to publish to the remediation server vital remediation infrastructure resources from the core server. These remediation infrastructure resources include:

- Security client (vulnerability scanner utility)
- Patches associated with the vulnerabilities contained in the Compliance group
- HTML pages that provide links that allow end users to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other security exposures.

You must first define your compliance security criteria in the Security and Patch Manager tool before you can publish to servers.

For information about these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Setting up a LANDesk DHCP server

A LANDesk DHCP server is required for the LANDesk DHCP implementation of LANDesk Network Access Control (NAC); but is not required in a Cisco-based NAC implementation.

Also, unlike the Cisco NAC solution, The LANDesk DHCP solution does not require a dedicated posture validation server because this functionality is included in the LANDesk DHCP server. In other words, the posture validation service that evaluates device health is built in to the LANDesk DHCP server.

The LANDesk DHCP server provides a temporary IP address (a quarantine IP address) to requesting devices. With a temporary IP address, the device can communicate with the remediation server, which runs the security client (a special version of the security scanner, also known as the vulnerability scanner). The security scanner checks for security definitions contained in the Compliance group, and if the vulnerability is detected, the remediation server will perform remediation by deploying the necessary patch files, or removing detected spyware, etc. Then, after remediation, the device requests an IP address again from the LANDesk DHCP server. If the device is healthy according to the compliance rules, the LANDesk DHCP server forwards the device to the primary corporate DHCP server to be assigned a valid network IP address.

Important: Technical knowledge and expertise required for setting up LANDesk NAC

Note that LANDesk NAC requires additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with either Cisco Network Access Control (NAC) and Cisco Secure Access Control Server (ACS) configuration and operation, and/or DHCP server management and DHCP protocols, as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

Setting up a LANDesk DHCP server

- "LANDesk DHCP server prerequisites" on page 401
- "Determining the server location on the network" on page 401
- "Installing the LANDesk DHCP server software" on page 402
- "Copying LANDesk certificate files to the LANDesk DHCP server" on page 402
- "Configuring the LANDesk DHCP server with the LANDesk DHCP Manager tool" on page 403
- "Configuring DHCP server settings" on page 403
- "Creating and managing scopes" on page 404
- "Configuring (adding) LANDesk DHCP servers in the console" on page 406
- "Configuring remediation server properties" on page 407
- "Using OS filters" on page 409
- "Adding devices to the posture exclusion list" on page 410
- "Configuring the LANDesk DHCP Watcher" on page 410
- "Restarting the LANDesk DHCP server" on page 412

LANDesk DHCP server prerequisites

You must make sure your network and router configuration meet the following conditions in order for the LANDesk DHCP solution to work properly:

Network and router configuration requirements

- The LANDesk core server should not be visible to the quarantine network
- The router must be located between the LANDesk DHCP server and connecting devices
- The router must have DHCP forwarding turned on
- Add a VLAN subnet to the client interface on your router
Change the IP address helper (relay agent) on the client interface to point to the LANDesk DHCP server instead of the primary DHCP server
- Add ACL rules on the router to restrict traffic from the VLAN so that devices can only reach the remediation server and subnet representatives. For example, an access control list might include the following:

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 any
access-list 101 permit ip any host 192.168.1.10
access-list 101 permit udp any eq bootpc any eq bootps
```

(Where 10.1.1.0 is the primary subnet gateway; and 192.168.1.10 is the LANDesk DHCP/remediation server.)

You should also make sure the server machine you want to set up as your LANDesk DHCP server meets the following requirements:

Special considerations and requirements for the LANDesk DHCP server

- Must be Windows 2000 or above, with .NET Framework 1.1
- Must be on the opposite side of the router from connecting devices
- Must have a static IP address (configured via Windows network configuration)
- Can't be a current DHCP server
- Can't be a PXE representative machine
- Can't be installed on the core server

Determining the server location on the network

As stated above, the LANDesk DHCP server must be on the opposite side of the router from the connecting devices, and on the same side of the router as the primary DHCP server.

You can see diagrams showing component location and process workflow for each LANDesk solution in their respective overview sections. See, "Using the LANDesk DHCP solution" on page 379, and "Using the Cisco NAC solution" on page 413.

Installing the LANDesk DHCP server software

To install and set up a LANDesk DHCP server

1. From the machine you want to set up as the LANDesk DHCP server, map a drive to your core server's LDMain\Install\TrustedAccess\LDDHCP folder.
2. Launch the LDDHCP.EXE install program.
3. Select the language version you want to install, and then click **OK**.
4. At the Welcome screen, click **Next**.
5. Accept the license agreement, and then click **Next**.
6. To copy the necessary files, click **Install**.
7. When the file copy process is complete, click **Finish**.

The LANDesk DHCP server is NOT running yet. You must first:

- Copy certificate files
- Configure the LANDesk DHCP server with the LANDesk DHCP Manager tool
- Start the DHCP service

Copying LANDesk certificate files to the LANDesk DHCP server

In order for the LANDesk DHCP Server to communicate with managed devices, you must copy your LANDesk certificate files to the LANDesk DHCP Server machine.

To copy the LANDesk certificate files,

1. From the LANDesk DHCP server machine, map a network drive to access the core server's administrative share. Use the following command syntax:
\\computername\c\$
(**Note:** You'll need administrator equivalent credentials in order to access this share on the core server.)
2. Copy the *.CRT and *.KEY files from the core server's C:\Program Files\LANDesk\Shared Files\keys folder to the same folder on the LANDesk DHCP server (this folder is automatically created by the installation program).

Configuring the LANDesk DHCP server with the LANDesk DHCP Manager tool

You've successfully installed the LANDesk DHCP server software. However, the LANDesk DHCP service is NOT yet running. The next step in setting up the LANDesk DHCP server and starting the service is to run the LANDesk DHCP Manager tool that has been installed on this machine by the setup program in order to configure DHCP server settings, configure posture validation server settings, create and manage scopes, and to add devices to the posture exclusion list.

Important note on opening firewall ports

Before you proceed in setting up the LANDesk DHCP server, you should disable the Windows Firewall if it is enabled. If you want to leave the Windows Firewall enabled, you must ensure the following UDP ports are completely open: 67, 68, 12576, and 12577.

The name of the LANDesk DHCP server configuration tool is LANDesk DHCP Manager. This tool can be launched either from the Start menu (**Start | Programs | LANDesk | LANDesk DHCP Server | LDDHCP Configuration**), or by double-clicking the **LDDHCP Configuration** icon that should now appear on the server's desktop.

The LANDesk DHCP Manager tool lets you:

- Configure LANDesk DHCP server settings
- Create and manage scopes (name, lease time, address range, relay address, exclusion range, and scope options)
- Configuring (adding) LANDesk DHCP servers in the console
- Configure remediation server properties
- View and modify OS filter options, and create new OS filters
- Add devices to the posture exclusion list
- View the health status of postured devices
- View the LANDesk DHCP server log file
- Configure the LANDesk DHCP watcher
- Stop and restart the LANDesk DHCP service

Configuring DHCP server settings

To configure LANDesk DHCP server settings

1. At the LANDesk DHCP server you've installed, click the LANDesk DHCP Configuration program icon located on the desktop. (Or you can click **Start | Programs | LANDesk | LANDesk DHCP Server | LDDHCP Configuration**)
2. Right-click the **LANDesk DHCP server** object, and then click **Properties**. The **Configure LANDesk DHCP settings** dialog displays.
3. Enter the IP address of the LANDesk DHCP server. This field defaults to the IP address of the primary NIC in the server.
4. Enter the IP address of the primary DHCP server on your network.
5. Specify the frequency of the address pool backup (in minutes). This setting controls how often the LANDesk DHCP server saves IP address pool information. This information is saved in an XML file on the DHCP server.

6. Click **OK** to save your settings and exit the Configure LANDesk DHCP settings dialog.

About the Configure LANDesk DHCP settings dialog

Use this dialog to configure the basic LANDesk DHCP server settings:

- **LANDesk DHCP server:** Identifies the IP address of the LANDesk DHCP server you're configuring. This field defaults to the IP address of the primary NIC in the server.
- **Primary DHCP server:** Identifies the IP address of the primary corporate DHCP server on your network. The LANDesk DHCP server communicates with the primary DHCP server in order to assign a permanent IP address to healthy connecting devices during the posture validation process.
- **Frequency of address pool backup (minutes):** Specifies how often the LANDesk DHCP server saves IP address pool information. This information is saved in an XML file on the DHCP server.

Creating and managing scopes

In order for the LANDesk DHCP server to lease temporary (or quarantine) IP addresses to connecting devices, you must first create and activate scopes. A scope is a range of possible IP addresses for a network or subnet.

Guidelines for creating scopes on your LANDesk DHCP server

- You should create a scope for each subnet (router) on your network
- **Important:** LANDesk DHCP supports only one scope per subnet
- Each scope should be configured with two gateways: one for a primary subnet and one for a quarantine subnet
- No two routers can have the same quarantine subnet IP range
- After you create a scope, you must configure the scope options (**Important:** option 001 and 003 are required)
- We recommend that you don't rename scopes after you've created them with the LANDesk DHCP manager tool.

To create and configure scopes

1. In the LANDesk DHCP Manager tool, right-click the **LANDesk DHCP server** object, and then click **New scope**. The **Scope properties** dialog displays. Or, to edit an existing scope, right-click the **scope** object in the LANDesk DHCP server tree, and then click **Properties**.
2. On the **Name** tab, enter a name and description for this scope. Each scope must have a unique name.
3. On the **Lease time** tab, enter a duration for IP addresses assigned to connecting devices by the LANDesk DHCP server. The duration should be equivalent to the amount of time a device is connected to the network.

4. On the **Address range** tab, enter a range of IP addresses (starting and ending IP addresses) that this scope can distribute to connecting devices. Make sure the range you specify provides enough IP addresses for the devices on your network.
(**Note:** You can't enter IP addresses that are part of the same subnet as the primary DHCP server's range.)
5. Also on the **Address range** tab, enter a subnet mask. You can enter either an IP address or a length. The subnet mask determines how many bits of an IP address to use for the network/subnet IDs, and how many bits of an IP address to use for the host IP.
6. Click **Finish**.

Now you can configure the scope's options.

To configure scope options

1. Right-click the **Scope options** object under the scope you want to configure, and then click **Properties**.
2. You must configure at least the following scope option in order for the scope to work properly: Option 003 (router gateway)
3. To configure an option, select it in the **Available options** list, fill in the required fields in the **Data entry** section below, check the option's checkbox to enable it, and then click **OK**.

About the Scope properties dialog

Use this dialog to create, configure, and modify scopes on the LANDesk DHCP server.

The **Scope properties** dialog includes the following tabs:

About the Name tab

- **Name:** Identifies the scope (range) of IP addresses for lease on the DHCP server by a unique descriptive name.
- **Description:** Helps you remember the purpose of this scope.

About the Lease time tab

- **Lease time limited to:** Specifies the duration for IP addresses assigned to connecting devices by the LANDesk DHCP server. The duration should be equivalent to the amount of time a device is connected to the network.

About the Address range tab

- **Start IP address:** Identifies the first possible IP address in this scope's address range.
- **End IP address:** Identifies the last possible IP address in this scope's address range. Make sure the range you specify provides enough IP addresses for the devices on your network.
- **Subnet mask:** Identifies the subnet to which an IP address belongs.

About the Subnet (Address pool properties dialog)

Use this dialog to modify a scope's IP address range or pool. You can access this dialog by right-clicking the **Address pool** object under the scope you want to modify, and then click **Properties**.

- **Start IP address:** Identifies the first possible IP address in this scope's address range.
- **End IP address:** Identifies the last possible IP address in this scope's address range. Make sure the range you specify provides enough IP addresses for the devices on your network.
- **Subnet mask:** Identifies the subnet to which an IP address belongs.

About the Exclusion range dialog

Use this dialog to configure and exclusion range. An exclusion range is a group of IP addresses that the DHCP server will not lease to devices. When creating a scope, you should determine whether any devices on your network, such as DNS servers, will need to use static IP addresses. If you have devices that need a static IP address, create an exclusion range so that you can assign all statically configured devices an IP address from the exclusion range.

To create a single IP address to exclude from the scope's lease pool, enter a starting IP address and leave the ending IP address field empty.

- **Start IP address:** Identifies the first possible IP address in this exclusion range.
- **End IP address:** Identifies the last possible IP address in this exclusion range.

About the Configure scope options dialog

Use this dialog to configure various scope options. Do not activate a scope until you specify the options you want. Scope options are inherited as default values for all devices in the applicable scope.

- **Available options:** Lists the scope options you can configure. Select the option you want to configure to display the data fields below.
- **Description:** Indicates the function of the selected scope option.
- **Data entry:** Specifies the information that must be filled in when configuring a scope option. This area displays when you select an option from the list of available scope options above. Fill in the fields, and then click **OK**.

Configuring (adding) LANDesk DHCP servers in the console

Once a LANDesk DHCP server is set up, you must add it to the list of valid LANDesk DHCP servers in the Configure LANDesk NAC dialog in the console. This allows the core server to communicate with (publish) compliance rules to the LANDesk DHCP server.

To add LANDesk DHCP servers in the console

1. In the Security and Patch Manager tool window, right-click the **Network Access Control** group, and then click **Configure LANDesk NAC**.
2. To add posture validation server(s) to your network, enter the IP address of a posture validation server in the field provided, and then click **Add**.
3. Click **OK**.

You can now publish LANDesk NAC content to the servers (as long as you've also configured a remediation server and user credentials).

Configuring remediation server properties

Once you've configured the basic settings for the LANDesk DHCP server, you can configure the remediation server properties and create scopes with the LANDesk DHCP Manager tool.

To configure the remediation server properties

1. In the LANDesk DHCP Manager tool, right-click the **Remediation server** object, and then click **Properties**. The **Remediation server properties** dialog displays.
2. Enter the IP address of the remediation server. (**Note:** You should have only one remediation server per LANDesk DHCP server.)
3. Enter the URL to the healthy status page. The name of this HTML file is: Healthy.html. This page informs the end user of a connecting device that their device has been scanned, passed the compliance security criteria, is considered healthy, and will be granted full access to the corporate network.

Note: For all of the HTML pages, enter the full path to the HTML file, including the http:// protocol identifier. HTML pages should have already been published from the core server to the remediation server, so typically the full path would be:
http://remediation_server_name/LDLogon/Healthy.html.

4. Enter the URL to the first time visitor status page. The name of this HTML file is: Visitor.html.
This page informs a visitor to your corporate network that you have implemented compliance or LANDesk NAC security on your network and that they can choose to either browse the Web (Internet access only) or have their computer scanned for vulnerabilities or other security risks, and remediated if necessary, before being allowed access to the corporate network. Links are provided on this HTML page that allow Internet access only or that allow the visitor to download and install the necessary software for compliance scanning and remediation so that their device can be have full access to the network.
5. Enter the URL to the unhealthy employee status page. The name of this HTML file is: FailedEmployee.html.
This page informs the end user of the connecting device that their device has been scanned and does not meet one or more of the compliance security credentials, is considered unhealthy, and has been denied access to the network. The network administrator should customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the end user must log into the network again to be allowed access.

6. Enter the URL to the unhealthy visitor status page. The name of this HTML file is: FailedVisitor.html.
This page informs a visitor to your corporate network that their device has been scanned and does not meet one or more of the compliance security credentials, and has been denied access to the network. As with the unhealthy employee status page, network administrators can customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the visitor should click the **Security scan for network access** icon that now appears on their desktop.
7. Click **OK** to save your settings and exit the **Posture validation server** dialog.

The HTML pages are merely templates and can be edited and customized to suit your specific LANDesk NAC security needs and requirements.

About the Remediation server properties dialog

Use this dialog to configure the remediation server so that it can communicate with the LANDesk DHCP server, and so that the LANDesk DHCP server knows where the HTML pages are hosted on the remediation Web share so that they can be served to connecting devices.

- **IP address:** Identifies the IP address of the remediation server. (**Note:** You should have only one remediation server per LANDesk DHCP server.)
- **Healthy URL:** Specifies the full path to the Healthy HTML page. This page informs the end user of a connecting device that their device has been scanned, passed the compliance security criteria, is considered healthy, and will be granted full access to the corporate network.
- **First time visitor's URL:** This page informs a visitor to your corporate network that you have implemented compliance or LANDesk NAC security on your network and that they can choose to either browse the Web (Internet access only) or have their computer scanned for vulnerabilities or other security risks, and remediated if necessary, before being allowed access to the corporate network. Links are provided on this HTML page that allow Internet access only or that allow the visitor to download and install the necessary software for compliance scanning and remediation so that their device can have full access to the network.
- **Employee's failed to connect URL:** This page informs the end user of the connecting device that their device has been scanned and does not meet one or more of the compliance security credentials, is considered unhealthy, and has been denied access to the network. The network administrator should customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the end user must log into the network again to be allowed access.
- **Visitor's failed to connect URL:** This page informs a visitor to your corporate network that their device has been scanned and does not meet one or more of the compliance security credentials, and has been denied access to the network. As with the unhealthy employee status page, network administrators can customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the visitor should click the **Security scan for network access** icon that now appears on their desktop.

Using OS filters

Operating system filters provide a way for you to easily control whether a device is automatically allowed or denied access to your network or whether it must first be scanned to see if it meets your compliance security criteria. You can configure this setting at the platform level in order to simplify LANDesk NAC security on your network.

The LANDesk DHCP server includes several predefined OS filters for various supported platforms. You can't delete the predefined filters. However, you can individually configure each filter's LANDesk NAC control functionality.

To view and modify predefined OS filter options

1. In the **LANDesk DHCP Manager** tool, click the **OS Filter Options** object. A list of predefined OS filters displays. (Each OS filter has a default Access Type setting that determines whether that platform is scanned, denied, or allowed on to the network.)
2. To modify a filter's access control, click its **Access Type** drop-down list and select one of the options. The options are: **Allow** (that always automatically grants network access and assigns a corporate IP address), **Deny** (that always automatically denies network access and assigns a quarantine IP address), and **Scan** (that always runs a compliance security scan to check for vulnerabilities and other security risks in order to determine the posture or health of the device and present the appropriate HTML page to the connecting device). You can change these settings at any time.

Note: If you set an OS filter to Scan but LANDesk doesn't have device agents for that operating system (e.g., Windows 95), those devices will be blocked from accessing the network.

You can also create your own operating system filters, if necessary.

To add new OS filters

1. In the **LANDesk DHCP Manager** tool, right-click the **OS Filter Options** object, and then click **Add**.
2. Enter a unique name for the operating system filter you want to add.
3. Enter the hex code for that operating system. You can obtain a platform's hex code by running a packet sniffer utility on a machine with that OS and reading its hex identifier.
4. Click **OK** to create the filter.
5. To specify the filter's access control, click its **Access Type** drop-down list and select one of the options.

About the Add operating system filter dialog

Use this dialog to create network access filters for different operating systems that are not included in the list of predefined OS filters.

- **Name:** Identifies the name of the operating system you want to create an access filter for.
- **Hex identifier:** Identifies the hexadecimal code for that operating system. You can obtain a hex code by running a packet sniffer utility on a machine with the OS you want to filter.

Adding devices to the posture exclusion list

To add devices to the posture exclusion list

1. Right-click **MAC exclusions** object, and then click **Properties**.
2. Enter the MAC (machine address) of the device you want to bypass the posture validation process altogether, and then click **Add**.

You can enter as many device MAC addresses as you want.

About the MAC address exclusions dialog

Use this dialog to add devices that you want to bypass the posture validation process.

- **MAC address:** Indicates the machine address of the device you want to bypass the posturing process.
- **Add:** Adds the device to the list.
- **Remove:** Remove the device from the list.

Importing and exporting MAC address exclusions

To import address exclusions, right-click the **MAC Exclusions** object, click **Import**, and then browse to select the CSV file that contains the MAC addresses of devices you want to bypass the posture validation process.

To export address exclusions in your list, right-click the **MAC Exclusions** object, click **Export**, and then save the CSV file.

Viewing the health status of postured devices

You can quickly view the status of all scanned devices to see which devices are healthy and which are unhealthy according to your compliance security policy.

To view a complete list of scanned devices and their health status, click the **Client Health** object in the LANDesk DHCP server tree view.

Viewing the LANDesk DHCP server log file

To view the LANDesk DHCP server log file in the LANDesk DHCP Manager tool window, simply click the **LANDesk DHCP Server Log** object in the tree view.

Configuring the LANDesk DHCP Watcher

The LANDesk DHCP Watcher is a utility that regularly checks to make sure the LANDesk DHCP service is running on the server by sending a test packet, and can be used to notify you if the service stops running and can't be restarted.

To configure the LANDesk DHCP Watcher

1. In the LANDesk DHCP Manager tool, click the **LDDHCP Watcher** object. The current settings display in the right-hand frame.
2. To modify the settings, right-click **LDDHCP Watcher**, and then click **Properties**.
3. On the **Frequency** tab, specify how often to verify whether the DHCP service is running, the duration to wait for a response from the DHCP service, the number of times to try by resending a test packet to the service, and the port number where the test traffic is sent. The default port on the LANDesk DHCP Server is: 12579.
4. If you want to be notified when the DHCP service stops and can't be restarted, click the **Notification** tab, and then check the **Send email notification** checkbox. Enter email addresses where the notification message will be sent, and fill in the SMTP mail server information.
5. To make sure that notification is working properly, click **Send test email**.

About the Configure LANDesk DHCP Watcher dialog

Use this dialog to specify how often the LANDesk DHCP Watcher verifies whether the DHCP service is running on the server, and notification information if the service stops and can't be restarted.

This dialog includes the following two tabs:

About the Frequency tab

- **Interval to check (minutes):** Specifies how often the LANDesk DHCP Watcher checks whether the DHCP service is running.
- **How long to wait for a response (seconds):** Specifies the amount of time the LANDesk DHCP Watcher will wait to receive a response to its test packet from the DHCP service.
- **Number of times to retry:** Specifies how many times a test packet is sent before a notification is sent out. With each attempt that fails to elicit a response, the LANDesk DHCP Watcher tries to restart the DHCP service. If the last retry also fails, the LANDesk DHCP server switches to a pass-through mode that passes all DHCP requests to the primary corporate DHCP server.
- **Port to send test traffic on:** Identifies the port to which the LANDesk DHCP Watcher sends test packets. The default port number is: 12579.

About the Notification tab

- **Send email notification:** Indicates whether email notification is enabled.
- **Email addresses to notify:** Specifies the email address (or addresses) where the notification is sent. Multiple addresses must be separated by a semi-colon character.
- **SMTP server:** Identifies the SMTP mail server to which the notification should be sent.
- **SMTP port:** Identifies the SMTP port for mail messages.
- **Authentication required for SMTP server:** Indicates whether authentication is required in order to send a message to the specified SMTP server.
- **SMTP user name:** Identifies a valid SMTP server user name.
- **SMTP password:** Identifies the user's password.
- **Confirm SMTP password:** Verifies the user's password.

- **Send test email:** Attempts to send a notification to the email addresses specified above. Use this feature to make sure notification works properly.

Restarting the LANDesk DHCP server

Any time you change LANDesk DHCP server settings, or scope settings, you must restart the LANDesk DHCP server in order for your changes to take affect.

You can restart the LANDesk DHCP server from the **File** menu, or by right-clicking the LANDesk DHCP server object and clicking **Restart**.

Using the Cisco NAC solution

This section describes how to plan, set up, configure, and enable the Cisco NAC implementation of LANDesk Network Access Control.

With the Cisco NAC solution, you can take advantage of existing Cisco hardware, software, agents, protocols, and posture evaluation processes that might already be a part of your network infrastructure. For detailed information about the Cisco router, servers, and NAC technologies you should refer to your official Cisco documentation.

Audience disclaimer and assumptions

"The intended audience for setting up Cisco NAC consists of system engineers and network administrators responsible for the implementation of Cisco NAC. This document assumes you are familiar with Microsoft Windows operating systems and client machines and with the configuration and operation of Cisco Secure ACS. It also assumes you know how to configure Cisco IOS devices, and are familiar with certificate authorities and the trust models provided by digital certificates."

The note above is taken from the official Cisco document entitled "Implementing Network Admission Control Phase One Configuration and Deployment."

In addition to the specific Cisco components, you must also set up a posture validation server and a remediation server in order to implement LANDesk Network Access Control (NAC).

Read this chapter to learn about:

Setting up a Cisco NAC implementation of LANDesk Network Access Control

- "Quickstart task list for setting up LANDesk Cisco NAC" on page 414
- "Understanding the Cisco NAC components and process" on page 415
- "Network topology and design considerations for a Cisco NAC implementation" on page 421
- "Setting up a Cisco router" on page 421
- "Setting up a Cisco Secure Access Control Server (ACS)" on page 422
- "Installing the Cisco Trust Agent on devices to enable compliance scanning" on page 422
- "Setting up and configuring a posture validation server" on page 423
- "Configuring a connection between the posture validation server and the Cisco Secure ACS" on page 423
- "Setting up and configuring a remediation server" on page 423

What you should do after setting up a Cisco NAC implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk NAC is to: define your compliance security policy, publish LANDesk NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. These tasks are generally the same and apply to the LANDesk DHCP, Cisco NAC, and LANDesk 802.1X solutions. For information on performing these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Additionally, to learn more about other ongoing LANDesk NAC management tasks such as: ensuring LANDesk NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing LANDesk NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Quickstart task list for setting up LANDesk Cisco NAC

Use this task checklist to help keep track of the steps required to set up the Cisco NAC solution: "Quickstart task list for setting up LANDesk integrated Cisco NAC" on page 425.

Understanding the Cisco NAC components and process

This section describes the components that comprise a Cisco NAC solution. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when LANDesk NAC is enabled. Scenarios with and without a Cisco Trust Agent (CTA) installed on the device are covered in the diagrams and process workflows below.

The following components are required for the Cisco NAC-based LANDesk NAC service.

Required components

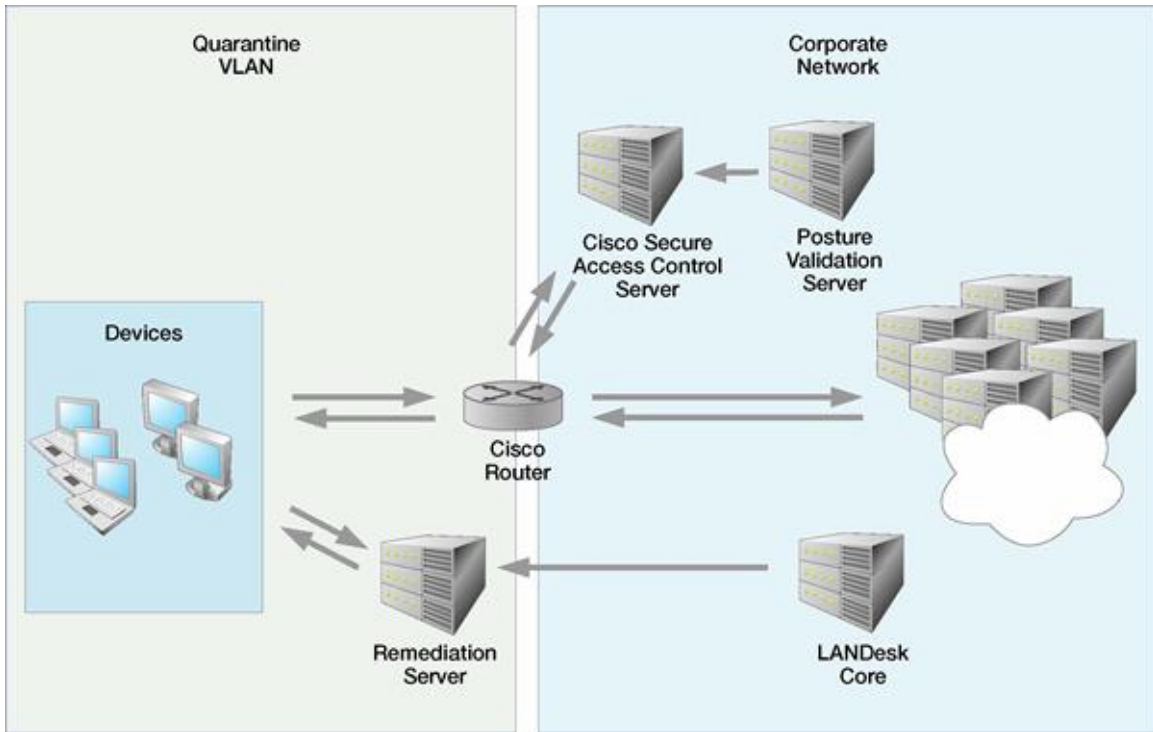
Component	Description
LANDesk core server	Provides the Security and Patch Manager tool used to: download security content (such as OS and application vulnerability definitions, spyware definitions, system configuration security threats, antivirus and firewall configuration definitions, etc.), define compliance criteria, configure posture validation servers and remediation servers, and configure and publish LANDesk NAC settings (including compliance security rules or policies and remediation resources for scanning and repairing devices).
Corporate DHCP server	Provides permanent IP addresses to devices.
Posture validation server	Determines whether the connecting device has a healthy or unhealthy posture based on two factors: your compliance security policy (the contents of the Compliance group in the Security and Patch Manager tool AND the number of hours since a healthy scan as specified in the Definition of healthy setting in the Configure LANDesk NAC dialog). The dedicated posture validation server is the policy decision point in the validation process. Note: Cisco NAC requires a dedicated posture validation server, but LANDesk DHCP does not.
Remediation server	Contains the necessary setup and support files (security client, security type definitions and required patches, as well as the HTML template pages used to scan devices for vulnerabilities) identified by your security policy and remediate (repair) any detected vulnerabilities so that the device can be scanned as healthy or compliant and access the network.
Cisco router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the Cisco

Component	Description
	Secure ACS to evaluate the posture credentials of the endpoint device. In other words, in a Cisco NAC environment the router is the policy enforcement point on the network and grants or denies access privileges.
Cisco Secure ACS	Cisco specific hardware device that acts as the primary posture validation server in a Cisco NAC environment. This server contains Access Control Lists (ACL) that define posture enforcement rules. The Cisco Secure ACS is configured to delegate posture decisions to the posture validation server (or servers) you set up and configure on the network.
Devices	Mobile or guest user devices, as well as regular network user devices, attempting to access your corporate network. Typical endpoint devices include desktop computers and laptops but may also be clientless devices such as printers, etc. LANDesk NAC allows you to evaluate the health status of these connecting devices and control network access based on their posture credentials.

The following diagrams show a typical configuration of the components described above, as well as the posture validation process or workflow between those components.

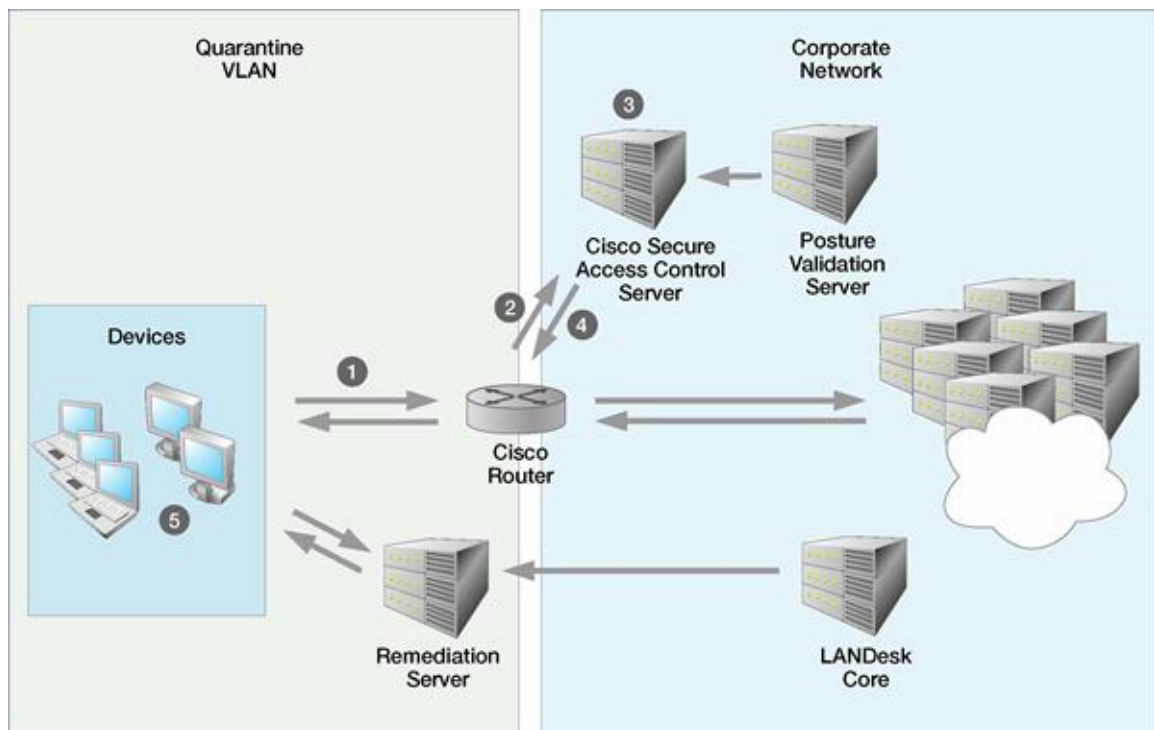
Cisco NAC components

The diagram below shows the specific Cisco NAC components.



Posture validation process for a device without the CTA installed

The diagram below shows the workflow or communication flow between the various components in a Cisco NAC environment when the device attempting to access the network does not have the Cisco Trust Agent installed. The callout numbers represent each stage of the process and are explained in the steplist below.



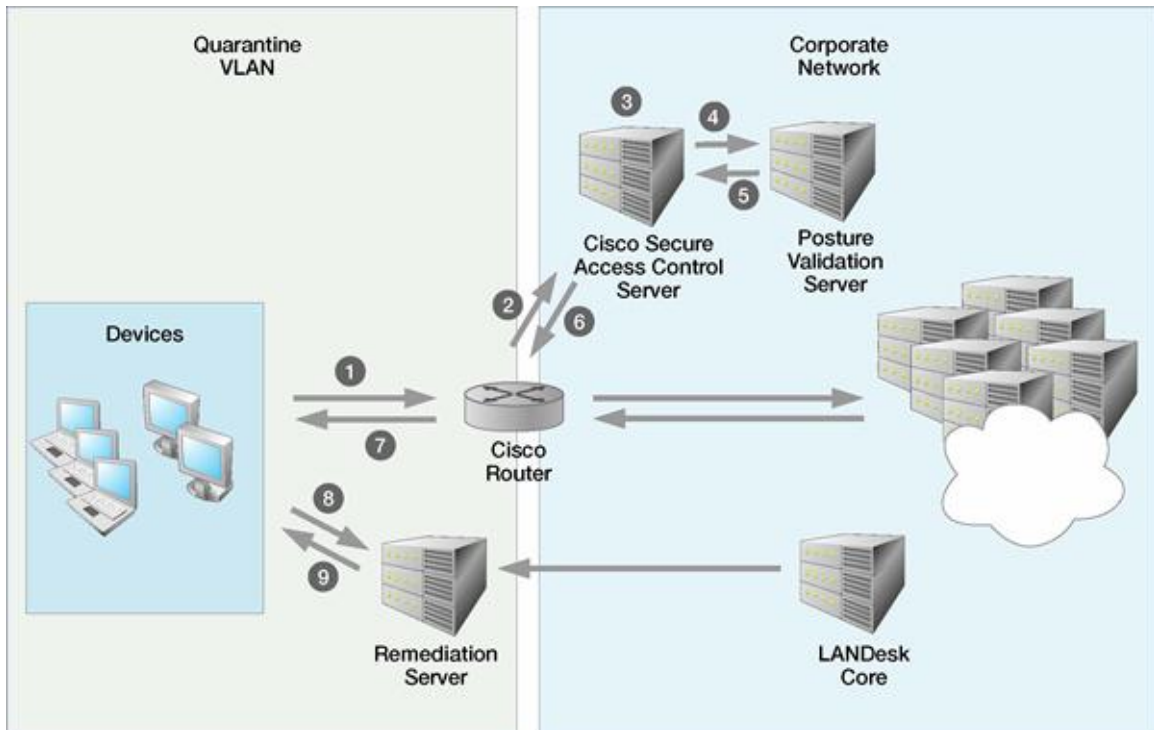
Process workflow:

1. A device that is NOT configured with the Cisco Trust Agent (CTA) makes an initial attempt to log in to the corporate network via the Cisco router.
2. The router forwards the device access request to the Cisco Secure Access Control Server (ACS) containing Access Control Lists (ACLs) defined by the administrator that determine access rights for each posture or health status.
3. Because the trust agent (CTA) isn't installed on the device, the Cisco ACS can't determine its posture or health status and doesn't forward the device access request to the posture validation server.
4. The Cisco ACS automatically rejects the "clientless" access attempt, and forwards the appropriate ACL on to the router.

5. According to the ACL (as defined by the administrator), a device in this situation is typically restricted to the quarantine VLAN and has no access to the corporate network at this point. The user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the network's security policy and gain full network access. In order to gain network access, first the CTA must be manually installed (via a UNC path or URL) to the CTA setup program, and then the device must access the remediation server in order to install the LANDesk Security Client that performs vulnerability assessment scanning and remediation. Once the device is repaired, the network access process is repeated and the healthy (i.e., compliant device is granted access to the corporate network).

Posture validation process for a device with the CTA installed

The diagram below shows the workflow or communication flow between the various components in a Cisco NAC environment when the device attempting to access the network has the Cisco Trust Agent installed. The callout numbers represent each stage of the process and are explained below.



Process workflow:

1. A device that is configured with the Cisco Trust Agent (CTA) makes an initial attempt to log in to the corporate network via the Cisco router.
2. The router forwards the device access request to the Cisco Secure Access Control Server (ACS) containing Access Control Lists (ACLs) defined by the administrator that determine access rights for each posture or health status.
3. Because the trust agent is installed on the device (and a connection between the posture validation server and the Cisco ACS has been configured), the Cisco ACS can forward the device access request to the posture validation server.
4. The posture validation server determines the health status or "posture" of the device against a security policy comprised of compliance rules or credentials predefined by the LANDesk administrator with the Compliance feature of the Security and Patch Manager tool. These compliance rules are published from the core server to the posture validation server. (Note that it is the posture validation server that acts as the decision point in the network access control process, meaning it determines the posture or health status of the device seeking network access.)

5. The posture validation server sends a posture statement (or token) for that particular device back to the Cisco ACS.
6. The Cisco ACS forwards the appropriate ACL (depending on the posture statement on to the router).
7. The posture statement is communicated back to the trust agent on the device in the quarantine area. If the device is considered healthy (or compliant), it is granted access to the corporate network.
8. However, if the device is considered unhealthy (or non-compliant) it remains in the quarantine VLAN. A message box displays informing the user how to contact the remediation server in order to install the LANDesk Security Client that performs vulnerability assessment scanning and remediation. The user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the network's security policy and gain full network access.
9. Remediation is performed by the remediation server by scanning for vulnerabilities and other security risks (the compliance rules mentioned above) and installing any required patches. Once the device is repaired, the network access process is repeated and the healthy (i.e., compliant device is granted access to the corporate network).

Network topology and design considerations for a Cisco NAC implementation

You should keep the following issues in mind when designing your Cisco NAC implementation:

- The LANDesk core server should not be visible to the quarantine network.
- The remediation server and posture validation server (and the Cisco ACS for that matter) can be installed on the same machine, but if performance or scalability issues arise they can be moved to their own server machines.
- The router needs to support a primary and secondary subnet for the client side of the router.
- The router must be configured with the real subnet as the primary subnet and the quarantined subnet as the secondary subnet.
- The secondary subnet should be restricted to only be able to see the remediation server.

Setting up a Cisco router

The Cisco NAC solution assumes a Cisco router on your network.

If you don't already have a Cisco router set up on your network and you want to use the Cisco NAC solution, LANDesk does offer some router setup information on its support Web site.

For detailed Cisco router setup information

You can view detailed setup instructions for a typical Cisco router to be used in a Cisco NAC environment on the LANDesk Software Support Website.

We also strongly recommend that you refer to your Cisco router documentation for more detailed instructions on setting up the router.

Setting up a Cisco Secure Access Control Server (ACS)

The Cisco NAC solution also assumes a Cisco Secure Access Control Server (ACS) on your network. The Cisco ACS is where you define posture credentials and configure external databases (such as a posture validation server) to communicate and resolve device posture status during the posture validation process.

If you don't already have a Cisco Secure ACS set up on your network and you want to use the Cisco NAC solution, LANDesk does offer some Cisco Secure ACS setup information on its support Web site.

For detailed Cisco Secure Access Control Server (ACS) setup information

You can view detailed setup instructions for a Cisco Secure ACS router to be used in a Cisco NAC environment on the LANDesk Software Support Website.

We also strongly recommend that you refer to your Cisco router documentation for more detailed instructions on setting up the router.

Installing the Cisco Trust Agent on devices to enable compliance scanning

In order to communicate with the Cisco Secure ACS and have its health posture evaluated, a device must have the Cisco Trust Agent (CTA) installed.

Manually installing the Cisco Trust Agent (CTA)

For Cisco NAC, the trust agent (CTA) must be installed manually, on both managed and unmanaged devices, from the core server using a UNC or URL path. You can use the `UnhealthyCisco.html` file located on the remediation Web share to install the CTA.

Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.

Important note on installing the full standard LANDesk agent: You must have the full standard LANDesk agent installed on a device in order to avoid having healthy devices that leave your network automatically be granted access to the network without being scanned for security compliance the next time they connect to your network (thereby circumventing the posture validation process).

If a device has only the applicable trust agent installed (either CTA or LTA), they will be considered healthy and let back on the network without having their posture validated.

To prevent this from happening, install the full standard LANDesk agent as soon as possible on your devices.

To install the Cisco Trust Agent on managed and unmanaged devices

1. From the device, create a UNC mapping to the location of the unhealthyCisco.html file. This HTML page should already be copied to a Web share on the remediation server. (This is the location you specified when you configured the remediation server in the **Location to copy compliance files** field).
2. Or, open the device's browser and enter the URL to the unhealthyCisco.html file located on the remediation server.
3. Follow the instructions on the page that displays.
4. When the CTA is installed, you can click the link to scan your computer for compliance, and then follow the instructions to gain Internet access only or to gain full access to the corporate network by installing the necessary security client.

Setting up and configuring a posture validation server

This is a required component for only the Cisco NAC solution. The LANDesk DHCP solution does not require a dedicated posture validation server.

For more information and step-by-step instructions, see "Setting up and configuring a dedicated posture validation server" on page 429.

Configuring a connection between the posture validation server and the Cisco Secure ACS

This is a unique procedure for the Cisco NAC solution.

For more information and step-by-step instructions, see "Configuring a connection between the posture validation server and the Cisco Secure ACS" on page 431.

Setting up and configuring a remediation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC solutions.

For more information and step-by-step instructions, see "Setting up and configuring a remediation server" on page 396.

What you should do after setting up a Cisco NAC implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk NAC is to: define your compliance security policy, publish LANDesk NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. These tasks are generally the same and apply to the LANDesk DHCP, Cisco NAC, and LANDesk 802.1X solutions. For information on performing these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Additionally, to learn more about other ongoing LANDesk NAC management tasks such as: ensuring LANDesk NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing LANDesk NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Quickstart task list for setting up LANDesk integrated Cisco NAC

Use this task list to complete the planning, setup, and configuration tasks required to implement the Cisco NAC solution on your LANDesk network.

You can print this task list and refer to it to track each step during the implementation process. If you're viewing this task list online, click the **For more information** link to view detailed information for a particular task.

Quickstart task list for setting up a Cisco NAC implementation

Done	Task	For more information, go to
	<p>Prerequisite: A LANDesk Management Suite core server must be installed and running on your network, activated with a LANDesk Security Suite license and security content subscriptions:</p> <ul style="list-style-type: none"> • Install the core server • Activate the core with a Security Suite license • Log in as an Administrator user or as a user with both the Security and Patch Management and Security and Patch Compliance rights (allows downloading security and patch content and copying it to the Compliance group) 	<p>"Security and Patch Manager" on page 315</p> <p>For information on the Cisco NAC components and process workflow (including diagrams), see "Understanding the Cisco NAC components and process" on page 415.</p> <p>For information on network topology and design considerations for a Cisco NAC implementation, see "Network topology and design considerations for a Cisco NAC implementation" on page 421.</p>
	<p>Set up a Cisco router:</p> <ul style="list-style-type: none"> • If a router is not already set up, the recommendation is to access the LANDesk Support site for basic instructions, and refer to Cisco documentation 	<p>"Setting up a Cisco router" on page 421</p>
	<p>Set up a Cisco Secure Access Control Server (ACS):</p> <ul style="list-style-type: none"> • If a Cisco Secure ACS is not already set up, the recommendation is to access the LANDesk Support site for basic 	<p>"Setting up a Cisco Secure Access Control Server (ACS)" on page 422</p>

Done	Task	For more information, go to
	instructions, and refer to Cisco documentation	
	<p>Install the Cisco Trust Agent (CTA) on devices to enable compliance scanning:</p> <ul style="list-style-type: none"> For all devices including managed, unmanaged, and new devices: Install the CTA manually using a UNC or URL path (with the unhealthyCisco.html page located on the remediation Web share) 	"Installing the Cisco Trust Agent on devices to enable compliance scanning" on page 422
	<p>Set up a dedicated posture validation server:</p> <ul style="list-style-type: none"> Note: This procedure applies only to the Cisco NAC solution, because this functionality is built into the LANDesk DHCP server On a separate server machine, Windows 2000 or above, with .NET Framework 1.1 Static IP address Run the setup program located in: <coreserver>\LDMain\Install\TrustedAccess\PostureServer 	"Setting up and configuring a dedicated posture validation server" on page 429
	<p>Configuring a connection between the posture validation server and the Cisco Secure ACS:</p> <ul style="list-style-type: none"> Note: This procedure applies only to the Cisco NAC solution, and step-by-step instructions are provided in the topic referenced to the right. 	"Configuring a connection between the posture validation server and the Cisco Secure ACS" on page 431
	<p>Set up a remediation server:</p> <ul style="list-style-type: none"> On a separate server machine, Run the CONFIGURE.REMEDIATION.SERVER.VBS setup script located in: <coreserver>\LDMain\Install\TrustedAccess\RemediationServer Note: This script automatically configures the server to perform remediation by: <ul style="list-style-type: none"> creating a Web share named LDLogon (typically) at: c:\inetpub\wwwroot\LDLogon enabling anonymous access to the 	"Setting up and configuring a remediation server" on page 396

Done	Task	For more information, go to
	LDLogon share with Read and Browse rights <ul style="list-style-type: none"> • adding a new MIME type for .lrd files, and setting it to application/octet-stream 	
	Define compliance security criteria and enable LANDesk NAC with the Security and Patch Manager tool: <ul style="list-style-type: none"> • In the console's Security and Patch Manager tool, • Download security content definitions and patches • Add security definitions to the Compliance group in order to define your compliance security policy • Make sure associated patches are downloaded and available for deployment • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Configure LANDesk DHCP/NAC, first make sure the Enable LANDesk NAC option is checked, and then define healthy and unhealthy postures 	"Defining compliance security criteria in the Security and Patch Manager tool" on page 433
	Configure (add) the posture validation server in the console: <ul style="list-style-type: none"> • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, and click Configure LANDesk DHCP/NAC • Enter the posture validation server name, click Add to add it to the list, and then click OK 	"Setting up and configuring a dedicated posture validation server" on page 429
	Configure (add) the remediation server in the console: <ul style="list-style-type: none"> • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Configure remediation servers, and then click Add • Enter the remediation server IP address, 	"Setting up and configuring a remediation server" on page 396

Done	Task	For more information, go to
	<p>the UNC path to the LDLogon Web share you've created on the remediation server where files are published, and user access credentials, and then click OK</p>	
	<p>Publish LANDesk NAC settings to appropriate servers:</p> <ul style="list-style-type: none"> • In Security and Patch Manager, open the Network Access Control object (under Settings), right-click LANDesk DHCP/NAC, click Publish LANDesk NAC settings, select All, and then click OK • Note: The initial publishing process must include ALL of the LANDesk NAC settings; subsequent publishing can include compliance content only 	<p>"Publishing LANDesk NAC settings" on page 437</p>
	<p>Ensure the posture validation process is working properly:</p> <ul style="list-style-type: none"> • Try a simple test of Cisco NAC by connecting a device to the network. 	
	<p>Perform ongoing compliance security management tasks:</p> <ul style="list-style-type: none"> • Ensuring LANDesk NAC is enabled • Using the allow/restrict Access to everyone option • Understanding what happens when connecting devices are postured • Viewing affected (non-compliant) devices • Modifying and updating compliance security policies • Adding unmanaged devices • Configuring and viewing compliance logging • Generating compliance reports 	<p>"Managing LANDesk NAC compliance security" on page 445</p>

To return to the main help topic for Cisco NAC, see [Using the Cisco NAC solution](#).

Setting up and configuring a dedicated posture validation server

With LANDesk Network Access Control (NAC), a dedicated posture validation server is required only for the Cisco NAC solution. The LANDesk DHCP server has posture validation functionality built in so you don't need a separate machine.

Important: Therefore, this topic applies only if you're implementing Cisco NAC.

The posture validation server evaluates a device's health posture statement against the compliance security rules defined in the Security and Patch Manager tool in the console, and then returns a health posture to the device via the router.

In a Cisco NAC environment, the posture validation server communicates the device's posture statement (or health status) via the Cisco Secure Access Control Server (ACS). See the relevant component and process diagrams in "Using the Cisco NAC solution" on page 413.

You can have more than one posture validation server on your network.

Read this chapter to learn about:

Setting up and configuring a posture validation server

- "Posture validation server prerequisites" on page 429
- "Determining the server location on the network" on page 429
- "Running the server setup program" on page 430
- "Configuring (adding) posture validation servers in the console" on page 430
- "Next steps: Publishing compliance rules to posture validation servers" on page 431
- "Configuring a connection between the posture validation server and the Cisco Secure ACS" on page 431

Posture validation server prerequisites

The machine you set up as a posture validation server must meet the following system requirements:

- Windows 2000 server, Windows 2003 server, Windows XP
- .NET Framework installed (version 1.1)
- The posture validation server can be combined onto another machine such as the LDMS core server.

Determining the server location on the network

You should comply with the following guidelines when deciding the location of the posture validation server on your Cisco network.

- The posture validation server can be installed on the LDMS core server or the primary DHCP server. However, if you have performance or scalability concerns then this should be installed on a separate server machine.
- It is recommended that you use an IP address to identify a posture validation server.
- If installed on a dedicated machine, the posture validation server should be accessible by the LANDesk core server and the Cisco Secure ACS server.

You can see diagrams showing component location and process workflow for each LANDesk NAC solution in their respective overview sections. See "Using the Cisco NAC solution" on page 413.

Running the server setup program

The setup files for posture validation servers are copied to the LANDesk core server during the main installation process. You set up a posture validation server using those setup files.

To set up the posture validation server

1. Map a drive from the machine you want to set up as a posture validation server to the LDMain folder on your core server. Navigate to the \Install\TrustedAccess\PostureServer folder.
2. Run the postureserversetup.exe program.
3. At the **Welcome** screen, click **Next**.
4. Accept the license agreement, and then click **Next**.
5. To copy the necessary files, click **Install**.
6. When the file copy process is complete, click **Finish**.

The posture server setup program copies files, starts the posture server service, and listens for incoming requests on TCP ports 12578 and 12576 (the default ports). You should ensure that any firewalls are open.

The posture validation server is now ready to be configured in the console.

Important additional task for dedicated posture validation servers in a Cisco NAC environment

For a Cisco NAC implementation, you also have to configure a connection between the posture validation server and the Cisco Secure ACS. This connection allows the posture validation server to send posture statements to the ACS for devices attempting to access the network based on the security compliance criteria. For more information, see "Configuring a connection between the posture validation server and the Cisco Secure ACS" on page 431.

Configuring (adding) posture validation servers in the console

Once a posture validation server is set up, you must add it to the list of valid posture validation servers in the **Configure LANDesk NAC** dialog in the console. This allows the core server to configure and communicate with (publish) compliance rules to the posture validation server.

To add posture validation servers in the console

1. In the Security and Patch Manager tool window, right-click the **Network Access Control** group, and then click **Configure LANDesk NAC**.
2. To add posture validation server(s) to your network, enter the IP address of a posture validation server in the field provided, and then click **Add**.
3. Click **OK**.

You can now publish LANDesk NAC content to the server (as long as you've also configured a remediation server and user credentials).

Next steps: Publishing compliance rules to posture validation servers

The next step in setting up and configuring a posture validation server is to publish compliance rules (LANDesk NAC settings) to the posture validation servers. You must first define your compliance security criteria in the Security and Patch Manager tool before you can publish to servers.

For information about these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Configuring a connection between the posture validation server and the Cisco Secure ACS

This task applies only to the Cisco NAC implementation.

For Cisco NAC, you must configure this connection between the posture validation server and the Cisco ACS so that they can communicate during the posture validation process when determining the posture or health status of a device attempting to connect to the network. As stated above, this procedure isn't relevant if you're using the LANDesk DHCP solution.

To configure a connection between the posture validation server and the Cisco Secure ACS

1. Copy the file named `landeskattributes.txt` (located on the core server in the `C:\ProgramFiles\LANDesk\ManagementSuite\Install\TrustedAccess\Cisco` folder) to the `C:` drive of your Cisco Secure ACS.
2. On the Cisco Secure ACS, open a `CMD.exe` window and run the following command:
`C:\ProgramFiles\CiscoSecure ACS v3.3\Utils\csutil -addAVP c:\landeskattributes.txt`
3. Stop and restart the following services on the Cisco ACS:
 - `csauth`
 - `csadmin`
 - `csutil`
4. The LANDesk attributes will now appear in the Available Credentials list.
5. Launch the Cisco Secure ACS console.
6. Click **External User Database | Database Configuration | Network Admission Control | Create a New Configuration**.
7. Enter a name for the new configuration, and then click **Submit**.
8. In the External User Database Configuration box, click **Configure**.

9. In the Mandatory Credential Type box, click **Edit List**.
10. If you ran the batch file mentioned above, the Available Credentials list should show the Landesk.LDSS credentials. Move this object to the Selected Credentials list, and then click **Submit**.
11. In the Credential Validation Policies box, click **External Policies | New External Policy**.
12. Enter the name: PVS1
13. Enter a description.
14. Enter the URL: http://<posture validation server name>:12576/pvs.exe
15. Set the timeout to 30 seconds.
16. Check the **Primary Server Configuration** check box.
17. In the Forwarding Credential Types box, move the Landesk.LDSS from the Available Credentials list to the Selected Credentials list, and then click **Submit**.
18. Add the PVS1 policy to the Selected Policies list, and then click **Submit**.
19. Click **Save Configuration**.

You've now completed the tasks that are specific to the Cisco Secure ACS component required in setting up a Cisco NAC implementation. For a complete list of all the tasks required in setting up a Cisco NAC environment, see the "Quickstart task list for setting up LANDesk integrated Cisco NAC" on page 425.

To return to the main help topic for Cisco NAC, see "Using the Cisco NAC solution" on page 413.

Configuring compliance security criteria and publishing LANDesk NAC settings

Once you've set up your LANDesk NAC environment, the compliance security management tasks described below generally apply to all the LANDesk NAC solutions.

Note: For the LANDesk Network Access Control (NAC) solutions you should have already set up a remediation server and configured (or added) it in the console. Specifically for the LANDesk DHCP solution, you should have a LANDesk DHCP server; and specifically for the Cisco NAC solution, you should have a dedicated posture validation server. For the LANDesk 802.1X solution, you should have an 802.1X Radius server. For more information, respectively, see "Setting up and configuring a remediation server" on page 396, "Setting up a LANDesk DHCP server" on page 400, and "Setting up and configuring a dedicated posture validation server" on page 429. For LANDesk 802.1X, see "Setting up a LANDesk 802.1X Radius server" on page 465.

Read this chapter to learn about:

Configuring compliance security and publishing LANDesk NAC settings

- "Defining compliance security criteria in the Security and Patch Manager tool" on page 433
 - "Using the Compliance group to define a compliance security policy" on page 434
 - "Using LANDesk NAC settings to define healthy and unhealthy postures" on page 435
- "Configuring alternate user credentials" on page 437
- "Publishing LANDesk NAC settings" on page 437
- "Understanding and using the LANDesk NAC remediation pages" on page 440
- "Customizing the HTML pages" on page 442

Other compliance security management tasks

To learn more about compliance scanning and other LANDesk NAC management tasks such as: updating compliance security rules and policies on posture validation servers, updating remediation resources on remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Defining compliance security criteria in the Security and Patch Manager tool

Compliance security criteria is defined by the following factors:

- The vulnerability definitions and other security content definitions you've added to the **Compliance** group in the Security and Patch Manage tool in the console.

AND

- For LANDesk DHCP and Cisco NAC, the healthy and unhealthy definitions for device postures you've specified in the **Configure LANDesk NAC settings** dialog in the console.
- For LANDesk 802.1X, the automatic quarantine time setting you've specified on the **LANDesk 802.1X support** page in the agent configuration.

See the appropriate steplists below for each of these tasks. See "Using the Compliance group to define a compliance security policy" on page 434, and "Using LANDesk NAC settings to define healthy and unhealthy postures" on page 435.

About Security Suite subscriptions

You must have a LANDesk Security Suite content subscription in order to download the various "types" of security content, such as application and operating system vulnerability definitions (and required patches), spyware definitions, blocked application definitions, virus definitions, system configuration security threat definitions, etc.

Without a Security Suite license (or a core server activated with a Security Suite license), you cannot access the LANDesk Security Suite services, and can't define compliance security using those security definitions.

Downloading security type definitions

Use the Security and Patch Manager tool to download different security type definitions, such as vulnerability, spyware, antivirus, and security threat definitions. This task is fully described in the Security and Patch Manager chapter. For more information on using the Security and Patch Manager download features, see "Downloading security content and patch updates" on page 334.

Using the Compliance group to define a compliance security policy

As explained above, the contents of the Compliance group determine your baseline compliance security policy. You can have minimal compliance security made up of just a few vulnerability and security threat definitions, or you can create a complex, strict security policy that is comprised of several security definitions. You can also modify the compliance security policy at any time simply by adding and removing definitions from the Compliance group.

Role-based administration right required to use the Compliance group

Only a LANDesk administrator or a user with the Security and Patch Compliance right can add or remove definitions to and from the Compliance group.

The following security content types can be added to the Compliance group to define a compliance security policy:

- Antivirus definitions
- Custom definitions
- Driver update definitions
- LANDesk software update definitions
- Security threat definitions (includes firewall definitions)

- Software update definitions
- Spyware definitions
- Vulnerabilities (OS and application vulnerability definitions)

Note: You can't add blocked application definitions to the Compliance group to define compliance security policies.

To add security definitions to the Compliance group

1. In Security and Patch Manager, select the type of security content you want to add to your compliance security policy from the **Type** drop-down list, and then drag and drop definitions from the item list into the **Compliance** group.
2. Or, you can right-click an individual definition or selected group of definitions, and then click **Add to compliance group**.
3. Make sure any necessary associated patches are downloaded before you publish LANDesk NAC content to posture validation servers and remediation servers. You can right-click a definition, selected group of definitions, or the **Compliance** group itself, and then click **Download associated patches** to download the patches necessary to remediate affected devices.

Using LANDesk NAC settings to define healthy and unhealthy postures

Your compliance security policy is also comprised of the healthy and unhealthy posture definitions you configure in the console.

To define healthy and unhealthy postures

1. **Prerequisite:** For the LANDesk DHCP solution, make sure you have already set up at least one remediation server, and the LANDesk DHCP server (that includes built-in posture validation functionality). For the Cisco NAC solution, make sure you have already set up a Cisco router, Cisco Secure ACS, posture validation server (with connection to the Cisco Secure ACS), and a remediation server.
2. Make sure you've downloaded the security definitions (spyware, vulnerabilities, security threats, etc.) and patches you want to include in your security compliance policy using the Security and Patch Manager tool, and added those definitions to the **Compliance** group.
3. In Security and Patch Manager, right-click the **Network Access Control** group, and then click **Configure LANDesk NAC**.
4. Check the **Enable LANDesk NAC** option in order to turn compliance security on.
5. To define the healthy posture (or status) for devices attempting to access the corporate network, select the number of hours since the last compliance security scan from the drop-down list. The default value is 96 hours.
(**Note:** This setting applies to both the LANDesk DHCP and Cisco NAC environments and posture validation processes.)

6. To define the unhealthy posture (or status), select the unhealthy posture from the drop-down list (possible unhealthy values include: Quarantine, Checkup, and Infected). These default postures should already be predefined in the Access Control Lists (ACLs) on the Cisco Secure ACS.
(**Note:** This setting actually applies only to Cisco NAC. With LANDesk DHCP, a device is either healthy or unhealthy based on the security definitions in the Compliance group and the healthy posture definition. If the device doesn't meet those conditions the device is unhealthy.)
7. (Optional) Specify the minimum logging level by selecting an option from the drop-down list. Available logging levels include: Information, Warning, Error, Critical Error, and Debug. The different logging levels determine how much information is written to the log file.

About the Configure LANDesk NAC dialog

Use this dialog to enable LANDesk NAC on your network, define healthy and unhealthy postures, configure logging, add LANDesk DHCP servers or posture validation servers, and publish LANDesk NAC settings to the appropriate servers on your network.

Note: You must first install and set up a LANDesk DHCP server or posture validation server before you can add them to your network with this dialog.

- **Enable LANDesk NAC:** Turns on LANDesk NAC compliance security (for both the LANDesk DHCP or Cisco NAC implementations). By default this option is unchecked, which essentially allows network access to every connecting device whether it is healthy or unhealthy. Leave this option unchecked if you want to allow everyone access to the network.

Considerations: By leaving this option unchecked, you can allow time to finalize the configuration of your LANDesk NAC network and baseline compliance security policy; let the regular Security and Patch Management process bring the majority of your managed devices into compliance; observe the various LANDesk NAC logs and reports; and choose the right time to begin enforcing a compliance security policy that restricts network access. Once the majority of managed devices are compliant, or whenever you as the network administrator feel it is time to begin enforcing compliance endpoint security, check this option to enable LANDesk NAC on your network and block network access to devices that are found to be non-compliant.

- **Definition of healthy:** Indicates the number of hours since the last compliance security scan that didn't detect any vulnerabilities (as defined by the contents of the **Compliance** group in Security and Patch Manager on the scanned device).
- **Definition of unhealthy:** Indicates the default unhealthy posture that determines whether the scanned device is unhealthy. Default postures are defined by the Access Control Lists in the Cisco NAC implementation.
- **Minimum logging level:** Indicates the logging level for the posture validation server log files.
- **LANDesk DHCP or posture validation server name:** Enter the name of the server in this field (LANDesk DHCP server if you're using the LANDesk DHCP solution, or dedicated posture validation server if you're using the Cisco NAC solution), and then click **Add** to add the server to your network. When you publish LANDesk NAC settings, they are published to all of the servers included in this list.

- **Publish:** Opens the **Publish LANDesk NAC settings** dialog that lets you specify which content you want to publish to posture validation servers, LANDesk DHCP servers, and remediation servers. Any time you change the LANDesk NAC settings, you must republish the new settings. (**Note:** Publishing **LANDesk NAC content** sends LANDesk NAC settings and compliance rules to posture validation servers or LANDesk DHCP servers; **AND** sends any associated patches to remediation servers. Publishing **Infrastructure** files sends setup and support files, including the security client scanner and trust agents as well as the HTML template pages, to remediation servers.)

Configuring alternate user credentials

If the connecting devices attempting to access the network are not logged in with local administrator rights, LANDesk NAC uses this list of alternate user credentials to attempt to gain administrative rights to the device. Otherwise, the security client scanner cannot run and the user will need to log off and back on with administrative rights and try again (such as vendors or visitors). LANDesk NAC uses these credentials to try to access the devices in order to scan for vulnerabilities and to deploy and install patches for remediation.

To configure alternate user credentials

1. In Security and Patch Manager, right-click the **Network Access Control** group, and then click **Configure credentials**.
2. Enter a user name for a user with administrative rights.
3. Enter the user password twice.
4. Click **Add** to add the user credentials to the list to the right
5. These user credentials will be used in the order they are listed if the end user of the connecting device is not logged in with administrative rights.

About the Configure credentials dialog

Use this dialog to identify alternate user credentials for access to end user devices for security scanning and remediation, in case the logged in end user doesn't have administrative access rights.

- **User name:** Enter a user name commonly used for an LANDesk Administrator user on your network.
- **Password:** Enter the password for that user.
- **Confirm password:** Re-enter the password.
- **Add:** Adds the user credentials in the list to the right.
- **Remove:** Removes the selected user from the User name list.
- **OK:** Saves your changes and exits the dialog.
- **Cancel:** Exits the dialog without saving your changes.

Publishing LANDesk NAC settings

Publishing LANDesk NAC settings sends information and resources to posture validation servers and remediation servers that is required in order to implement the posture validation process and enforce compliance security.

The publishing LANDesk NAC settings process applies to both the LANDesk DHCP and Cisco NAC solutions.

In order to publish LANDesk NAC settings from the console, you must have at least one posture validation server, one remediation server, and user credentials configured.

The initial publish must include All settings

The first time you publish LANDesk NAC settings to your posture validation servers and remediation servers, you must include ALL of the LANDesk NAC settings, including: LANDesk NAC content and infrastructure files (see below for details about these files). Subsequent publishing can include LANDesk NAC content or compliance rules only. Typically, the infrastructure files only need to be published once to remediation servers.

To publish LANDesk NAC settings

1. You can access the **Publish LANDesk NAC settings** dialog and publish the settings from several locations in the Security and Patch Manager tool. For example, you can right-click the **Network Access Control** object or the **Compliance** group, and then click **Publish**. You can also find the **Publish** button on the **Configure LANDesk NAC** and **Configure remediation server** dialogs. Additionally, you can click the **Publish LANDesk NAC settings** toolbar button in the Security and Patch Manager window.
2. To publish all of the LANDesk NAC settings, including the LANDesk NAC content and the Infrastructure files to all of your posture validation servers and remediation servers at once, select the **All** checkbox and click **OK**.
3. If you want to publish only the LANDesk NAC content (security definitions, LANDesk NAC settings or compliance rules, and associated patches) to posture validation servers and remediation servers, check the **LANDesk NAC content** checkbox, and then click **OK**.
4. If you want to publish only the Infrastructure files (security client scanner, trust agent installs, and HTML pages to remediation servers), check the **Infrastructure** checkbox, and then click **OK**. (Typically, you have to publish the Infrastructure files only one time to remediation servers.)

About the Publish LANDesk NAC settings dialog

Use this dialog to publish LANDesk NAC settings to posture validation servers, and to publish remediation settings (resources) to remediation servers on your LANDesk network.

- **All:** Published both LANDesk NAC content and Infrastructure files to the appropriate servers.
- **LANDesk NAC content:** Publishes the LANDesk NAC content and settings you've defined in the Security and Patch Manager tool to all of the posture validation servers and remediation servers that have been added to your network.
Important: You must have at least one posture validation server on your network in order to publish LANDesk NAC content.

- LANDesk NAC content represents the vulnerability and other security content type definitions that currently reside in the **Compliance** group in the Security and Patch Manager tool, as well as the LANDesk NAC settings such as healthy and unhealthy posture settings, logging levels, etc. that are defined in the **Configure LANDesk NAC settings** dialog. Security definitions, healthy and unhealthy posture settings, and logging levels are published to posture validation servers, while associated patch files are published to remediation servers (based on the contents of the Compliance group at the time you publish).
(**Note:** If you change the contents of the **Compliance** group or change LANDesk NAC settings on the **Configure LANDesk NAC** dialog, you must republish this data to your servers.)
- **Infrastructure:** Publishes the following remediation resources to all of the remediation servers that have been added to your network.
 - **Setup and support files:** Setup and support files represent the security client scanner and trust agent installs. The security client scanner performs security scanning and remediation on devices. There are currently four versions of the security client: NAC, NAC for NT4 clients, DHCP, DHCP for NT4 clients. The security client scanner also includes a minimal LANDesk standard agent. Trust agent installs let end users install the LTA and CTA on their devices from a Web URL.
 - **HTML pages:** Represents the template HTML pages that are served by the remediation server to devices with trust agents installed that are trying to access your corporate network. These pages tell the end user what to do in order to gain limited access to the network, or to have their computers remediated in order to become compliant with your security policy and gain full access to the corporate network. These HTML pages are templates that you can modify.
(**Note:** Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the LANDesk NAC content (compliance criteria), you don't need to republish these files every time you change the compliance security policy.)

Understanding and using the LANDesk NAC remediation pages

The LANDesk NAC remediation pages are HTML files that are published to remediation servers with the Publish LANDesk NAC settings tool in the console. These remediation pages are part of the remediation infrastructure files. Typically, these files only need to be published once to remediation servers.

After installing LANDesk Management Suite, these files are located in the following folder on the core server: ManagementSuite\Install\TrustedAccess\RemediationServer

The HTML pages are merely templates, and you should modify them to suit your own compliance security needs and requirements. For information on how to customize the HTML pages, see "Customizing the HTML pages" on page 442.

The sections below describe the purpose of each HTML page.

Healthy status page (for LANDesk DHCP)

This HTML page is used to inform the corporate end user of a connecting device that the device posture has been evaluated and is determined to be healthy, according to the compliance security credentials, and that it has been granted full access to the corporate network.

The name of this HTML page is: Healthy.html

The healthy status page will ONLY be seen when a device transitions from unhealthy to healthy. It will not display each time a device postures as healthy.

The URL to this page on the remediation server should be entered in the **Healthy URL** field when you configure remediation server properties with the LANDesk DHCP Manager tool.

First time visitor status page (for LANDesk DHCP)

This HTML page is used to inform a visitor to your corporate network that you have implemented compliance or network access control security on your network and that they can choose to either browse the Web (Internet access only) or have their computer scanned for vulnerabilities or other security risks, and remediated if necessary, before being allowed access to the corporate network. Links are provided on this HTML page that allow Internet access only or that allow the visitor to download and install the necessary software for compliance scanning and remediation so that their device can be have full access to the network.

The name of this page is: Visitor.html

This page provides links that lets the user either be granted Internet access only, or lets them download and install the trust agent and necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network.

The URL to this page on the remediation server should be entered in the **First time visitor's URL** field when you configure remediation server properties with the LANDesk DHCP Manager tool.

Unhealthy employee status page (for LANDesk DHCP)

This HTML page is used to inform the end user of the connecting device that their device has been scanned and does not meet one or more of the compliance security credentials, is considered unhealthy, and has been denied access to the network. The network administrator should customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the end user must log into the network again to be allowed access.

The name of this page is: FailedEmployee.html

The URL to this page on the remediation server should be entered in the **Employee's failed to connect URL** field when you configure remediation server properties with the LANDesk DHCP Manager tool.

Unhealthy visitor status page (for LANDesk DHCP)

This page is used to inform a visitor to your corporate network that their device has been scanned and does not meet one or more of the compliance security credentials, and has been denied access to the network. As with the unhealthy employee status page, network administrators can customize this HTML page so that it can show which vulnerabilities or other security exposures were detected on the device, and provide specific instructions on how to remediate them. Once the device is repaired, the visitor should click the Security scan for network access icon that now appears on their desktop.

The name of this page is: FailedVisitor.html

The URL to this page on the remediation server should be entered in the **Visitor's failed to connect URL** field when you configure remediation server properties with the LANDesk DHCP Manager tool.

Unhealthy Cisco page (for Cisco NAC)

Note: This HTML page applies only in a Cisco NAC environment. This file is not used if you've implemented the LANDesk DHCP solution for compliance security. Likewise, all of the other HTML pages described above apply to a LANDesk DHCP environment, and aren't used with the Cisco NAC solution.

This HTML page should be used to inform the user of a device attempting to access your network that the device has been scanned and does not meet the compliance security credentials, is considered unhealthy, and has been denied access to the network.

The name of this page is: UnhealthyCisco.html

This page provides links that lets the user either be granted Internet access only, or lets them download and install the trust agent and necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network.

Customizing the HTML pages

As mentioned previously, the HTML pages provided by LANDesk NAC are merely templates that you can manually edit and modify to suit your specific compliance security requirements and policies.

You can use your HTML editor of choice to modify the HTML files. You can modify the existing text to provide additional helpful information specific to your corporate network, and add HTML DIV sections for the security definitions that are included in your compliance security policy (i.e., the definitions contained in the **Compliance** group in the Security and Patch Manager tool). Keep in mind that if you change an HTML file on the core server after it has been published to remediation servers, you must republish the files to the remediation servers before they can be presented to connecting devices (select **HTML pages** under the **Infrastructure** group on the **Publish LANDesk NAC Settings** dialog).

Adding DIV sections to dynamically show security definitions whose remediation failed

It can be especially useful for corporate end users as well as visitors to your network if you customize the "failed" (or unhealthy) pages so that they can see exactly what the security problems are with their computer and what specific steps need to be taken in order to remediate the problem so their device can be rescanned, evaluated as healthy, and allowed full access to the network.

These pages are designed to dynamically display content when a detected vulnerability can't be repaired by the security scanner's remediation tool. In other words, if the end user device is scanned and vulnerabilities or other security exposures are detected (such as system configuration security threats, spyware, etc.), and the repair job fails, the failed (or unhealthy) HTML page can show those specific security definitions identified by their unique ID number along with other additional information that instruct the end user how to remediate the problem AS LONG AS the system administrator has added a DIV section for that security definition (see a DIV section example below). If remediation fails for a security definition, and that definition does not have a corresponding DIV section in the HTML file, no information specific to that definition will display in the end user device's browser.

To customize an HTML page

1. Open the HTML file in your HTML editor.
2. Edit any of the existing boilerplate text in order to provide as much detailed information as you want your end users (corporate employees and visitors) to see when they log into your corporate network.

3. For the failed HTML pages, add new DIV sections in the HTML code (using the example DIV sections as a model) for the security content definitions you've placed in the Compliance group that defines your compliance security policy.
Adding DIV sections for every security definition is not required, but only those definitions with DIV sections in the HTML file can appear if that security exposure is detected AND wasn't repaired by the security scan. See the sample DIV entry below.
You can add steps needed to repair the security problem, links to software download sites, and any other information you think will assist the end user in resolving the issue.
4. Save your changes.
5. Republish modified HTML pages to your remediation servers.

Sample DIV entry in a failed (unhealthy) HTML file

Below is an example of text that would appear in the browser if a device failed the compliance security scan and was determined to be unhealthy. This example is based on the boilerplate text already in the failed HTML files, and describes two security definitions that could not be remediated:

Automatic Windows Update (ST000003):

- Step 1: Click on Start
- Step 2: Click on Control Panel
- Step 3: Open Automatic Updates
- Step 4: Click on Automatic
- Step 5: Click OK

No Antivirus Software (AV-100): Click here to install the Symantec Anti-Virus Client

And here is the actual HTML code for that example:

```
<div style="display:block;clear:both;">&nbsp;&nbsp;&nbsp;</div>
<div id="ttip">
<p>
<ul>
<li>Step 1: Click on Start</li>
<li>Step 2: Click on Control Panel</li>
<li>Step 3: Open Automatic Updates</li>
<li>Step 4: Click on Automatic</li>
<li>Step 5: Click OK</li>
</ul>
</p>
</div>
<div id="ttip">
<p>
<strong>No Antivirus Software (AV-100):</strong>&nbsp;&nbsp;&nbsp;<a
href="symantec.exe"><strong>Click here</strong></a> to install the
Symantec Anti-Virus Client
</p>
</div>
```

Finding and inserting definition IDs

The security definition is identified by the following code in the HTML file:

```
<div id="ttip">
```

Where "ttip" is the actual ID of the security definition. You can find a definition's ID on its properties page in Security and Patch Manager. Type the ID exactly as it appears in the definition's properties.

If that particular security definition's remediation fails, the contents of the DIV section will dynamically appear in the end user browser and provide the end user with useful information to remediate the problem (to the extent that you've entered that information).

Managing LANDesk NAC compliance security

Once you've set up LANDesk Network Access Control (NAC), the subsequent ongoing compliance security management tasks described in this chapter apply to one or more of the LANDesk NAC solutions.

Read this chapter to learn about:

Managing compliance security

- "Ensuring LANDesk NAC services is enabled" on page 445
- "Using the allow/restrict access to everyone option" on page 446
- "What happens when connecting devices are postured" on page 447
- "Viewing affected (non-compliant devices)" on page 449
- "Modifying and updating compliance security policies" on page 449
- "Adding unmanaged devices to the Unmanaged Device Discovery tool" on page 449
- "Configuring and viewing compliance logging" on page 450
- "Generating compliance reports" on page 451

Ensuring LANDesk NAC services is enabled

LANDesk NAC services is essentially enabled when ALL of the following conditions exist:

- A network control device is set up and configured properly, with the necessary services running. For Cisco NAC, this is the router and the Cisco Secure ACS. For LANDesk DHCP, this is your network router/switch and the LANDesk DHCP server. For LANDesk 802.1X, this is your network switch and the 802.1X Radius server.
- The Security and Patch Manager tool can be accessed in the console by a user with the necessary rights, and a valid Security Suite content subscription allows you to download some or all security content types (definitions and required patches).
- At least one security content definition is contained in the Compliance group in the Security and Patch Manager tool. You can have as many definitions as you want to define your current compliance security policy depending on your security needs and goals, and the existing exposure risks. The contents of the Compliance group is the primary factor that defines your compliance security policy, and can include OS and application vulnerabilities, spyware, antivirus, software updates, custom definitions, and system configuration security threats including firewall configurations, whatever is critical in protecting your network at any given time. However, keep in mind that you must have at least one definition in the Compliance group in order for LANDesk NAC to be enforced and the posture validation process to occur. If the Compliance group is empty, there are no security credentials to check for, posture validation can't take place, and LANDesk NAC isn't operational.
- (Cisco NAC only) At least one dedicated posture validation server is set up and configured properly, with security compliance rules published to it from the core server (i.e., LANDesk NAC settings defining healthy and unhealthy postures, and Compliance group content information). In a Cisco NAC implementation, the posture validation server must be configured to communicate with the Cisco Secure ACS.

- At least one remediation server is set up and configured properly, with remediation resources published to it from the core server (i.e., the security client or vulnerability scanner utility, patches associated with the vulnerabilities contained in the Compliance group, and the HTML pages that provide links to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other problems).

AND

- For LANDesk DHCP and Cisco NAC, the **Enable LANDesk NAC** option on the **Configure LANDesk NAC** dialog is checked. For LANDesk 802.1X, the **Enable 802.1X Radius server** option on the **Configure LANDesk 802.1X** dialog is checked.

Establishing your own desired level of endpoint compliance security

If all of the conditions listed above are met, LANDesk NAC services IS running on your network.

Of course, there is flexibility built in to the service and you can customize how LANDesk NAC handles devices with options such as the Exclusion List and Allow Everyone On. You can also control the level of security by how many and exactly which security content definitions you place in the Compliance group, as well as the number of hours you specify before a compliance security scan runs automatically on connected devices.

By adjusting these options and policy criteria, you can define very strict, complex security policies or simple, lenient security policies, or any level in between. In other words, you have the ability to customize the degree of difficulty, or ease, with which a connecting device can comply with the security criteria you specify.

Most importantly, you can change the nature of your compliance security policy at any time in order to meet constantly changing circumstances and requirements. Just remember that any time you change your compliance security criteria (for example, the contents of the **Compliance** group in Security and Patch Manager, or the LANDesk NAC setting on the **Configure LANDesk NAC** dialog), you need to republish LANDesk NAC settings to your posture validation servers and remediation servers.

Using the allow/restrict access to everyone option

For the LANDesk DHCP and Cisco NAC solutions, you can turn on and off the entire posture validation process for your network with each solution's respective allow/restrict access option.

You can use this option to allow time to finalize the configuration of your LANDesk NAC and compliance security policy, to let the regular Security and Patch Management process bring the majority of your managed devices into compliance, to observe the various LANDesk NAC logs and reports, and to choose the right time to begin enforcing a compliance security policy and restricting network access. Once the majority of managed devices are compliant, or whenever you as the network administrator feels it is time, enabling this option turns on LANDesk NAC on your network and blocks network access to devices that are found to be non-compliant.

To allow access to everyone (disabling the posture validation process)

If you leave this option enabled, LANDesk NAC (the posture validation process) will in effect be turned off and any device, whether healthy or unhealthy, can access the network.

For both LANDesk DHCP and Cisco NAC

1. In Security and Patch Manager, right-click the **Network Access Control** group, and then click **Configure LANDesk NAC settings**.
2. Make sure the **Enable LANDesk NAC** option is not checked.
3. Healthy and unhealthy devices will be allowed on to your network until you change this setting.

What happens when connecting devices are postured

This section briefly describes the conditions when devices are checked for compliance via the posture validation process, and what happens when devices are postured.

Viewing posture validation process diagrams for LANDesk NAC solutions

You can also view the posture validation process for devices with or without trust agents in both LANDesk NAC environments. See the following two sections for the diagrams:

- "Understanding the LANDesk DHCP components and process" on page 381
- "Understanding the Cisco NAC components and process" on page 415

In a LANDesk DHCP environment

A connecting device is forced to posture when:

- Acquiring an IP address
- Changing its IP address (release/renew)
- Renewing its IP address

When a connecting device without the LTA installed is postured:

- The device is placed in the quarantine network without warning or notification.
- The device may have limited network resources provided to it in the quarantine network
- A clientless status event is logged in the log file reports
- The end user can install the trust agent at this point
- Or the end user can choose to browse the Web only (if the network administrator has set this up as an option)

When a connecting device with the LTA installed is postured and found to be unhealthy or non-compliant:

- The device is scanned

When a connecting device with the LTA installed is posture and found to be healthy or compliant:

- The device is allowed onto the network with no interruption
- A healthy status event is logged in the log file reports

In a Cisco NAC environment

A connecting device is forced to posture when:

- Attempting to connect to a network segment protected by Cisco NAC
- Periodically on a configurable interval

When a connecting device without the CTA installed is postured:

- The device is handled as clientless, and follows whatever rules have been set up for a clientless user in the Cisco Secure ACS

When a connecting device with the CTA installed is postured and found to be unhealthy or non-compliant:

- The device is presented with a message box (health statement), which can be set up in ACS to give instructions on what to do next for remediation
- A status is logged in the ACS log file (Healthy, Infected, Checkup, Quarantine, and Unknown)
- The end user must manually browse to the remediation page. Ideally the Cisco ACS message box (health statement) should be configured to display the URL
 - The end user can click the appropriate link to scan the device (NT4 machines use a different link)
 - The device is scanned and remediated
 - The Healthy URL is presented
 - A healthy status event is logged
 - The device is allowed access to the network
- Or, the end user can choose to browse the Web without having to scan

When a connecting device with the CTA installed is postured and found to be healthy or compliant:

- The device is allowed onto the network with no interruption
- A healthy status event is logged

Viewing affected (non-compliant devices)

When you want to see which devices have been postured and are found to be unhealthy or non-compliant,

1. In the Security and Patch Manager tool, click the **Computers out of compliance** toolbar button.
2. Or, right-click the **Compliance** group, and then click **Affected computers**.
3. A dialog displays that lists non-compliant devices.
4. You can select a device in the list to view the security definitions with which the device is vulnerable or out of compliance.

Modifying and updating compliance security policies

You can modify and update your compliance security policy at any time.

You do this by changing the content of the **Compliance** group in Security and Patch Manager. For LANDesk DHCP and Cisco NAC, you can also by change LANDesk NAC settings such as the definitions of healthy and unhealthy postures and logging level in the **Configure LANDesk NAC settings** dialog in the console.

You then must republish the LANDesk NAC content to posture validation servers and remediation servers. Remember that publishing LANDesk NAC content sends LANDesk NAC settings and compliance rules to posture validation servers AND any associated patches to remediation servers; while publishing Infrastructure files sends setup and support files (including the security client scanner, trust agent installs, and HTML template pages to remediation servers). (**Note:** Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the LANDesk NAC content, you don't need to republish these files every time you change the compliance security policy.)

For detailed information, see "Defining compliance security criteria in the Security and Patch Manager tool" on page 433.

Adding unmanaged devices to the Unmanaged Device Discovery tool

If you want to add unmanaged devices in to the Unmanaged Device Discovery tool, so that they can be configured with LANDesk agents and scanned and remediated for compliance, follow the procedure below.

1. In Security and Patch Manager, right-click the **Network Access Control** group, and then click **Add unmanaged devices**. (**Note:** In order to add unmanaged devices you must have at least one posture validation server set up and configured in the console.)
2. Click **Tools | Configuration | Unmanaged Device Discovery** to open the tool, and then click the **Computers** group. You might need to refresh to see the newly added devices.

Configuring and viewing compliance logging

LANDesk NAC provides the ability to configure and generate several log files for various posture validation processes. You can customize the logging levels (the amount of information written to the log files for these logs). The log files are useful if you need to analyze certain processes or for troubleshooting.

About the posture validation server log (Cisco NAC only)

This log file is located on the posture validation server, at:

- C:\Program Files\LANDesk\PostureServer\PostureServer.log

The posture validation server log shows

- All logged posture events (Healthy, Unhealthy, Unknown)
- Reasons for Unhealthy and Unknown events

To configure the logging level for posture validation server logs

1. In Security and Patch Manager, right-click the **Network Access Control** group, and then click **Configure LANDesk NAC**.
2. Select a **Minimum logging level** from the drop-down list. Available logging levels include: Information, Warning, Error, Critical Error, and Debug.
Note: The logging level you specify applies to all posture validation servers and LANDesk DHCP servers in the list.

To view posture validation server logs

- You can view the log file directly at the posture validation server at the path noted above.
- Or, a more convenient access to the posture validation server logs is from the console's Security and Patch Manager tool. Simply open the **Network Access Control** object in the Security and Patch Manager tree, and double-click the log file you want to view online.

About the LANDesk DHCP service log

This log file applies only to the LANDesk DHCP solution.

This log file is located on the LANDesk DHCP server, at:

- C:\Program Files\LANDesk\LDDHCP\DHCPService.log

The LANDesk DHCP service log shows:

- All logged DHCP events from the LDDHCP service
- Posture status of devices requesting DHCP leased IP addresses

You can configure the logging level for LANDesk DHCP logs by setting a **Minimum logging level** from the drop-down list on the **Configure LANDesk NAC** dialog.

About the Cisco ACS log

This log file applies only to the Cisco NAC solution.

This log file is located on the Cisco Secure ACS machine. You can access this log file from the Cisco Secure ACS utility, under **Failed Authentications Log**.

Generating compliance reports

LANDesk NAC is represented by several new LANDesk NAC and compliance related reports in the Reports tool. These reports provide a variety of useful information about LANDesk NAC connection attempts, unmanaged device discovery, healthy and unhealthy devices postures, compliance trends, compliance security policy, and compliance status for your LANDesk network. Data for the LANDesk NAC and compliance reports comes from the server log files (mentioned above).

For example, some of the LANDesk NAC and compliance reports include:

- **All Log Entries**
- **Device/User Log Entries**
- **Devices Discovered**
- **Healthy Log Entries**
- **Summary**
- **Unhealthy Log Entries**

In order to access the Reports tool, and generate and view reports, a LANDesk user must have either the LANDesk Administrator right (implying full rights) or the specific Reports right.

LANDesk NAC reports follow the same rules as the reports in the Software License Monitoring group, including their ability to be copied, removed, exported, and so on from the My Reports and User Reports groups.

Running and publishing reports

You can run any report from the Reports window. From the Reports window, right-click the report you want to run, and then click **Run** (or, click the **Run** toolbar button). The report data displays in the Report View.

You can also publish reports to a secure file share where they can viewed by any user you've given the proper access credentials.

For more information about using the Reports tool, and a complete listing of the LANDesk NAC and compliance security reports with descriptions, see "Reports" on page 123.

Using the LANDesk IP Security solution

This section describes how to plan, set up, configure, and enable the LANDesk IP Security implementation of LANDesk NAC.

LANDesk NAC overview

For an overview of LANDesk NAC, see the LANDesk NAC chapter in the *LANDesk Management Suite Users Guide* or *LANDesk Security Suite Users Guide*.

The LANDesk IP Security solution leverages existing IP security (IPsec) protocols native to TCP/IP in order to provide network access control at a base network level. IP security secures network communication through certificate-based authentication.

Important: Technical knowledge and expertise required for setting up LANDesk NAC

Note that all of the LANDesk NAC implementations require additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with one or more of the following security technologies: Cisco NAC and Cisco Secure Access Control Server (ACS) configuration and operation; DHCP server management and DHCP protocols; TCP/IP and IPSec protocols and certificate-based authentication; 802.1X RADIUS server configuration and 802.1X authentication and health posture validation; as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

- "LANDesk IP Security overview" on page 452
- "Understanding the LANDesk IP Security process" on page 453
- "Setting up LANDesk IP Security" on page 453
 - "Installing the LANDesk Trust Agent on devices to enable compliance scanning" on page 454
 - "Creating a master certificate for the IP security healthy policy" on page 455
 - "Importing and exporting master certificates" on page 456
 - "Customizing the IP security health policies (Internet access, exclusion lists)" on page 458
- "Setting up and configuring a remediation server" on page 459
- "Understanding and using the IP Security HTML remediation page" on page 460
- "Viewing IP Security information in the Inventory" on page 460
- "Monitoring IP Security policies with LANDesk Agent Watcher" on page 460

LANDesk IP Security overview

LANDesk IP Security works by providing certificates signed by the LANDesk core certificate authority to managed devices that have passed an initial posture check. If the initial posture check fails then the device is assigned a unique certificate that isolates it from communicating with any other device on the network. If a device is denied access, a prompt instructs the end user how to comply with the security policies outlined by the core server. Once the device is found to be in compliance with the security policy it is assigned a healthy certificate and is granted access to the network and is able to communicate with other healthy devices.

LANDesk IP Security is a network access control solution ideally suited for network with static IP addresses.

LANDesk IP Security doesn't require separate configuration of additional hardware components such as VLANs, posture servers, etc.

LANDesk IP Security lets you enforce your customized compliance security policies defined at the core server.

Understanding the LANDesk IP Security process

Below is a basic outline of the process used to enforce LANDesk NAC when a device attempts to access or connect to the corporate network when LANDesk IP Security is enabled.

Posture validation process

1. When attempting to connect to the network, managed devices are scanned for security compliance to determine their posture as being healthy or unhealthy.

Compliance security policies for IP security are defined by: The vulnerability definitions and other security content definitions you've added to the **Compliance** group in the Security and Patch Manager tool in the console; AND the settings you've configured for the IP Security healthy policy (see below).

2. Healthy (compliant) devices are assigned matching IP security certificates from the core server certificate authority. All healthy devices are assigned the same certificate. A healthy policy is applied to the device. Network access is granted and healthy devices, with matching IP security certificates, are allowed to communication with each other.

Note that when the certificate expires (a setting you configure when creating the master certificate), the device must be scanned again for security compliance in order to validate its health status, and reconfigured with a new certificate.

3. Unhealthy (non-compliant) devices are given a randomly generated key (for the unhealthy policy) that ensures unhealthy machines can't infect each other. An unhealthy policy is applied to the device. Network access is denied and unhealthy devices are isolated (on the same network) and can't communicate with any device except those on the unhealthy exception list. Remediation is then attempted by the remediation or core server and the security compliance scan runs again.

Unmanaged devices are not supported

Unmanaged devices must be configured (via agent configurations) with IP Security certificates in order to communicate with managed devices.

Setting up LANDesk IP Security

Before you can use LANDesk IP Security for network access control, you must first perform a few setup and configuration tasks.

- "Installing the LANDesk Trust Agent on devices to enable compliance scanning" on page 454
- "Creating a master certificate for the IP security healthy policy" on page 455
- "Importing and exporting master certificates" on page 456
- "Backing up and restoring master certificates" on page 456
- "Enabling IP security and deploying compliance settings to managed devices" on page 457
- "Customizing the IP security health policies (Internet access, exclusion lists)" on page 458

Installing the LANDesk Trust Agent on devices to enable compliance scanning

In order to communicate with the LANDesk core server and its certificate authority(CA) function, and to have its health posture evaluated, a device must have the LANDesk Trust Agent (LTA) installed.

The LANDesk Trust Agent (LTA) is used by both the LANDesk DHCP solution, and the LANDesk IP Security solution.

Note: Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.

To install the LANDesk Trust Agent on managed employee devices

- If they already have the standard LANDesk agent, install the LTA with a new device agent configuration
- Or, if they don't have the standard LANDesk agent, install the LTA with the initial agent configuration
- Or, install the LTA with an agent configuration to devices in UDD

To install the LANDesk Trust Agent on unmanaged employee devices

- Install the LTA by pulling with the standard LANDesk agent (wscfg32.exe)
- Or, by using a self-contained Agent Configuration

To install the LANDesk Trust Agent on new end user devices (employee or visitor)

- Install the LTA manually using a UNC or URL path (with the Visitor.html page located on the remediation Web share)

Creating a master certificate for the IP security healthy policy

To create a master certificate

1. In the Security and Patch Manager window, expand the **Network Access Control** node, right-click **IP Security**, and then click **Create Master Certificate**.

Master certificates are automatically encrypted and backed up in the Shared Files\Keys folder. Master certificate backup files have a .B12 file extension

Note that if the master certificate already exists, you're prompted whether you want to create a new certificate that overwrites the old one. If you're replacing the master certificate currently being used, all devices using LANDesk IP Security must be updated with the new certificate.

2. In the Create IP Security Master Certificate dialog, enter the organization name and common name.
3. Enter your name and the purpose for creating the master certificate. This information is stored with the certificate and is used for auditing and tracking purposes which can be useful when importing and exporting master certificates between core servers.
4. Enter and confirm a password for the certificate.
5. Specify the number of days before the copy of the certificate on the client expires.
6. Specify the number of years before the master certificate on the core server expires.
7. Click **OK** to save the master certificate and its settings.

Note: If you're using multiple core servers, you should copy the same master certificate to each core server that you want to manage IP Security-based network access control. Copy the certificate to the: \LDLogon\LTA directory.

About the Create IP security master certificate dialog

Use this dialog to create IP security master certificates.

This dialog contains the following options:

- **Organization:** Enter the full name of your organization.
- **Common name:** Enter the common name of your organization.
- **Name of the individual performing the action:** Enter your name. This information is stored with the certificate and is used for auditing and tracking purposes which can be useful when importing and exporting master certificates between core servers.
- **Purpose:** Enter the reason for performing the action. This information is stored with the certificate and is used for tracking purposes.
- **Password:** Enter the password. Master certificate files are password protected by the administrator.
- **Confirm password:** Verifies the accuracy of the password.
- **Days until client certificate expires:** Specifies the duration (in days) until the certificate on the client expires. You can select between 5 and 365 days.

- **Years until master certificate expires:** Specifies the duration (in years) until the master certificate on the core server expires. You can select between 1 and 16 years.

You can also import, export, backup and restore master certificates.

Importing and exporting master certificates

LANDesk IP Security allows you to import and export master certificates so that you can share them between core servers on your network.

Exported master certificate files have a .X12 file extension.

To import or export a master certificate, in the Security and Patch Manager window, expand the **Network Access Control** node, right-click **IP Security**, and then select the task you want to perform.

Note that if the master certificate already exists, you're prompted whether you want to import a new certificate that overwrites the old one. If you're replacing the master certificate currently being used, all devices using LANDesk IP Security must be updated with the new certificate.

About the Import (and Restore) IP Security master certificate dialog

Use this dialog to import (or restore) IP Security master certificates.

This dialog contains the following options

- **Location of certificate file:** Enter the path to the certificate file, or click **Browse** to find the file.
- **Name of individual performing the action:** Enter your name. This information is stored with the certificate and is used for auditing and tracking purposes which can be useful when importing and exporting master certificates between core servers.
- **Purpose:** Enter the reason for performing the action. This information is stored with the certificate for tracking purposes.
- **Password:** Enter the correct password. Master certificate files are password protected by the administrator.

Backing up and restoring master certificates

LANDesk IP Security allows you to back up and restore master certificates in order to ensure certificate integrity.

To backup or restore a master certificate, in the Security and Patch Manager window, expand the **Network Access Control** node, right-click **IP Security**, and then select the option you want to perform.

Note that if the master certificate already exists, you're prompted whether you want to restore a new certificate that overwrites the old one. If you're replacing the master certificate currently being used, all devices using LANDesk IP Security must be updated with the new certificate.

About the Export (and Backup) IP Security master certificate dialog

Use this dialog to export (or backup) IP Security master certificate.

This dialog contains the following options

- **Location of certificate file:** Enter the path to the certificate file, or click **Browse** to find the file.
- **Name of individual performing the action:** Enter your name. This information is stored with the certificate and is used for auditing and tracking purposes which can be useful when importing and exporting master certificates between core servers.
- **Purpose:** Enter the reason for performing the action. This information is stored with the certificate for tracking purposes.
- **Password:** Enter the correct password. Master certificate files are password protected by the administrator.

Enabling IP security and deploying compliance settings to managed devices

Now that you've created a master certificate, you can enable LANDesk IP Security on your network.

You do this by configuring security compliance settings in the console, and then deploying those IP security-enabled compliance settings to target devices.

To enable IP security in the console

1. In the Security and Patch Manager window, click the **Configure settings** toolbar button, and then click **Compliance settings**.
2. Click **New**.
3. Enter a name for the compliance setting.
4. Click the **Compliance** tab.
5. Specify a scan frequency.
6. Under Actions, check the **Enforce current IP Security configuration after scan** checkbox.
7. Click **OK** to save the compliance setting with IP Security enabled.

To deploy IP Security compliance to target devices

1. In the Security and Patch Manager window, click the **Create a task** toolbar button, and then click **Change settings task**.
2. Select which task type you want to create (scheduled task or policy).
3. Under Compliance settings, select the compliance settings you just created.
4. Click **OK** to save the task.

Once you've configured IP Security with a master certificate, and deployed a compliance settings with IP Security enforcement enabled to your desired target devices, IP Security is in effect on the network.

Customizing the IP security health policies (Internet access, exclusion lists)

You can customize how IP security runs on your network. For example, your network probably includes devices that need to be able to communicate that don't support the IP security protocol such as printers and non-Windows servers and workstations, as well as devices you don't want to control access with IP security. You can accommodate these types of devices with exclusion lists. Or you may want to allow your healthy devices to communicate with other devices that don't have IP security enabled. You can also define an Internet access policy.

LANDesk IP Security lets you modify your healthy (and unhealthy) policies by using the following features:

- IP Security fallback
- Internet access policy
- Exclusion lists

To configure the healthy policy, right-click **Healthy devices policy**, and select an option.

- **Enable IP security fallback:** Allows healthy devices to communicate with other devices that do not have IP Security enabled.
- **Configure Internet access policy:** You can either allow direct access or block direct access to the Internet.
 - Allow direct access adds public Internet IP addresses to the exclusion list so that IP Security managed devices can access the Internet. These public addresses are commonly used by public websites. This option works well as long as you don't have a proxy server and the IP security managed device doesn't use an IP address in the public range.
 - Use the Block direct access option if the managed device has a public IP address. In this case the workstation will need a proxy server configured with the proxy server's IP address in the list of healthy exclusions, otherwise IP security will not work.

Next, you can create exclusion lists to control access.

Using exclusion lists to allow (or disallow) access for specific devices

Exclusion lists (a.k.a., exception lists or allowed devices) let you allow (and disallow) access for certain devices. Exclusion lists can be created for both healthy and unhealthy policies.

You can manually create exception lists, or import devices to the exception list. You can also export exception lists in order to share lists between core servers.

Healthy exceptions are those devices that don't support IP security or that aren't configured with LANDesk IP Security, but must still be able to access the network. For example, you should add devices that don't support IP security, such as Linux or Unix, to the exclusion list for the healthy policy. This ensures those devices are allowed access.

Unhealthy exceptions are approved systems for the unhealthy device to talk to in order to get healthy again. By default this list includes the core server, the local DNS and DHCP servers, and the local gateway.

You can create an exclusion list by adding devices identified by their IP address information.

To manually create an exclusion list

1. In the Security and Patch Manager window, expand the **Network Access Control** node, expand the **IP Security** node, expand the **Healthy devices policy** node, right-click **Allowed devices**, and then click **New**.
2. Specify the devices you want to allow, either by single IP address, or by subnet in order to allow an entire network.
3. Click **OK**.

You can also create exclusion lists by importing devices with the Extended Device Discovery (EDD) tool or from a CSV file.

Additional guidelines and considerations when using exclusion lists

We recommend as a general rule that you add only devices or subnets that don't have IP Security enabled to Healthy exclusion/exception lists.

The exception to this rule is when two devices are both IP Security enabled but don't trust each other because they're using different master certificates. In this case, you should put both nodes into each other's Healthy exception list.

The outline below might be helpful to better understand how exception lists work in the LANDesk IP Security environment. If we look at two healthy devices A and B as an example:

- If node A is IP Security enabled but node B is not IP Security enabled, and
- B is not in A's exception list, then A and B can't communicate
- B is in A's exception list, then A and B can communicate
- If node A and node B are both IP Security enabled, and
- A and B are not in each other's exception list, then A and B can communicate
- B is in A's exception list and A is in B's exception list, then A and B can communicate
- B is in A's exception list, then A and B can't communicate

Setting up and configuring a remediation server

This is a common component and therefore a common task for the LANDesk DHCP, Cisco NAC, and LANDesk IP Security solutions.

For more information and step-by-step instructions, see "Setting up and configuring a remediation server" on page 396.

Understanding and using the IP Security HTML remediation page

As with the other trusted access implementations, LANDesk provides an HTML remediation page (web page) for IP Security. This HTML page displays on a device when it fails the compliance security scan and is determined to be unhealthy. The device is denied access and the page displays.

Administrator must manually edit this file, to enable dynamic display of vulnerability information and any remediation steps, just like with the other "failed" HTML pages.

For more information, see "Understanding and using the LANDesk NAC remediation pages" on page 440.

Viewing IP Security information in the Inventory

You can view IP Security information in the device inventory. This inventory data allows you to do queries based on the IP Security posture/status of scanned devices (whether they are healthy or unhealthy according to the IP Security policies).

To view the IP Security entry in the inventory, go to **Inventory | Network | TCPIP | Active IP Security Policy**.

To see if LANDesk IP Security is enabled on the device, you can view the device compliance setting by going to **Inventory | Landesk Management | Vulnerability Scan | Settings | Compliance Settings Name**.

Monitoring IP Security policies with LANDesk Agent Watcher

You can monitor the IP Security policy of managed devices.

1. Right-click one or more devices in the console network view, click **Update Agent Watcher settings**.
2. Select the Agent Watcher setting from the list.
3. In the Agent Watcher settings dialog, check the **Monitor IP Security Policy** checkbox.

Using the LANDesk 802.1X solution

This section describes how to plan, set up, configure, and enable the LANDesk 802.1X implementation of LANDesk NAC.

LANDesk NAC overview

For an overview of LANDesk NAC, see the LANDesk NAC chapter in the *LANDesk Management Suite Users Guide* or *LANDesk Security Suite Users Guide*.

LANDesk 802.1X is a Radius proxy solution that works with all major switching vendors supporting the 802.1X standard. With the LANDesk 802.1X solution, a Radius server (either a Microsoft IAS server with the LANDesk EAP IAS plug-in, or a Radius server with the LANDesk 802.1X proxy) performs posture validation, or in other words checks for security policy compliance.

Standard 802.1X authentication requires a username and password in order to access the network. LANDesk 802.1X network access control extends this basic model by also requiring the standard LANDesk agent (CBA) is installed on managed devices requesting network access, and the supplicant device is determined to be compliant with your custom security policy

In addition to the specific 802.1X Radius server component, and required switch and router configuration, you must also set up a remediation server in order to implement LANDesk Network Access Control (NAC).

Important: Technical knowledge and expertise required for setting up LANDesk NAC

Note that all of the LANDesk NAC implementations require additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with one or more of the following security technologies: Cisco NAC and Cisco Secure Access Control Server (ACS) configuration and operation; DHCP server management and DHCP protocols; TCP/IP and IPSec protocols and certificate-based authentication; 802.1X Radius server configuration and 802.1X authentication and health posture validation; as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

Setting up a LANDesk 802.1X implementation of LANDesk NAC

- "Quickstart task list for setting up LANDesk 802.1X" on page 462
- "LANDesk 802.1X overview" on page 462
- "Understanding the LANDesk 802.1X components and process" on page 463
- "Network topology and design considerations for a LANDesk 802.1X implementation" on page 465
- "Setting up and configuring a remediation server" on page 465
- "Setting up a LANDesk 802.1X Radius server" on page 465
 - "Using the IAS Radius server plug-in" on page 466
 - "Using the Radius proxy" on page 468

- "Deploying the LANDesk 802.1X agent to managed devices to enable compliance scanning" on page 471
- "Configuring a switch for LANDesk 802.1X" on page 472
- "Configuring a router for LANDesk 802.1X" on page 472
- "What happens on a managed device configured with 802.1X" on page 472
- "Troubleshooting LANDesk 802.1X" on page 473

What you should do after setting up a LANDesk 802.1X implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk NAC is to: define your compliance security policy, publish LANDesk NAC settings to the appropriate servers, and customize the HTML remediation pages as desired. These tasks are generally the same and apply to the LANDesk DHCP, Cisco NAC, and LANDesk 802.1X solutions. For information on performing these tasks, see "Configuring compliance security criteria and publishing LANDesk NAC settings" on page 433.

Additionally, to learn more about other ongoing LANDesk NAC management tasks such as: ensuring LANDesk NAC services is enabled, using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing LANDesk NAC settings, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see "Managing LANDesk NAC compliance security" on page 445.

Quickstart task list for setting up LANDesk 802.1X

Use this task checklist to help keep track of the steps required to set up the LANDesk 802.1X solution. Use this [Quickstart task list for setting up LANDesk 802.1X](#).

LANDesk 802.1X overview

802.1X is a IEEE security protocol used for port-based network access control. 802.1X provides authentication to devices by either establishing a connection or preventing access if authentication fails. 802.1X is based on EAP, or the Extensible Authentication Protocol. 802.1X is supported by most network switches, and can be configured to authenticate clients that have agent software installed.

LANDesk 802.1X is a Radius proxy solution that works with all major switching vendors supporting the 802.1X standard. With the LANDesk 802.1X solution, a Radius server (either a Microsoft IAS server with the LANDesk EAP IAS plug-in, or a Radius server with the LANDesk 802.1X proxy) performs posture validation, or in other words checks for security policy compliance.

Standard 802.1X authentication requires a username and password in order to access the network. LANDesk 802.1X network access control extends this basic model by also requiring the standard LANDesk agent (CBA) is installed on managed devices requesting network access, and the supplicant device is determined to be compliant with your custom security policy. LANDesk NAC verifies the presence of the standard LANDesk agent (CBA) by looking for a unique device ID created by the agent itself. (Note: The LANDesk EAP will not try to authenticate unless it can find the device ID.)

LANDesk 802.1X with the LANDesk EAP IAS plug-in uses a proprietary LANDesk NAC EAP agent that resides on both the IAS Radius server and on managed devices. The LTA EAP agent is installed on your managed devices via an agent configuration.

With LANDesk 802.1X, the Radius server acts as the network access decision point and works in conjunction with the network switch. The switch acts as the network access control device and forwards device authentication requests to the Radius server which performs the actual authentication. Depending on the results that are returned to the switch from the Radius server, the switch allows or denies device access to the network.

Understanding the LANDesk 802.1X components and process

This section describes the components that comprise a LANDesk 802.1X solution. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when LANDesk NAC is enabled.

The following components are required for the LANDesk 802.1X NAC solution.

Required components

Component	Description
LANDesk core server	Provides the Security and Patch Manager tool used to: download security content (such as OS and application vulnerability definitions, spyware definitions, system configuration security threats, antivirus and firewall configuration definitions, etc.), define compliance criteria, configure remediation servers, and configure and publish LANDesk NAC settings (including compliance security rules or policies and remediation resources for scanning and repairing devices).
Radius server or proxy	Use the LANDesk 802.1X IAS server plug-in if you want to utilize an existing IAS server (or configure a new IAS server) for 802.1X authentication. Use the Radius proxy method if you have a Radius server other than IAS. Or if you don't want to use the LANDesk EAP plug-in.
Remediation server	Contains the necessary setup and support files (security client, security type definitions and required patches, as well as the HTML remediation pages used to scan devices for vulnerabilities) identified by your security policy and remediate (repair) any detected vulnerabilities so that the device can be scanned as healthy or compliant and access the network.
Switch	Acts as the network access control device and forwards device authentication requests to the Radius server which performs the actual authentication.

Component	Description
Router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the 802.1X Radius server to evaluate the posture credentials of the endpoint device. In other words, in an 802.1X NAC environment the router is the policy enforcement point on the network and grants or denies access privileges.
Devices	User devices, attempting to access your corporate network. Typical endpoint devices include desktop computers and laptops but may also be clientless devices such as printers, etc. LANDesk NAC allows you to evaluate the health status of these connecting devices and control network access based on their posture credentials.

The steplist below describes the communication flow between the various components in a LANDesk 802.1X environment when the device attempting to access the network has the 802.1X LTA EAP agent installed.

Process workflow:

1. A managed device configured with the 802.1X LTA EAP agent makes an initial attempt to access the corporate network.
2. The network switch (configured for 802.1X pass-thru forwarding, and acting as the access control point) sends out an EAP-request identity to the supplicant device.
3. A prompt appears on the device asking for a username and password. The end user must type in valid login credentials, which are forwarded by the switch, along with a token added to the EAP-response packet, to the Radius server (configured with either the LTA EAP plug-in or with the LTA Radius proxy, and acting as the access decision point).
4. If the authentication credentials are recognized and the token indicates the device has the standard LANDesk agent installed, LANDesk NAC then runs a compliance security scan that determines the device posture or health status according to the criteria defined by your custom security policy. This scan is performed by a Compliance scan task using a Compliance settings that has the **Enforce 802.1X scan** option enabled on the **Compliance** tab.
5. If the device is considered healthy (or compliant), it is granted access to the corporate network.
6. However, if the device is considered unhealthy (or non-compliant) it remains in the quarantine VLAN. A message box displays informing the user how to contact the remediation server in order to perform vulnerability assessment scanning and remediation. The user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the network's security policy and gain full network access.
7. Remediation is performed by the remediation server by scanning for vulnerabilities and other security risks (the compliance rules mentioned above) and installing any required patches. Once the device is repaired, the network access process is repeated and the healthy (i.e., compliant device is granted access to the corporate network).

Compliance security scans

With Security and Patch Manager you can create and configure a compliance-specific security scan, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task or as a policy.

For information on updating compliance security rules and policies and republishing LANDesk NAC settings, see "Managing LANDesk NAC compliance security" on page 445.

Network topology and design considerations for a LANDesk 802.1X implementation

You should keep the following issues in mind when designing your LANDesk 802.1X implementation:

- The LANDesk core server should not be visible to the quarantine network.
- The remediation server and Radius server can be installed on the same machine, but if performance or scalability issues arise they can be moved to their own server machines.
- The router needs to support a primary and secondary subnet for the client side of the router.
- The router must be configured with the real subnet as the primary subnet and the quarantined subnet as the secondary subnet.
- The secondary subnet should be restricted to only be able to see the remediation server.

Setting up and configuring a remediation server

This is a common component and therefore a common task for LANDesk NAC solutions, including LANDesk 802.1X. You need to set up and configure a remediation server only if you've selected to use a DHCP quarantine network instead of the TCP/IP self-assigned IP address method to quarantine unhealthy devices. LANDesk 802.1X with self-assigned IP addressing uses the built-in NIC TCP/IP functionality.

For more information and step-by-step instructions, see "Setting up and configuring a remediation server" on page 396.

Setting up a LANDesk 802.1X Radius server

LANDesk 802.1X requires an 802.1X Radius server. Choose one of the following methods to implement LANDesk 802.1X on a Radius server:

- "Using the IAS Radius server plug-in" on page 466
- "Using the Radius proxy" on page 468

The sections below provide step-by-step instructions for both methods of setting up the LANDesk 802.1X Radius server.

After you set up the Radius server, you must also configure your network switch and router for 802.1X network access control.

Using the IAS Radius server plug-in

Use the LANDesk 802.1X IAS server plug-in if you want to utilize an existing IAS server (or configure a new IAS server) for 802.1X authentication.

The steps below describe how to install (if necessary) and configure an IAS server with the LANDesk EAP plug-in. Complete all of the steps before enabling LANDesk 802.1X in the console.

Step 1: Install the Radius server and LTA EAP type

1. Install IAS (Internet Authentication Server) on the server you want to set up as the remote access Radius server. You can install IAS from the Windows 2003 CD. (**Note:** The Radius protocol is supported with Windows 2000 and Windows 2003 only.) Follow the installation prompts.
2. Install the LTA EAP type on the Radius server. LTA EAP is the LANDesk proprietary authentication protocol. You install LTA EAP from your LANDesk core server. Map a drive to the core server, and then run the executable file named **LTAEAP.EXE** found in the: `\LDMain\Install\Radius` directory.
3. Reboot the server to register the LTA EAP on the server.

Note: You can verify this new EAP type in the Remote Server Properties page. To do this, go to **Administrative Tools | Routing and Remote Access**. Right-click the remote server, click **Properties**, click the **Security** tab, click **Authentication Methods**, and then click **EAP Methods**. The LTA EAP type should appear in the methods list. If LTA EAP isn't in the list, you need to install it from the core server.

Step 2: Configure and start the remote access service on the Radius server

1. Click **Control Panel | Administrative Tools | Routing and Remote Access**.
2. Right-click the server, and then click **Configure and Enable Routing and Remote Access**. The Routing and Remote Access Server Setup Wizard displays.
3. Click **Next**.
4. Select **Custom Configuration**, and then click **Next**.
5. Select **Dial-up Access**, and then click **Next**.
6. Click **Finish**.
7. If prompted, click **Yes** to start the service.

Step 3: Customize the remote access service (set EAP as the preferred authentication method for remote devices)

1. In the Routing and Remote Access tool, right-click the server you just configured, and click **Properties**.
2. On the **General** tab, verify that the **Remote access server** option is checked.
3. On the **Security** tab, check the **Extensible Authentication Protocol (EAP)** checkbox. (You may want to click the **EAP Methods** button to make sure the new LTA EAP method is in the list of methods.)
4. Click **OK** to exit the Authentication Methods dialog.
5. Click **OK** again to exit the Properties dialog.

Creating a remote access policy on the Radius server

You need to configure a remote access policy that uses the LANDesk EAP method for authentication.

You can do this in either the IAS tool, or in the Routing and Remote Access tool.

Step 1: Create the remote access policy

1. Under the remote server node, right-click **Remote Access Policies**, and then click **New**. The Remote Access Policies wizard displays.
2. Click **Next**.
3. Select **Typical** as the policy type, enter a name for the policy, and then click **Next**. (Note: Enter a descriptive name that easily identifies the policy, such as LANDesk EAP.)
4. Select **Ethernet** as the access method, and then click **Next**.
5. Select **User** for granting access (not Group), and then click **Next**.
6. Select **LTA EAP** as the authentication method, and then click **Next**.
7. Click **Finish** to create the remote access policy.

Step 2: Configure the remote access policy to support both wired and wireless networks

1. Right-click the new remote access policy you just created, and then click **Properties**.
2. Check the **Grant Remote Access Permission** option to enable wireless support.
3. Click **OK**.

Setting up (adding) network switches as Radius clients

Now you need to add the network switches (as Radius clients) that you want to use with LANDesk 802.1X authentication.

You perform this task in the IAS tool (**IAS | Radius Clients**).

By adding a switch as a Radius client, the Radius server is able to recognize and process authentication requests through that switch.

Creating a common user on the Radius server

You must now create a new user on the Radius server in order to establish login credentials. This user's user name and password will determine the authentication credentials for managed devices configured with LANDesk 802.1X LANDesk NAC that attempt to access the network.

Use the server's Computer Management tool to perform this task.

To create a user on the Radius server

1. At the Radius server, click **Start | Programs | Administrative Tools | Computer Management**.
2. Open **Local Users and Groups**, right-click **Users**, and then click **New User**.

3. Enter a user name.
4. Enter and confirm a password.
5. Configure the password with the following settings:
 - uncheck the **User must change password** checkbox
 - check the **User cannot change password** checkbox
 - check the **Password never expires** checkbox
 - make sure the **Account is disabled** checkbox is clear
6. Click **Create**.

The user name and password entered here are the login credentials that an end user must provide in order to respond successfully to the authentication identify request during the LANDesk 802.1X authentication process. Then, the credentials are sent to the Radius server, along with the device LANDesk EAP data, in order to determine whether the device is granted access to the network.

You can now enable LANDesk 802.1X in the console. (The other method of implementing LANDesk 802.1X is to configure and install a Radius proxy. For more information, see "Using the Radius proxy" on page 468.)

Enabling LANDesk 802.1X with the IAS Radius server plug-in

After you've completed all of the setup tasks noted above, you can now enable LANDesk 802.1X authentication.

You do this from the LANDesk console (**Security and Patch Manager | Trusted Access**).

This essentially turns on LANDesk 802.1X authentication services on your network. However, you must still configure managed devices with the LANDesk 802.1X agent before their network access can be managed and enforced through LANDesk 802.1X authentication. See "Deploying the LANDesk 802.1X agent to managed devices to enable compliance scanning" on page 471.

To enable LANDesk 802.1X with the IAS Radius server plug-in

1. In the **Security and Patch Manager** tool, expand the **Settings** node, and then expand the LANDesk NAC node.
2. Right-click the **802.1X** object, and click **Configure 802.1X | Radius server**.
3. Check the **Enable 802.1X Radius Server** checkbox. This turns on 802.1X authentication on your network (for devices with the 802.1X agent) using the IAS Radius server with the LANDesk EAP plug-in that you've configured.
4. Select **EAP type 4**.
5. Select **Use LTA EAP IAS plug-in**.
6. Click **OK**.

The next section describes how to configure LANDesk 802.1X using the Radius proxy method.

Using the Radius proxy

Use the Radius proxy method if you have a Radius server other than IAS. Or if you don't want to use the LANDesk EAP plug-in.

The LANDesk 802.1X Radius proxy can be installed on the following types of Radius servers:

- Cisco ACS
- A10 Networks
- CAMS (Comprehensive Access Management System)
- IAS (Internet Authentication Service)

Coexisting with Radius server software

The LANDesk 802.1X Radius proxy can coexist on servers running Radius server software. If your Radius server is hardware-based, you should install the LANDesk 802.1X Radius proxy on a separate server.

The Radius proxy communicates between the switch and the device with the LANDesk 802.1X agent installed. The proxy is in the middle and the device authenticates with the Radius proxy and the proxy passes the ID and password on to the Radius server. If the agent is not installed on the device attempting to make a connection, then the Radius proxy denies access.

Enabling LANDesk 802.1X with the Radius proxy

In order to use the Radius proxy method of implementing LANDesk 802.1X authentication, you must configure the settings for a Radius proxy installation file, enable LANDesk 802.1X (with the Radius proxy option), and install the Radius proxy on your Radius server.

You do this from the LANDesk console (**Security and Patch Manager | Trusted Access**).

This essentially turns on LANDesk 802.1X authentication services on your network. However, you must still configure managed devices with the LANDesk 802.1X agent before their network access can be managed and enforced through LANDesk 802.1X authentication. See "Deploying the LANDesk 802.1X agent to managed devices to enable compliance scanning" on page 471.

To enable LANDesk 802.1X with a Radius proxy

1. In the **Security and Patch Manager** tool, expand the **Settings** node, and then expand the LANDesk NAC node.
2. Right-click the **802.1X** object, and click **Configure 802.1X | Radius server**.
3. Check the **Enable 802.1X Radius Server** checkbox. This turns on 802.1X authentication on your network (for devices with the 802.1X agent) after you install the Radius proxy that you're configuring here.
4. Select **EAP type 4**.
5. Select **Use LTA Radius proxy**.
6. Specify the Radius server and proxy settings.
7. Enter a name for the Radius proxy install file (MSI). The install file is created in the LDMAIN directory, under Install\Radius\ , you can have multiple Radius proxy server installations, also Radius proxy is supported on any Windows 32-bit platform.
8. Click **OK**.

To install a Radius proxy

1. From the server that you want to configure with the LANDesk 802.1X Radius proxy, connect to the core server and browse to the folder where you saved the proxy installation file.
2. Double-click the MSI file to execute the installation.
3. Click **Close** when the installation is complete. A system reboot is not required.

The Radius proxy installation adds data (such as address and port information) to the server registry.

Not supported on 64-bit platforms

Do NOT install the Radius proxy on Windows 98, or on any 64-bit platform.

The section below describes the dialogs referenced in the tasks above.

About the 802.1X configuration settings: Radius server page

Use this dialog to select a remediation server and publish network access control settings to the remediation server, and to enable LANDesk 802.1X LANDesk NAC on your network.

If you're using the IAS Radius server plug-in method of implementing LANDesk 802.1X, you simply enable the Radius server and specify the EAP type, and then select the IAS plug-in option.

If you're using the Radius proxy method of implementing LANDesk 802.1X, you must not only enable the Radius server and specify the EAP type, but you must also configure the Radius proxy settings for a Radius proxy installation file, and then install the Radius proxy to your designated server.

This dialog contains the following options:

- **Remediation server:** Click **Add** to specify the remediation server you want to use to remediate unhealthy devices placed in the quarantine network. Click on a Help button for information about the remediation server. A remediation server contains the necessary setup and support files (security client, security type definitions and required patches), as well as the HTML template pages used to scan devices for vulnerabilities identified by your security policy and remediate (repair any detected vulnerabilities) so that the device can be scanned as healthy or compliant and access the network.
- **Enable 802.1X Radius Server:** Turns on 802.1X LANDesk NAC. By default this option is unchecked, which essentially allows network access to every connecting device whether it is healthy or unhealthy. Leave this option unchecked if you want to allow everyone access to the network.
- **EAP Type:** Identifies the EAP type used by LANDesk 802.1X authentication. EAP type 4 is a standard EAP type supported by most devices. EAP type 4 uses an MD5 hash challenge, meaning it requires a username and password for authentication.
- **Use LTA EAP IAS plug-in:** Select this option if you want to use the LANDesk EAP plug-in on an IAS Radius server.
- **Use LTA Radius proxy:** Select this options if you want to configure and install a LANDesk 802.1X Radius proxy. Once you select this option, the Radius proxy settings fields can be edited.

- **Radius proxy:**
 - **Radius server address:** Specifies the IP address of your Radius server.
 - **Radius server port:** Specifies the port number of your Radius server. The default port number for Radius authentication is UDP port 1812.
 - **Shared key:** Specifies the shared key (i.e., shared secret) that provides security for communication between the switch and the Radius server. The shared key is a text string. The string you enter here must match the shared key string configured on the switch and on the Radius server.
 - **Radius proxy port:** Specifies the port number of your Radius proxy. This port communicates with the switch. Note that this port number must be different than the Radius server port (above) if they're on the same machine.
 - **Radius proxy forwarding post:** Specifies the forwarding port number of your Radius proxy. This port forwards data to the Radius server.
- **Proxy install file name:** Identifies the Radius proxy installation file. The installation file is created in the LDMain directory, under Install\Radius\. You can create multiple Radius proxy installation files. A Radius proxy is supported on any Windows 32-bit platform.

Deploying the LANDesk 802.1X agent to managed devices to enable compliance scanning

As the final step in setting up LANDesk 802.1X authentication, you must deploy the LANDesk 802.1X agent to target managed devices. This allows the managed devices to be authenticated and either allowed access to the network, or quarantined and remediated.

To deploy the LANDesk 802.1X agent to managed devices

1. In the **Agent Configuration** tool, click **New Windows Configuration**.
2. On the **LANDesk 802.1X support** page, check the **Enable LANDesk 802.1X support** checkbox. (Note: This option is unavailable if you haven't already enabled the 802.1X Radius Server in the console's LANDesk NAC tool.) LANDesk 802.1X uses the EAP type specified in LANDesk NAC in the Security and Patch Manager tool. The EAP type setting is core-wide. In other words, all devices configured with this agent configuration will be configured with the EAP type specified in the console.
3. Select the method you want to use to quarantine any devices found to be unhealthy. (Use IP address in self-assigned range, or Use DHCP in quarantine network.)
4. Configure automatic quarantine by specifying how many hours can transpire since the last health scan has been run on a device before it is considered unhealthy and is logged off the corporate network and placed in the quarantine network.
5. Specify any other device agent configuration settings you want for the target devices being configured.
6. Click **Save**.

You can now deploy the agent configuration to target devices that you want to use 802.1X authentication, and then create compliance scan tasks that scan 802.1X enabled devices for compliance with your security policy.

Creating a compliance security scan task

LANDesk NAC runs a compliance security scan that determines the device posture or health status according to the criteria defined by your custom security policy. This scan is performed by a Compliance scan task using a Compliance settings that has the **Enforce 802.1X scan** option enabled on the **Compliance** tab.

You use the Security and Patch Manager tool to create security scan tasks, including compliance security scans. For step-by-step instructions, see "Creating security (and compliance) scan tasks" on page 350.

Compliance security scans

With Security and Patch Manager you can create and configure a compliance-specific security scan, that checks target devices for compliance with your customized security policy. A compliance scan is based on the contents of the Compliance group and can be run as a scheduled task or as a policy.

For information on updating compliance security rules and policies and republishing LANDesk NAC settings, see "Managing LANDesk NAC compliance security" on page 445.

Configuring a switch for LANDesk 802.1X

Go to the LANDesk Support site for detailed instructions and sample configurations.

Configuring a router for LANDesk 802.1X

Go to the LANDesk Support site for detailed instructions and sample configurations.

What happens on a managed device configured with 802.1X

When a managed device configured with 802.1X authentication attempts to connect to the network, a prompt appears asking for a username and password. The end user must type in the correct login information (which is sent to the Radius server, along with the LANDesk EAP data) in order for the compliance security scan to run on the device. The compliance security scan determines whether the device is healthy or unhealthy according to your custom security policy.

If the scanned device is healthy (compliant) it is granted access to the corporate network.

If the scanned device is unhealthy (non compliant), it is placed in the quarantine network where it can be remediated and scanned again in order to gain access to the corporate network.

Manually resetting 802.1X authentication

You can manually reset the local network card to force another authentication attempt. On the managed device, click **Start | LANDesk Management | 802.1X reset**.

Login dialog behavior: When you run the 802.1X reset option, make sure you first close any open Windows pop-up dialogs, otherwise the login dialog won't display. If the login dialog goes away too quickly, it is most likely caused by the LINK-3-UPDOWN state timing out, and all you need to do is simply try the 802.1X reset feature again.

Troubleshooting LANDesk 802.1X

This section contains information about some possible situations you might encounter with LANDesk 802.1X, and how to address them.

Scheduled compliance security scan task returns "lost connection" status

If a scheduled 802.1X compliance security scan task returns a status that indicates the target device has "lost connection" or that the "task failed" it might be because the task status was sent to the core server while the machine was being restarted. If you see this status, you can check the target device to verify whether it was quarantined or not.

Multiple 802.1X login prompts

When using a Layer 2 Huawei switch (H3C S3900 Series), if a device displays more than one 802.1X login prompt and the end user cancels or closes one of them without entering the correct credentials, the 802.1X authentication process is canceled. In this case, users must enter the correct credentials in each login prompt. If the authentication is canceled, use the 802.1x Reset menu option to restart the authentication process.

LANDesk 802.1X and LANDesk DHCP do not work together

Note that these two LANDesk NAC solutions will not work together as compliance security technologies. The reason for this is that LANDesk 802.1X blocks LANDesk DHCP from releasing IP addresses to clients.(add this note to the overview topics as well)

LANDesk 802.1X is designed to work on desktop platforms only

LANDesk 802.1X is not supported on server platforms.

LANDesk Antivirus

LANDesk Antivirus, a fully integrated antivirus solution in both LANDesk Security Suite and LANDesk Management Suite, protects your managed devices from malicious virus attacks by scanning and cleaning viruses based on the latest known virus definition files.

LANDesk Antivirus offers configurable virus protection features, including: on-demand and automatic virus definition file updates, pilot tests, control of antivirus scan operation and end user interactive options, infected object handling, real-time file and email protection, and scanned device information and reports.

Read this chapter to learn about:

- "LANDesk Antivirus overview" on page 474
 - "Supported device platforms" on page 476
 - "Role-based administration with LANDesk Antivirus" on page 477
 - "Antivirus task workflow" on page 477
- "Configuring devices for LANDesk Antivirus protection" on page 478
 - "Antivirus products that can be automatically removed during configuration" on page 478
 - "Removing LANDesk Antivirus from devices" on page 479
- "Updating virus definition files" on page 480
- "Evaluating virus definition files with a pilot test" on page 481
- "Backing up virus definition files" on page 482
- "Scanning devices for viruses" on page 482
 - "Scanning methods" on page 482
 - "Enabling real-time antivirus protection (file, email)" on page 484
 - "Configuring antivirus scan options with antivirus settings" on page 485
 - "Configuring which files to scan (infectable files only, exclusions, heuristics, riskware)" on page 487
- "What happens on a device during an antivirus scan" on page 490
 - "LANDesk Antivirus client interface and end user actions" on page 490
 - "When an infected object is detected" on page 491
 - "Automatic scanning of quarantined files" on page 491
- "Viewing antivirus activity and status information" on page 492
- "Using antivirus alerts" on page 492
- "Generating antivirus reports" on page 493
- "Viewing antivirus information in the Web console executive dashboard" on page 493

LANDesk Antivirus overview

LANDesk Antivirus is comprised of a built-in antivirus scanner agent, a continuously updated virus signature database, and antivirus configuration options and features available in the console's Security and Patch Manager tool. The LANDesk Antivirus agent is distinct from the Security and Patch Manager scanner agent.

LANDesk Security services maintains a current database of virus definition/pattern files that can be downloaded, evaluated and tested, and distributed to target devices on your LANDesk network.

With LANDesk Antivirus, you can:

- Download the latest virus definition/pattern file updates (the LANDesk Security antivirus signature database is updated several times a day)
- Schedule recurring virus definition file updates
- Archive previous virus definition files
- Create and deploy LANDesk Antivirus agent installation tasks
- Run on-demand and scheduled antivirus scans on target devices
- Configure antivirus scan behavior and end user options
- Select which types of files to scan, and whether to scan for riskware
- Enable real-time file and email virus protection
- View antivirus activity and status information for scanned devices
- Configure antivirus alerts
- Generate antivirus reports

Security content types and subscriptions

When you install LANDesk Management Suite or LANDesk Security Suite, the Security and Patch Manager tool is included by default. However, without a Security Suite content subscription, you can only scan for LANDesk software updates and custom definitions. A Security Suite content subscription enables you to take full advantage of the Security and Patch Manager tool by providing access to additional security and patch content (definition types), including antivirus scanner detection rules and the actual LANDesk Antivirus virus definition files used by the antivirus scanner.

LANDesk Security Suite content types include:

- Antivirus updates (for third-party scanners, includes antivirus scanner detection content only; for LANDesk Antivirus, includes both scanner detection content AND virus definition files, as well as riskware definition files available in an extended database)
- Blocked applications (see the "Legal disclaimer for the blocked applications type" on page 333)
- Custom vulnerability definitions
- Driver updates
- LANDesk software updates
- Security threats (system configuration exposures; includes firewall detection and configuration)
- Software updates
- Spyware
- Vulnerabilities (known platform vulnerabilities, and application-specific vulnerabilities)

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Note that the **Updates** tab of the **Download updates** dialog includes several Antivirus updates in the definition type list, including one named LANDesk Antivirus Updates. When you select LANDesk Antivirus Updates, both the scanner detection content AND the LANDesk Antivirus virus definition file updates are downloaded.

For third-party scanner engines, antivirus updates include scanner definitions that detect:

- Installation of common antivirus scanner engines (including the LANDesk Antivirus tool)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

For the LANDesk Antivirus scanner, antivirus updates includes not only the scanner detection content listed above, but also the virus definition files used by the LANDesk Antivirus scanner.

Antivirus scanner detection content versus virus definition content

Antivirus updates does not imply actual virus definition/pattern files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download LANDesk Antivirus updates, both the scanner detection content AND the LANDesk Antivirus-specific virus definition files are downloaded. LANDesk Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the `\\LDLogon\Antivirus\Bases` folder.

Supported device platforms

LANDesk Antivirus supports most of the same platforms supported by Security and Patch Manager's security scanning capabilities and the standard LANDesk-managed device platforms, including the following operating systems:

- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP2
- Windows 2003
- Windows XP SP1
- Windows XP 64-bit
- Windows XP Home Edition/Professional
- Windows Vista 32-bit and 64-bit

Reboot required for Windows NT 4.0 machines

In order for the LANDesk Antivirus service to be activated, Windows NT 4 machines must be rebooted after agent configuration deployment.

Other system requirements

Make sure the managed devices you want to configure with the LANDesk Antivirus agent meet the following system requirements:

- Microsoft Internet Explorer 6.0 or higher

- No other antivirus programs installed (**Note:** Because this can cause software conflicts, if LANDesk Antivirus is installed on a machine with another antivirus program LANDesk Antivirus will not be activated until that product is uninstalled from the managed device.)

Role-based administration with LANDesk Antivirus

LANDesk Antivirus, just like Security and Patch Manager, uses LANDesk's role-based administration to allow users access to the LANDesk Antivirus features. Role-based administration is LANDesk's access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each LANDesk user is assigned specific rights and scope that determine which features they can use and which devices they can manage.

A LANDesk Administrator assigns these rights to other users with the Users tool in the console. LANDesk Antivirus introduces one new role and corresponding right to role-based administration. The right is called Antivirus, which appears under the Security rights group in the User Properties dialog. In order to see and use LANDesk Antivirus features, a LANDesk user must be assigned the necessary Security and Patch Manager right.

The Antivirus right provides users the ability to:

- Deploy agent configurations with LANDesk Antivirus to target devices
- Download virus definition file updates
- Create scheduled updates
- Create scheduled antivirus scan tasks
- Create antivirus settings
- Deploy antivirus scan tasks and change settings tasks associated with antivirus settings
- Enable real-time file and email protection
- Configure antivirus scans to scan for certain file types
- Exclude certain files, folders, and file types (by extension) from antivirus scans
- View antivirus scan activity and status information for scanned devices
- Enable antivirus alerts
- Generate antivirus reports

Antivirus task workflow

The steps below provide a quick summary outline of the typical processes or tasks involved in implementing antivirus protection on your network with LANDesk Antivirus. Each of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using LANDesk Antivirus:

1. Configuring managed devices for antivirus scanning.
2. Downloading virus definition\pattern file definition updates from a LANDesk Security content server.
3. Determining whether to make virus definition files available to managed devices immediately, or to first evaluate them in a pilot test environment.
4. Creating on-demand and scheduled scan tasks and policies.
5. Configuring antivirus scan operation and end user options.
6. Scanning managed devices for known viruses and suspicious files.
7. Viewing antivirus scan results for scanned devices.
8. Configuring antivirus alerts.

9. Generating, viewing, and distributing antivirus reports.

Configuring devices for LANDesk Antivirus protection

Before managed devices can be scanned for viruses and cleaned, they must have the LANDesk Antivirus agent installed. You can do this either during initial device agent configuration or with a separate installation/update task.

Deployment considerations

If you deploy LANDesk Antivirus to a device that already has another antivirus solution installed and running, LANDesk Antivirus does not enable its real-time protection functionality in order to avoid any potential software conflicts. Once you remove the other antivirus product, you can enable LANDesk Antivirus real-time antivirus protection.

You can now select to automatically remove existing antivirus software from target devices when deploying LANDesk Antivirus, either during initial agent configuration or as a separate LANDesk Antivirus install/update task. See below for a list of antivirus products that can be removed.

Clear password protected antivirus software

If the existing antivirus software is password protected, you must first clear the password before LANDesk Antivirus can uninstall the software.

Antivirus products that can be automatically removed during configuration

Antivirus products that can be automatically removed when deploying LANDesk Antivirus include:

- Symantec* Antivirus (versions 7, 8, 9, and 10)
- McAfee* Enterprise (versions 7.0, 8.0i, and 8.5)
- Trend Micro* PC-cillin 2004, 2005, and 2006
- Trend Micro OfficeScan
- Trend Micro ServerProtect
- eTrust* Antivirus (versions 6, 7, 7.1, and 8)

Configuring devices for LANDesk Antivirus

To configure devices with LANDesk Antivirus via an agent configuration

1. In the console, click **Tools | Configuration | Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, you must first click the **Start** page, and select the **LANDesk Antivirus** option.
4. Now you can access the options on the **LANDesk Antivirus** page.

5. Select an antivirus settings from the available list to apply it to the agent configuration you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.
6. Finish specifying settings for the agent configuration and then click **Save**.

If you want to install or update LANDesk Antivirus at a later time, you can do so with as a separate task from the Security and Patch Manager tool.

To install or update LANDesk Antivirus as a separate scheduled task

1. In the console, click **Tools | Security | Security and Patch Manager**.
2. Click the **Create a task** toolbar button, and then click **Install/Update LANDesk Antivirus**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show UI** option.
6. Select an antivirus settings from the available list to apply it to the task you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.
7. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during LANDesk Antivirus agent installation.
8. Click **OK**.

Removing LANDesk Antivirus from devices

If you want to remove LANDesk Antivirus from managed devices, you can also do that as a separate task from the Security and Patch Manager tool.

To remove LANDesk Antivirus

1. In the console, click **Tools | Security | Security and Patch Manager**.
2. Click the **Create a task** toolbar button, and then click **Remove LANDesk Antivirus**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show UI** option.
6. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during LANDesk Antivirus agent removal.

7. Click **OK**.

Updating virus definition files

LANDesk Antivirus lets you download the most current virus definition (pattern) files from the LANDesk Security web service's content servers. The LANDesk virus signature database is updated several times a day in order to ensure you have all of the latest known virus definitions so that you can protect your managed devices from these rapidly evolving threats.

You can download virus definition file updates from the console, either manually or as a regularly scheduled task that you create. You can specify where definition files are copied, whether they are stored in the default virus definition file repository where they are deployed to target devices or in a pilot test folder where they can be deployed to a limited scope of devices in order to test them before full deployment.

Deploying virus definition files to end user devices

The virus definition updates that you download can be deployed to end user devices remotely from the core server. From their own computer, users can also perform the task of updating virus definition files. By default they download files from their LANDesk core server. However, if they need to be able to download the latest virus definition updates while they're not connected to the network (for example, while traveling or using a laptop), you can provide the option of letting users download files directly from the LANDesk Security content server via an Internet connection.

To download virus definition file updates

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Download updates** toolbar button.
3. Select the update source site from the list of available content servers. Choose the one closest to your location.
4. Select **LANDesk Antivirus Updates** in the Definition types list. (You can select more than one definition type for a single download. However, you must have the corresponding depending on your LANDesk Security Suite content subscription. The more types you select, the longer the update will take.)
5. Select the languages whose content you want to update for the types you've specified.
6. If you want new content (content that does not already reside in any groups in the Security and Patch Manager tree) to automatically be placed in the Unassigned group instead of the default location, which is the Scan group, check the **Put new definitions in the Unassigned group** check box.
7. Click the **LANDesk Antivirus** tab to configure the download location, pilot test approval, automatic backups.
8. Select where you want virus definition files to be downloaded. Click Immediately approve if you want definitions to be downloaded to the default folder (\LDLogon\Antivirus\Bases folder on the core server) where they can be deployed to target devices. If you want to evaluate virus definition files before deploying them, you can select to do that with the pilot test option (you can also set an automatic approval time period to avoid having to do this manually after the test). If you choose to do a pilot test first, virus definition files are downloaded to a pilot test folder so that they are deployed to only those devices whose antivirus setting says to download the "pilot" version of definition files.
9. If you want to download the latest definition files right now, click **Get latest definitions**.

10. If you want to approve virus definitions currently residing in the pilot test folder, click **Approve now**. This moves definition files from the pilot test folder to the default folder (\LDLogon\Antivirus\Bases).
11. If you want to save the current contents of the Bases folder, check the **Make backups** option. You can restore definition file backups at anytime. Backups are useful if you want to revert to an earlier virus definition file version. (Virus definition file backups are saved in separate folders named by the date and time they were created, under: \LDLogon\Antivirus\Backups\)
12. Click **Apply** from any of the tabs at any time to save your settings.
13. Click **Update Now** to download your selected security content updates. The **Updating Definitions** dialog displays the current operation and status.
14. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the security and patch security content that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining security and patch content.

Note: Whenever virus definition files are updated on managed devices, a mini-scan of memory processes runs on the device. This scan is performed to ensure that the processes running in memory at the time of the update are still clean.

Scheduling automatic virus definition file updates

You can also configure virus definition file updates as a scheduled task to occur at a set time in the future, or as a recurring task.

To do this, configure security content download options in the **Update downloads** dialog, making sure to select LANDesk Antivirus updates in the definition type list on the **Updates** tab, configure virus definition file options on the **LANDesk Antivirus** tab, and then click the **Schedule Update** button. The **Scheduled update information** dialog shows task-specific settings for the task. Click **OK** to create a Download Security and Patch Content task in the Scheduled Tasks window, where you can specify the scheduling options.

Task-specific settings and global settings Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other tabs of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global setting it is effective for all security content download tasks from that point on.

Evaluating virus definition files with a pilot test

You may want to first evaluate virus definition files before deploying them to all of your managed devices. You can easily do this by specifying on the LANDesk Antivirus tab to restrict virus definition file updates to a pilot test folder, and then applying an antivirus setting with the **Download pilot version of virus definition files** option selected.

To run a pilot test of virus definition files

1. On the **Download update** dialog's **LANDesk Antivirus** tab, click **Restrict them to a pilot test first**.
2. If you don't want to have to manually move tested virus definition files from the pilot test folder to the default folder (\LDLogon\Antivirus\Bases), click **Automatically approve**, specify the minimum time period. When this time period elapses, the virus definition files are automatically approved and moved.
3. To download the most recent virus definition files from the LANDesk Security content server, click **Get latest definitions**.
4. To immediately approve the virus definition files currently residing in the pilot test folder, click **Approve now**.
5. Next, create a pilot test antivirus setting that allows you to deploy antivirus definition files to a limited set of testing machines. On the antivirus setting's **Virus definition file updates** tab, select **Download pilot version of definition files**.
6. Apply that pilot test antivirus setting to an antivirus scan task (see Creating an antivirus scan task below) that you can use to target your limited set of test machines. Observe the antivirus scan activity and results on these devices in order to evaluate the effectiveness of the downloaded virus definition files before deploying them to a wider audience.

Backing up virus definition files

If you want to save older versions of downloaded virus definition files, use the **Virus definition backups** settings on the **LANDesk Antivirus** tab.

Backing up virus definition files can be very useful if you need to go back to an older virus definition file to scan and clean specific infected files, or to restore a virus definition file that resolved a particular problem.

Virus definition file backups are saved in separate folders, named by the date and time the files were saved, under the parent \LDLogon\Antivirus\Backups\ folder.

Scanning devices for viruses

This section provides information on scanning managed devices for known viruses as well as suspicious objects.

Scanning requires the proper content subscription

Remember that in order to scan for a specific security content type, including viruses, you must have the corresponding LANDesk Security content subscription. For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Scanning methods

There are several different methods of running an antivirus scan on managed devices that have LANDesk Antivirus installed:

- Scheduled antivirus scan
- On-demand antivirus scan

- User-initiated antivirus scan
- Real-time file protection
- Real-time email protection

Running a scheduled antivirus scan from the console

From the console, you can configure antivirus scan tasks that can be run as either an on-demand scan or as a scheduled task or policy from the core server.

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

To create an antivirus scan task

1. Click **Tools | Security | Security and Patch Manager**.
2. Make sure virus definition files have been updated recently.
3. Make sure the default virus definition file folder (\LDLogon\Antivirus\Bases) contains only those definitions you want to scan for.
4. Click the **Create a task** toolbar button, and then click **LANDesk Antivirus scan**.
5. Enter a name for the scan.
6. Specify whether the scan is a scheduled task or a policy-based scan, or both.
7. If you want to scan ALL of your managed devices with LANDesk Antivirus agent installed, select a scheduled task, and then select to target all LANDesk Antivirus devices. You can also select to start the antivirus scan of all LANDesk Antivirus devices immediately.
8. Select an antivirus setting from the available list (or create a custom setting for this scan by clicking the **Configure** button), to determine how the scanner operates on end user devices. If you want the antivirus scan to use the device's local antivirus setting (default settings), select that option from the drop-down list. For more information about configuring the antivirus scan with an antivirus setting, see "About the Antivirus settings dialog" on page 653.
9. If you want to ensure that the scan uses the latest known virus definition files, check the **Update virus definitions** option.
10. Click **OK**. (For a typical scheduled task scan, click **OK**, and then add target devices and configure the scheduling options in the Scheduled tasks tool.)

Running an on-demand antivirus scan from the console

You can also run an immediate (red-button) antivirus scan on one or more target devices.

To do this, right-click the selected device (or up to 20 multi-selected devices), click **LANDesk Antivirus scan now**, select an antivirus setting, choose whether to update virus definition files before scanning, and then click **OK**.

When you click OK, the **Status of requested actions** dialog displays the following information:

- Progress
- Results
- Scan time information

Running an antivirus scan at a managed device

Additionally, if you've configured antivirus settings to display the LANDesk Antivirus icon in the device system tray, end users can perform their own on-demand antivirus scans.

To do this at the managed device, right-click the **LANDesk Antivirus** taskbar icon, and then select **Scan my computer**. Or from the LANDesk Antivirus dialog, click **Scan my computer**.

Enabling real-time antivirus protection (file, email)

Real-time antivirus protection provides ongoing background scans of specified files, file types, email messages, and email attachments, based on known virus definitions. You can also enable real-time notification to inform end users about infected files.

Real-time file protection, email scanning, and notification are all configured with antivirus settings.

LANDesk Antivirus system tray icon indicator

When real-time antivirus protection is enabled, the LANDesk Antivirus system tray icon (on the end user device) is yellow. When real-time protection is disabled, the icon is gray.

Real-time file protection

Configure real-time file protection with the options on the **Real-time protection** tab of the **Antivirus settings** dialog. For more information, click **Help**.

When real-time protection is running, files are scanned for viruses every time the file is:

- Opened
- Closed
- Accessed
- Copied
- Saved

Real-time email scanning

Configure real-time email scanning with the **Enable email scanning option** on the **General** tab of the **Antivirus settings** dialog.

Real-time email protection provides an ongoing scan of incoming and outgoing messages. LANDesk Antivirus scans the message body as well as attached message's bodies and file attachments.

LANDesk Antivirus real-time email protection supports:

- Microsoft Outlook

When real-time email protection is running, messages and attachments are:

- Scanned when opened or previewed
- Not scanned when selected

When an infected email is discovered on a managed device, LANDesk Antivirus attempts to clean it. If it can be cleaned: a new header is placed in the message body to inform the end user. If the infected email can't be cleaned: the entire message body is deleted and replaced with a new header.

When a suspicious email message is discovered, the message body is converted to plain text and a header is added to the message.

Also, a dialog displays on the end user device that shows:

- File path
- File name
- Virus name
- Note telling the end user to contact their network administrator

Real-time (infected file) notification

End users can be notified when a file infected by a virus is detected, quarantined, deleted, skipped, or cleaned.

Configure real-time infected file notification with the option on the **Real-time protection** tab of the **Antivirus settings** dialog.

A dialog displays on the end user device that shows:

- File path
- File name
- Virus name
- Note telling the end user to contact their network administrator

Configuring antivirus scan options with antivirus settings

LANDesk Antivirus gives you complete control over how antivirus scans run on target devices, and which options are available to end users. For example, depending on the purpose or scheduled time of an antivirus scan, you may want to show the LANDesk Antivirus client on end user devices, allow the end user to perform antivirus scans, view and restore quarantined objects, download virus definition file updates on their own, etc. You can do this by creating and applying antivirus settings to a scan task.

Create and apply antivirus settings (a saved set of configured options) to antivirus scan tasks. You can create as many antivirus settings as you like. Antivirus settings can be designed for a specific purpose, time, or set of target devices.

With antivirus settings, you can configure the following options:

- Whether the LANDesk Antivirus icon appears in device system trays (providing end user access to antivirus scanning, quarantine and backup viewing, and file handling tasks)
- Real-time email scanning
- End user right-click scans
- CPU usage
- Setting owner (to restrict access)
- Scheduled antivirus scans
- Quarantine/backup folder size
- Restoring infected and suspicious objects
- Which files, folders, and file types to scan
- Scan exclusions
- Whether to use heuristic analysis for detecting suspicious files
- Whether to scan for riskware
- Real-time file protection (including which files to scan, heuristics, and exclusions)
- Downloading virus definition file updates (pilot test versions, scheduled downloads, end user download permission, and direct downloads from the LANDesk Security content server)

All of the antivirus settings you create are stored in the **LANDesk Antivirus** group located under **Settings** in the **Security and Patch Manager** tree view.

To create antivirus settings

1. In the Security and Patch Manager window, click the **Configure setting** toolbar button, and then click **LANDesk Antivirus settings**.
2. Click **New**. (Or, you can click **Edit** or **Configure** on any of the task dialogs that let you apply an antivirus setting.)
3. Enter a name for the antivirus setting.
4. Specify the settings on the tabs as desired for the particular task. For more information about an option, click **Help**.

Once configured, you can apply antivirus settings to antivirus scan tasks (or to a change settings task).

Changing device default antivirus settings

A device's default antivirus settings are deployed as part of the initial agent configuration. When a specific task has a different antivirus setting associated or assigned to it, the default settings are overridden. You can also choose to use the device's default settings by selecting it when you create a task.

At some point you may want to change these default antivirus settings on certain devices. Security and Patch Manager provides a way to do this without having to redeploy an entirely new and complete agent configuration. To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button. The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing antivirus setting as the default or use the Edit button to create a new antivirus setting as the default for target devices.

Viewing device antivirus settings in the Inventory

You can discover and/or verify device antivirus settings in their Inventory view.

To do this, right-click the selected device, click **Inventory | LANDesk Management | AV Settings**.

Configuring which files to scan (infectable files only, exclusions, heuristics, riskware)

You can specify which files (items) you want to scan which files you don't want to scan with both antivirus scans and real-time antivirus file protection.

See the following sections for information on customizing what to scan:

- "All files or infectable files only" on page 487
- "Excluding items from antivirus scans and real-time protection" on page 489
- "Using heuristic analysis to scan for suspicious objects" on page 489
- "Scanning for riskware (extended database)" on page 489

All files or infectable files only

Configure to scan all files or infectable files only on the **Virus scan** and **Real-time protection** tabs of an antivirus setting.

- **All files:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean.

Infectable file types

Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned.

Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files. See below for a list of infectable file types by the file format's standard or original file extension.

- ACM
- ACV
- ADT
- AX
- BAT

- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

Excluding items from antivirus scans and real-time protection

You can also specify what not to scan for with both antivirus scans and real-time file protection. Configure antivirus scan exclusions by adding files, folders, and file types to the exclusion list on the **Virus scan** and **Real-time protection** tabs of an antivirus setting.

Trusted Items list on managed devices

Note that you can also enable an option that allows end users to specify files and folders they don't want to be scanned by LANDesk Antivirus. This feature is called the trusted items list, and is configured on the **General** tab of an antivirus setting.

Using heuristic analysis to scan for suspicious objects

You can enable heuristic analysis to check for suspicious (possibly infected) files with both antivirus scans and real-time file protection.

Enable heuristic scanning on the **Virus scan** and **Real-time protection** tabs of an antivirus setting.

Heuristic analysis scanning attempts to detect files suspected of being infected by an unknown virus (not defined in the virus signature database) by looking for suspicious behavior. Suspicious behavior can include a program that is self-modifying, immediately tries to find other executables, or that is modified after terminating. A heuristic analysis emulates program execution to make protocols of observed suspicious activity, and uses those protocols to identify possible virus infections. In almost all cases, this mechanism is effective and reliable, and rarely leads to false positives.

LANDesk Antivirus utilizes a heuristic analyzer to verify files that have already been scanned by an antivirus scan based on known virus definitions.

Note that heuristic scanning may negatively affect performance on managed devices.

Scanning for riskware (extended database)

LANDesk Antivirus lets you enable scanning for risky software, also known as riskware, on target devices. Risky software is essentially client software whose installation presents a possible but not definite risk for the end user.

For example: adware, proxy-programs, pornware, remote admin utilities, IRC, dialers, activity monitors, password utilities, and Internet tools such as FTP, Web, Proxy and Telnet.

When you specify to scan managed devices for risky software, LANDesk Antivirus loads an extended database that contains definition files used to perform the scan. The extended database scan requires more time than the standard antivirus scan.

Additional notes about scanning files

- **System restore point scanning:** LANDesk Antivirus will scan the files in any system restore point folders that may exist on the managed device.

What happens on a device during an antivirus scan

This section describes how LANDesk Antivirus displays on end user devices with LANDesk Antivirus installed and what happens when devices are scanned for viruses by an antivirus scan or through real-time virus protection. Possible end user options are listed as well as the actions end users can take when an infected object is discovered by the scan.

LANDesk Antivirus client interface and end user actions

If the **Show LANDesk Antivirus icon in the system tray** option is checked on the device's antivirus setting, the LANDesk Antivirus client appears and shows the following elements:

System tray icon

- Real-time protection is enabled (system tray icon is yellow) or disabled (system tray icon is gray)

LANDesk Antivirus window

- Real-time protection is enabled or disabled (If the option is enabled in antivirus settings, the end user can disable real-time protection for as long a period of time as you specify)
- Email scanning is enabled or disabled
- Latest scan (date and time)
- Scheduled scan (date and time)
- Scan engine version number
- Virus definitions (the last time pattern files were updated)
- Quarantine (shows the number of objects that have been quarantined. End users can click **View details** to access the Quarantined objects dialog. If the option is enabled, end user can also restore files. If the password requirement option is enabled, the end user must enter that password.)
- Backup (shows the number of objects that have been backed up)
- Trusted items (shows the items the end user has added to their trusted items list that won't be scanned for viruses or risky software)

End user actions

If LANDesk Antivirus is installed on their computer, and their antivirus settings (default or task-specific) allow, users can perform the following tasks:

- Scan my computer (can view scan status, and pause and cancel the scan)
- Right-click to perform antivirus scan on files and folders in Windows Explorer (if the option is enabled by the antivirus setting)
- View local scheduled antivirus scans tasks
- Create local scheduled antivirus scans on their own machine (if the option is enabled by the antivirus setting).
- Update virus definition files
- Temporarily disable real-time protection (if the option is enabled by the agent configuration, and limited to a specified period of time)
- View quarantined objects
- View backup objects
- View trusted items
- Restore suspicious objects (if the option is enabled by the antivirus setting)
- Restore infected objects and risky software (if the option is enabled by the antivirus setting)
- Add and remove files and folders\subfolders to their trusted items list

Note that end users can't configure antivirus scan settings, or disable email scanning.

When an infected object is detected

This process applies to both infected files and email messages.

The infected object is:

1. Automatically backed up. (The backup file is saved in \LDClient\Antivirus\ folder, with a *.bak extension.)
2. An attempt is made to clean the infected object.
3. If the infected object can be cleaned, it is restored to its original location.
4. If the infected object can't be cleaned, it is quarantined. (The virus string is removed and the file is encrypted so it can't be run. The quarantined file is saved in \LDClient\Antivirus\ folder, with a *.qar extension.)

If the corresponding option is enabled in their antivirus setting (default or task-specific), end users can restore, delete, and rescan quarantined objects.

Automatic scanning of quarantined files

When an on-demand antivirus scan is executed, or when the virus definition files are updated, the antivirus scanner automatically scans objects in the quarantine folder to see if any infected files can be cleaned with the current virus definition files.

If a quarantined file can be cleaned, it is automatically restored and the user is notified.

End users can open a backup file to see a header that provides information on the original file location, and the reason for the file being backed up.

Note that only the original user is allowed to delete or modify backup files. The user that is logged in when the infected file is discovered.

Viewing antivirus activity and status information

If the antivirus scanner discovers any of the selected virus definitions on target devices, this information is reported to the core server. You can use any of the following methods to view detected security data after running a scan.

For antivirus information throughout your network, click the **Antivirus activity** toolbar button in Security and Patch Manager. The window displays antivirus activity and status information by the following categories:

- Infections by computer
- Infections by virus
- Computers not recently scanned
- Computers with recent antivirus activity

Additionally, for a scanned device, right-click the device, select Security and Patch Information, in the Type drop-down list select Antivirus. You can view:

- Missing antivirus updates
- Installed antivirus updates
- Purge repair history

Using antivirus alerts

You can configure antivirus alerting so that you can be notified when specific antivirus events are detected on managed devices in your system. LANDesk Antivirus uses the standard LANDesk alerting tool.

To configure antivirus alerting

Antivirus alert settings are found on the **LANDesk Antivirus** tab of the **Alert settings** dialog.

You must first configure the antivirus alerts in the Alert Settings tool in the console. Antivirus alerts include:

- An alertable antivirus action failed
- An alertable antivirus action succeeded
- Virus outbreak alert (per virus)

The following antivirus events can generate antivirus alerts:

- Virus removal failed
- Virus removal succeeded
- Quarantine failed
- Quarantine succeeded
- Deletion failed
- Deletion succeeded

Select which alerts you want generated. The time interval option lets you prevent too many alerts. More than one alert (for any antivirus trigger) during the specified time interval is ignored.

You can view the complete antivirus alert history for a device in its Security and Patch Information dialog. Right-click a device, select Security and Patch Information, select the Antivirus type in the Type drop-down list, and then select the Antivirus History object.

Generating antivirus reports

LANDesk Antivirus is represented by several antivirus-related reports in the Reports tool. These reports provide a variety of useful information for scanned devices on your network.

In order to access the Reports tool, and generate and view reports, a LANDesk user must have either the LANDesk Administrator right (implying full rights) or the specific Reports right.

Antivirus reports can be copied, removed, exported, and so on from the My Reports and User Reports groups. Antivirus reports are located in the Reports tool window, under the Security and Patch Manager group.

Running and publishing reports

You can run any report from the Reports window. From the Reports window, right-click the report you want to run, and then click Run (or, click the Run toolbar button). The report data displays in the Report View.

You can also publish reports to a secure file share where they can viewed by any user you've given the proper access credentials.

For more information about using the Reports tool, and a complete listing of the Security and Patch Manager reports with descriptions, see [Managing Reports](#).

Viewing antivirus information in the Web console executive dashboard

You can also view antivirus scan information in the Executive Dashboard. This data is useful in identifying virus outbreaks and to show antivirus protection over time.

LANDesk Antivirus-specific widgets show:

- Top five viruses detected (in the past 10 days or weeks)
- Managed devices infected with viruses (in the past 10 days or weeks)
- Percentage gauge of managed devices with real-time protection enabled
- Percentage gauge of managed devices with up-to-date virus definitions

LANDesk Host Intrusion Prevention System

LANDesk® Host Intrusion Prevention System, or LANDesk HIPS, is a security management tool that adds an extra layer of protection to your managed devices. LANDesk HIPS gives administrators the ability to protect their systems from known and unknown malware attacks before they contaminate systems on their enterprise network.

LANDesk HIPS enhances LANDesk Antivirus by proactively monitoring processes, and detecting and preventing malicious zero-day attacks. HIPS constantly and continuously monitors specified files, applications, and registry keys to prevent unauthorized behavior. You can control which applications run on devices and how they are allowed to execute. Unlike vulnerability detection and remediation, spyware detection and removal, or antivirus scanning, HIPS protection does not require patch file, definition/pattern file, or signature database updates. LANDesk HIPS provides non-stop security, based on customized settings that meet your environment and requirements.

The LANDesk Host Intrusion Prevention (HIPS) tool window and features are accessed from the main LANDesk console (**Tools | Security | Host Intrusion Prevention System**). The LANDesk HIPS tool lets you create LANDesk HIPS agent installation, update, and removal tasks; configure HIPS settings that can be deployed to target devices you want to protect; and customize HIPS display/interaction settings that determine how HIPS appears and operates on managed devices, and which interactive options are available to end users. You can also view HIPS activity and status information for protected devices.

This chapter introduces the LANDesk HIPS security management tool. You'll find an overview, step-by-step instructions on how to use LANDesk HIPS features, as well as corresponding online help sections that describe the LANDesk HIPS tool's dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog.

Read this chapter to learn about:

- "LANDesk HIPS overview" on page 495
 - "Supported device platforms" on page 496
 - "Role-based administration with LANDesk HIPS" on page 497
 - "LANDesk HIPS task workflow" on page 497
- "Configuring devices for LANDesk HIPS protection" on page 498
- "Protecting managed devices with LANDesk HIPS" on page 500
- "Configuring LANDesk HIPS protection options with HIPS settings" on page 501
- "What happens on a device configured with LANDesk HIPS" on page 508
- "Viewing HIPS activity information" on page 509

LANDesk HIPS overview

HIPS stands for Host-based Intrusion Prevention System. LANDesk HIPS provides another layer of protection on top of antivirus, anti-spyware, patch management and Windows firewall configuration to prevent malicious activity on your machine. Because it is a rule-based system, instead of a definition-based system, it can be more effective at protecting systems against zero-day attacks (malicious exploitation of vulnerable code before patches are available).

LANDesk HIPS protects servers and workstations by placing software agents between applications and the operating system's kernel. Using predetermined rules based upon the typical behavior of malware attacks, these systems evaluate activities such as network connection requests, attempts to read or write to memory, or attempts to access specific applications. Behavior known to be good is allowed, behavior known to be bad is blocked, and suspicious behavior is flagged for further evaluation.

HIPS proactive security features

- Provides kernel-level protection against applications that would attempt to modify binaries (or any files you specify) on your machine or application memory of running processes. It will also block changes to certain areas of the registry and can detect rootkit processes.
- Uses memory protection against buffer-overflow and heap exploits.
- Executes protection schemes to keep an attacker from building and executing code in a data segment.
- Watches for unauthorized or unusual file access.
- Offers real-time protection for your computer without relying on signature databases.

LANDesk HIPS offers the following system-level security:

- Kernel-level, rule-based file-system protection
- Registry protection
- Startup control
- Detection of stealth rootkits
- Network filtering
- Process and file/application certification
- File protection rules that restrict actions that executable programs can perform on specified files

HIPS client features

The LANDesk HIPS client gives administrators a powerful new tool for controlling what applications run on enterprise desktops and servers, and how those applications are allowed to execute.

HIPS client software uses proven heuristic and behavior-recognition techniques to recognize typical patterns and actions of malicious code. For example, a file that attempts to write to the system registry could be blocked and flagged as potentially malicious. The LANDesk HIPS client uses a variety of proprietary techniques to reliably detect malware even before a signature has been identified.

HIPS console features

LANDesk HIPS provides administrators with the ability to define and manage separate profiles for different user groups: HIPS settings accommodates the needs of any and all user groups by allowing administrators to create multiple, highly flexible configurations for different user profiles. Each HIPS setting can include custom password protection, WinTrust handling, protection mode, custom whitelists, network and application access control policies, file certifications, and file protection rules.

Supported device platforms

LANDesk HIPS supports many of the same desktop and server platforms supported by LANDesk Security Suite's scan and remediation capabilities and the standard LANDesk-managed device platforms, including the following operating systems:

- Windows 2000 SP2
- Windows 2003
- Windows XP SP1
- Windows Vista 32-bit

LANDesk HIPS is not supported on core servers or rollup cores

You should not install/deploy LANDesk HIPS to a core server or a rollup core. However, you can deploy LANDesk HIPS on an additional console.

Other system requirements

Make sure the managed devices you want to configure with the LANDesk HIPS protection meet the following system requirements:

- LANDesk HIPS is supported on (is compatible with) LANDesk Antivirus and Symantec Antivirus (Enterprise versions) only. Compatibility means that LANDesk HIPS will not interfere with antivirus processes such as scans, real-time protection, etc.
- Do NOT deploy LANDesk HIPS to devices with any other antivirus solution/product installed.

LANDesk HIPS Licensing

In order to access the LANDesk HIPS tool you must first activate your core server with a LANDesk HIPS license.

For information about LANDesk HIPS licensing, contact your LANDesk reseller, or visit the LANDesk Web site.

Role-based administration with LANDesk HIPS

LANDesk HIPS, just like Security and Patch Manager, uses LANDesk's role-based administration to allow users access to the LANDesk HIPS features. Role-based administration is LANDesk's access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each LANDesk user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see Role-based administration.

A LANDesk Administrator assigns these rights to other users with the Users tool in the console. LANDesk HIPS introduces one new role and corresponding right to role-based administration. The right is called Host Intrusion Prevention System, which appears in the User Properties dialog. In order to see and use LANDesk HIPS features, a LANDesk user must be assigned the necessary right.

The HIPS right provides users the ability to:

- See and access the Host Intrusion Prevention System (HIPS) tool in the console's Tools menu and Toolbox
- Configure managed devices for HIPS protection
- Manage HIPS settings (password protection, signed code handling, action, protection mode, file certifications, file protection rules, etc.)
- Deploy HIPS install or update tasks, and change settings tasks
- View HIPS activity for protected devices
- Define HIPS data threshold settings for recording and displaying HIPS activity throughout the network

LANDesk HIPS task workflow

The steps below provide a quick summary outline of the typical processes or tasks involved in implementing HIPS protection on your LANDesk network. All of these procedures are described in detail in subsequent sections.

Basic steps in implementing and using LANDesk HIPS:

1. Configuring managed devices for HIPS protection (i.e., deploying the LANDesk HIPS agent to target devices).
2. Configuring HIPS options, such as: signed code handling, protection mode, whitelists (applications allowed to execute on devices), file certifications, file protection rules, and end user interactive/options, with HIPS settings.
3. Discovering file/application behavior on devices with the HIPS learn mode.
4. Enforcing HIPS protection on managed devices with the HIPS automatic (block) mode.
5. Viewing HIPS activity for protected devices.

Configuring devices for LANDesk HIPS protection

Before managed devices can be protected from zero-day attacks, they must have the LANDesk HIPS agent installed. You can do this either during initial device agent configuration or with a separate installation/update task.

Configuring devices for LANDesk HIPS

To configure devices with LANDesk HIPS via an agent configuration

1. In the console, click **Tools | Configuration | Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, you must first click the **Start** page, and select the **Host Intrusion Prevention** option under **Security**.
4. Now you can access the options on the **Host Intrusion Prevention System** page.
5. Select a HIPS setting from the available list to apply it to the agent configuration you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. HIPS settings determine whether the LANDesk HIPS client is password protected, WinTrust signed code handling, action on programs added to system startup, buffer overflow protection, operating mode, whitelists, file certifications, and file protection rules.
6. Finish specifying settings for the agent configuration and then click **Save**.

If you want to install or update LANDesk HIPS at a later time, you can do so with as a separate task from the HIPS tool in the console.

To install or update LANDesk HIPS as a separate task

1. In the console, click **Tools | Security | Host Intrusion Prevention**.
2. Click the **Create a task** toolbar button, and then click **Install/Update LANDesk HIPS**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show UI** option.
6. Select a HIPS settings from the available list to apply it to the agent configuration you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. HIPS settings determine whether the LANDesk HIPS client is password protected, WinTrust signed code handling, action on programs added to system startup, buffer overflow protection, operating mode, whitelists, file certifications, and file protection rules.
7. Select a Scan and repair settings from the list to apply its reboot configuration (only) to the agent configuration you're creating. As with the HIPS settings option above, you can create a new setting or edit an existing setting by clicking **Configure**. Keep in mind that **ONLY** the reboot options specified on the Scan and repair settings you select are used by this agent configuration's LANDesk HIPS agent deployment to target devices. You can use an existing Scan and repair settings that already includes the reboot configuration you want, or you can create a brand new Scan and repair settings specifically for your LANDesk HIPS deployment.
8. Click **OK**.

The section below describes the fields in the dialog referenced by the tasks above.

About the Install or update LANDesk HIPS task dialog

Use this dialog to create and configure a task that installs the LANDesk HIPS agent on target devices that don't yet have it installed, or updates the existing version of the LANDesk HIPS agent on target devices that already have it installed.

The LANDesk HIPS installation is executed by the Security and Patch Manager tool's security scanner.

This task lets you conveniently deploy and update a managed device's LANDesk HIPS agent (and associated settings) without having to redeploy a full agent configuration.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Show UI:** Indicates whether the security scanner dialog displays the progress of the LANDesk HIPS agent installation\update on target devices.
- **LANDesk HIPS settings:** Specifies HIPS settings associated with this particular LANDesk HIPS agent installation. Select a setting from the drop-down list. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Host Intrusion Prevention settings dialog" on page 502.
- **Scan and repair settings (reboot only):** Specifies the scan and repair settings associated with this particular LANDesk HIPS agent installation. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during LANDesk HIPS agent installation.

Removing LANDesk HIPS from devices

If you want to remove LANDesk HIPS from managed devices, you can also do that as a separate task from the HIPS tool in the console.

To remove LANDesk HIPS

1. In the console, click **Tools | Security | Host Intrusion Protection**.
2. Click the **Create a task** toolbar button, and then click **Remove LANDesk HIPS**.
3. Enter a name for the task.
4. Specify whether the installation is a scheduled task or a policy-based task, or both.
5. If you want to display the installation progress in the security scanner dialog on target devices, check the **Show UI** option.
6. Select a scan and repair settings from the available list to apply its reboot configuration to the task you're creating. You can create a new setting or edit an existing setting by clicking **Configure**. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during LANDesk HIPS agent removal.

7. Click **OK**.

About the Remove LANDesk HIPS task dialog

Use this dialog to create and configure a task that removes the LANDesk HIPS agent from target devices.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Show UI:** Indicates whether the security scanner dialog displays the progress of the LANDesk HIPS agent removal from target devices.
- **Scan and repair settings:** Specifies the scan and repair settings associated with this particular LANDesk HIPS agent removal task. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during agent removal.

Protecting managed devices with LANDesk HIPS

LANDesk HIPS can run in either automatic blocking mode where all HIPS violations are blocked, or in learn mode.

Using the HIPS learn mode

Below is a description of the HIPS learn mode process:

- In learn mode, HIPS learns what kind of applications are installed on the device, how they behave, and their rights (privileges).
- HIPS monitors activity on the device and records information in an action history file.
- Action history data is sent from the device to the core server.
- Administrators read the action history to see which applications are doing what on the device (The files/applications and associated rights listed in the action history file (XML) are displayed in the File certifications page of the HIPS settings dialog.)
- Then administrators can customize HIPS settings to allow and deny privileges for relevant applications.

Learn mode can be applied to managed devices generally allowing HIPS violations to occur until a new HIPS settings is deployed, or learn mode can be applied initially for a specified period of time in order to discover what applications are run and their behavior and to create a whitelist (applications allowed to execute on devices). If the general protection mode is automatic blocking, you can still use learn mode to discover application behavior and then re-enforce automatic blocking mode once the learning period has expired.

Note that both the core server and the managed device must be operating in learn mode in order for the action history communication to take place.

Configuring LANDesk HIPS protection options with HIPS settings

LANDesk HIPS gives you complete control over how LANDesk HIPS operates on target devices, and which options are available to end users.

You can create and apply HIPS settings to a HIPS installation or update task or to a change settings tasks. You can create as many HIPS settings as you like. HIPS settings can be designed for a specific purpose, time, or set of target devices.

All of the HIPS settings you create are stored in the **Application Certification** group located under **Settings** in the **Host Intrusion Prevention** tree view.

See the following sections for information on creating and managing HIPS settings:

- "Creating and using HIPS settings" on page 501
- "Changing device default HIPS settings" on page 507
- "Viewing device HIPS settings in the Inventory" on page 507

Creating and using HIPS settings

To create HIPS settings

1. In the Host Intrusion Prevention window, click the **New settings** toolbar button. (Or, you can click **Configure Settings | New**.)
2. At the Settings page, enter a name for the HIPS settings, and then specify the general requirements and actions. For information about an option, click **Help** (see below).
3. At the Mode configuration page, select whether you want to enforce HIPS automatic blocking protection mode, or learn mode. You can also select to create a whitelist (applications allowed to execute on devices) based on the current certified files, and if you want the whitelist generation to run for a specified period of time initially and then re-enforce automatic blocking mode or continue using learn mode. Note that if you select learn mode as the general protection mode and want to generate a whitelist, the enforce automatic mode option is disabled. For information about an option, click **Help** (see below).
4. At the File certifications page, add, modify, or delete file certifications. For information about an option, click **Help** (see below).
5. At the File protection rules page, add, modify, prioritize, or delete file protection rules. LANDesk HIPS includes a predefined (default) set of protection rules. For information about an option, click **Help** (see below).
6. At any of the HIPS settings pages, click **Save** at any time to save your configured options for the HIPS setting, or click **Cancel** to exit the dialog without saving the setting.

Once configured, you can deploy HIPS settings to target devices by applying the HIPS installation/update tasks (or to a change settings task).

About the Configure HIPS settings dialog

Use this dialog to manage your LANDesk HIPS settings. Once configured, you can apply HIPS settings to agent configuration tasks, LANDesk HIPS install or update tasks, and change settings tasks.

HIPS settings determine whether the LANDesk HIPS client is password protected, availability of interactive options to end users, signed code handling, operating mode, and file certifications.

This dialog contains the following options:

- **New:** Opens the LANDesk HIPS settings dialog where you can configure the HIPS options.
- **Edit:** Opens the LANDesk HIPS settings dialog where you can modify the selected setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename. This is useful if you want to make minor adjustments to settings and save them for a specific purpose.
- **Delete:** Removes the selected setting from the database. (Note the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.)
- **Close:** Closes the dialog without applying a setting to the task.

About the Host Intrusion Prevention settings dialog

Use this dialog to create and edit a HIPS setting. When creating HIPS settings, you first define the general requirements and actions, and then add specific file certifications. You can create as many HIPS settings as you like and edit them at any time.

If you want to modify the device default HIPS settings without reinstalling the LANDesk HIPS agent or redeploying a full agent configuration, make your desired change to any of the options on the HIPS settings dialog, assign the new setting to a change settings task, and then deploy the change settings task to target devices.

Once configured, you can apply HIPS settings to install or update LANDesk HIPS tasks (and to change settings tasks).

The **HIPS settings** dialog contains the following pages:

- "About the HIPS Settings page" on page 502
- "About the HIPS Mode configuration page" on page 503
- "About the HIPS File certifications page" on page 504
- "About the HIPS File protection rules page" on page 505

About the HIPS Settings page

Use this page to configure the general requirements and actions for the HIPS settings.

This page contains the following options:

- **Name:** Identifies the HIPS setting with a unique name. This name appears in the LANDesk HIPS settings drop-down list on a Install or update LANDesk HIPS task dialog.
- **Administrator password:** Specifies the password required on devices configured with this HIPS settings in order to perform certain actions on the protected device. Actions requiring a password include: accessing the LANDesk HIPS client interface, installing unsigned software, authorizing HIPS violations, unloading LANDesk HIPS, erasing the local report, and switching the HIPS operating mode.
- **Password confirmation:** Ensures password accuracy.
- **WinTrust:** Determines how rights are provided to digitally signed software. An executable file that is digitally signed by its publisher is considered trusted, and will show this digital signature in its file properties dialog. HIPS allows rights to digitally signed software based on the option you select from the list below.
 - **Don't check for signed code**
 - **Automatically allow signed code**
 - **Automatically allow signed code from these vendors**
- **Action: When a program is added to the system's startup:** Determines the action taken when a program is added to the startup. This provides a second line of defense for authorizing processes in the system startup folder. HIPS monitors the contents of startup and if it finds a new process, it performs the action you select from the list below.
 - **Alert and prompt for action**
 - **Simply log in report, without alert**
 - **Remove from startup, without alerting**
- **Allow end user to stop HIPS service:** Lets the end user stop the HIPS service on their machine.
- **Use buffer overflow protection:** Allows you to protect devices from system memory exploits that take advantage of a program or process that is waiting on user input.
- **Set as default:** Assigns this setting as the default setting for tasks that use HIPS settings.
- **ID:** Identifies this particular setting. This information is stored in the database and can be used to keep track of each settings.
- **Save:** Saves your changes and closes the dialog.
- **Cancel:** Closes the dialog without saving your changes.

About the HIPS Mode configuration page

Use this page to configure the operating mode for LANDesk HIPS protection.

This page contains the following options:

- **Protection mode:** Specifies HIPS behavior when security violations occur on managed devices.
 - **Automatic:** All HIPS security violations are automatically blocked. In other words, all of the file certification rules you've created for specific files are enforced. If you select automatic blocking mode and also want to use the whitelist feature, you can apply either of the whitelist modes below (enforce or learn).

- **Learn:** All security violations (software and system modifications) are allowed, but are monitored and recorded in an action history file. Additionally, all of the applications that are run on the device are learned, and can be added to the device whitelist (allowed applications) by using the whitelist learn option below. Use this mode of operation to discover application behavior on a specific device or set of devices, and then use that information to customize your HIPS policies before deploying them and enforcing HIPS protection throughout the network. In contrast with automatic mode, if you select learn mode and also want to use the whitelist feature, only the learn mode is applicable.
- **Whitelist**
 - **Use certified files as a whitelist: Creates a whitelist (allowed applications) based on the current files whose certification has the allow execution option enabled.**
 - **First-time learn mode:** Allows the administrator to specify a period of time during which the end user can run any of the applications on their machine. During this period, HIPS observes or learns which applications are run. The administrator can use the options below to specify which HIPS operating mode is in effect after that time period expires: either enforce regular automatic mode of operation where only certified files are allowed to execute OR let the device continue to run in learn mode where all applications are allowed to execute and are automatically added to the certified files whitelist.
- **Security model devices:** Specifies the HIPS protection mode for a subset of devices that are configured with the same HIPS settings. You can use this feature to observe or learn software and system modifications and which applications are run on a limited group of devices. For example, you could use the same HIPS setting with the protection mode set to Automatic blocking mode, but identify a few target devices that you want to learn from by adding those machines to the security model devices list with their protection mode set to Learn.

About the HIPS File certifications page

Use this page to view and manage file certifications. File certifications are a set of rights (privileges or authorizations) that allow and deny certain actions that can be performed BY an application on managed devices.

This page contains the following options:

- **Certified files:** Lists the files that have certification rights configured for LANDesk HIPS.
- **Add:** Opens a file explorer dialog where you can browse and select a file you want to configure with file certifications.
- **Configure:** Lets you edit the selected file's certifications.
- **Delete:** Deletes the selected file and its certifications.

About the HIPS Configure file certification dialog

Use this dialog to configure certifications for a specific application file.

This dialog contains the following options:

- **File name:** Identifies the application file that is being assigned certifications.

- **Full path:** Specifies the location of the file.
- **File size:** Specifies the size (in KB) of the file.
- **File date:** Indicates the creation date and time of the file.
- **Version:** Indicates the version number of the file, if available.
- **Certified:** Indicates the date and time the file's certifications were created or last modified.
- **MD5 hash:** Shows the file's MD5 hash. A hash file is used to ensure the integrity of the file.
- **Description:** Provides a text box for you to enter a description of the file.
- **Bypass all protection:** Allows the application file complete privileges. The file is completely unfiltered and unmonitored.
- **Bypass buffer overflow protection:** Allows you to bypass buffer overflow protection. You will want to use this option for files (processes) that are certified and that you trust.
- **System security**
 - **Modify executable files:** Allows the application the right to modify other executable files.
 - **Modify protected files:** Allows the application the right to modify protected files. You can generate a list of protected files, such as the LANDesk device agents.
 - **Modify protected registry keys:** Allows the application the right to modify protected registry keys. Protected keys prevent malware infections
- **Network security**
 - **Send emails:** Allows the application to send email messages. (**Note:** LANDesk HIPS recognizes standard email client applications and automatically certifies them so that they can send emails.)
- **Files on disk**
 - **Add to system startup:** Allows the application the right to add files to the system startup.
 - **Allow execution:** Allows the application (process) to run on the device. Certified files are automatically have allow execution enabled. Also, if a file's certification provides partial rights, then the allow execution option is automatically enabled.
- **Advanced security rules**
 - **Protect application in memory:** Enforces protection for the application as it is running in memory. The application is protected from termination or modification.
 - **Inherit to child processes:** Assigns the same file certifications (rights) to any subordinate processes executed by this application. For example, you can use with a setup or installation executable to pass the same rights to subsequent processes launched by the setup program.
 - **Authorized installer:** Indicates that the application is allowed to perform software installation or deployment. This is the case for LANDesk software distribution tool, and can be applied to other software distribution applications as well.
- **Lock file certification (authorizations will not be updated via learn mode):**
- **OK:** Saves the file certifications and adds it to the list of certified files in the main HIPS settings dialog.
- **Cancel:** Closes the dialog without saving the file certifications.

About the HIPS File protection rules page

Use this page to view, manage, and prioritize file protection rules. File protection rules are a set of restrictions that prevent specified executable programs from performing certain actions ON specified files. With file protection rules, you can allow or deny access, modification, creation, and execution by any program on any file.

This dialog contains the following options:

- **Protection rules:** Lists all of the predefined (default) file protection rules provided by LANDesk, as well as all of the file protection rules that you've created.
 - **Rule name:** Identifies the file protection rule.
 - **Restrictions:** Displays the specific actions by programs on files that are restricted by the file protection rule.
 - **Apply rule to:** Displays the executable programs that are protected by the protection rule.
- **Move Up \ Down:** Determines the priority of the file protection rule. A file protection rule higher in the list takes precedence over a rule that is lower in the list. For example, you could create a rule that restricts a program from accessing and modifying a certain file or file type, but then create another rule that allows an exception to that restriction for one or more named programs. As long as the second rule is higher in the list of rules, it will take effect.
- **Reset:** Restores the predefined (default) file protection rules that are provided by LANDesk.
- **Add:** Opens the Configure file protection rule dialog where you can add and remove programs and files and specify the restrictions.
- **Configure:** Opens the Configure file protection rule dialog where you can edit an existing file protection rule.
- **Delete:** Removes the file protection rule from the database.

Note: File protection rules are stored in the FILEWALL.XML file, located in:
ProgramFiles\Landesk\ManagementSuite\ldlogon\AgentBehaviors\Hips_Behavior.ZIP.

About the Configure file protection rule dialog

Use this page to configure file protection rules.

This dialog contains the following options:

- **Rule name:** Identifies the file protection rule with a descriptive name.
- **Apply rule to**
 - **All programs:** Specifies that all executable programs are restricted from performing the actions selected below on the files specified below.
 - **Programs named:** Specifies that only the executable programs in the list have the restrictions selected below applied to them.
 - **Add:** Lets you choose which programs are restricted by the file protection rule. You can use filenames and wildcards.
 - **Edit:** Lets you modify the program name.
 - **Delete:** Removes the program from the list.
- **Restrictions**
 - **Deny access:** Prevents the programs specified above from accessing the protected files.
 - **Deny modification:** Prevents the programs specified above from making any changes to the protected files.
 - **Deny creation:** Prevents the programs specified above from creating the files.
 - **Deny execution:** Prevents the programs specified above from running the protected files.
- **Exceptions**

- **Allow exceptions for certified programs:** Allows any of the executable programs that currently belong to your list of certified files to bypass the restrictions associated with this file protection rule.
- **Files**
 - **Any files:** Specifies that all files are protected from the programs specified above according to their restrictions.
 - **Files named:** Specifies that only the files in the list are protected.
 - **Add:** Lets you choose which file or files are protected by the rule. You can use filenames or wildcards.
 - **Edit:** Lets you modify the file name.
 - **Delete:** Removes the file from the list.
 - **Apply to sub-directories too:** Enforces the file protection rules to any subdirectories of a named directory.

Changing device default HIPS settings

The device default HIPS settings are deployed as part of the initial agent configuration.

At some point you may want to change these default HIPS settings on certain devices. LANDesk HIPS provides a way to do this without having to redeploy an entirely new and complete agent configuration. To do this, use the **Change settings** task located in the drop-down list of the **Create a task** toolbar button. The dialog that appears allows you to enter a unique name for the task, specify whether it is a scheduled task or policy, and either select an existing HIPS setting as the default or use the Edit button to create a new HIPS setting as the default for target devices.

About the Create change settings task dialog

Use this dialog to create and configure a task that changes the default settings on target devices for LANDesk HIPS services.

With a change settings task you can conveniently change a managed device's default settings (which are written to the device's local registry) without having to redeploy a full agent configuration.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **HIPS settings:** Specifies the HIPS settings associated with this particular change settings task. Select the HIPS settings you want to deploy to target devices, modify an existing settings by selecting the settings and clicking **Edit**, or create a new settings by clicking **Configure | New**.

Viewing device HIPS settings in the Inventory

You can discover and/or verify device HIPS settings in their Inventory view.

To do this, right-click the selected device, click **Inventory | LANDesk Management | Host Intrusion Prevention**.

What happens on a device configured with LANDesk HIPS

LANDesk HIPS client enables signatureless, behavior-based intrusion prevention on managed devices.

This section describes how LANDesk HIPS displays on managed devices with LANDesk HIPS installed, what happens on end user devices when they are being protected by LANDesk HIPS, and the actions end users can take when a security violation is discovered.

LANDesk HIPS client interface and user actions

Once LANDesk HIPS has been deployed to managed devices, the LANDesk HIPS client can be accessed through either the **Start** menu or the system tray icon.

Administrator password protection

If the administrator has enabled the password protection option in the HIPS settings, the correct password must be entered in order to access and use HIPS client features.)

System tray icon

The system tray icon shows whether HIPS is running in learn mode or automatic blocking mode.

End users can right-click the HIPS icon to access its shortcut menu and select the following options:

- **Open:** Opens the LANDesk HIPS client.
- **Options:** Displays the HIPS options that have been configured by the administrator at the console (ready-only).
- **Automatic mode:** Enables LANDesk HIPS to run in automatic mode where all predefined security violations are blocked.
- **Learn mode:** Enables LANDesk HIPS to run in learn mode where all security violations are allowed, but are monitored and recorded in an action history file.
- **Install software:** Opens a file explorer window where the end user can select an installation or setup program to run.
- **Unload:** Lets the end user uninstall LANDesk HIPS from their machine.

LANDesk HIPS client and end user actions

The LANDesk HIPS client displays in a window that includes the following elements:

- View the activity log.
- View the HIPS options that have been configured by the administrator at the console (read-only).

- On the **Status** page: View HIPS client information, current operating mode, and activity occurring on the client. Change the operating mode (automatic or learn).
- On the **Activity** page: View running applications and their authorizations. Select programs and view all of their authorizations or kill the process. Modify display options.
- On the **Startup** page: View and edit the contents of the system startup. Also, services running on the client and Internet Explorer extensions.
- On the **Protection** page: View program access rights and folder protections. Create, edit, and delete file protection rules, and change rule priority in the ordered list.
- On the **Certifications** page: View programs with special file certifications. Add and delete file certifications.

Viewing HIPS activity information

If HIPS detects violations to its rules and certification rights, this information is reported to the core server. You can use the following methods to view detected HIPS activity.

For information about HIPS activity throughout your network, click the **HIPS activity** toolbar button in the LANDesk HIPS tool. The window displays HIPS activity by the following categories:

- Preventions by computer
- Preventions by application
- Preventions by action

You can also view specific host intrusion activity at the bottom of the window, including the following details:

- Action Date
- Action
- Description
- Application
- File version
- File size
- File date
- Mode
- MD5 hash

About the Host Intrusion Prevention activity dialog

Use this dialog to view detailed HIPS activity for all of your managed devices with the LANDesk HIPS agent. This data is used to generate the LANDesk HIPS reports available in the **Reports** tool.

To customize the scope and focus of data that is displayed, click **Thresholds** and change the time period threshold for storing HIPS activity information in the core database, and for the number of items to display in the HIPS activity window lists.

You can also right-click a device in this view to access its shortcut menu and directly perform available tasks.

This dialog contains the following options:

- **Refresh:** Updates the fields in the dialog with the latest HIPS information from the database.
- **Thresholds:** Opens the **Threshold settings** dialog, where you can define the duration (in days) for storing HIPS data in the core database and the number of items to display in the HIPS activity lists.
- **Purge:** Completely and permanently removes HIPS activity data from both this display window and the core database.
- **Preventions by computer:** Lists devices in the right pane on which HIPS violations were discovered. Select a device to see the specific violations..
- **Preventions by application:** Lists applications in the right pane that were discovered on managed devices. Select an application to see the devices it was discovered on.
- **Preventions by action:** Lists actions in the right pane that were taken on managed devices. Select an action to see the devices on which it was taken.

About the Threshold Settings dialog (for LANDesk HIPS)

Use this dialog to define time periods for HIPS activity that appears in the **HIPS activity** dialog.

- **Automatically delete HIPS activity older than:** Indicates the maximum number of days to keep reported HIPS activity for protected devices in the core database. You can specify 1 day to 999 days. However, we recommend that you carefully watch the amount of data being sent to the core and find an optimal number of days so that HIPS data doesn't use too much space or hamper performance.
- **When displaying results, truncate lists to:** Indicates the maximum number of entries to display in the lists in the HIPS activity dialog. You can specify 1 item to 999,999 items.

LANDesk Agent Watcher

LANDesk Agent Watcher allows you to proactively monitor the status of selected LANDesk agent services and files in order to ensure their integrity and preserve proper functioning of vital LANDesk services on managed devices. Agent Watcher can be enabled and agent watcher settings deployed with an initial device agent configuration. It can also be updated at anytime without having to perform a full agent configuration.

Agent Watcher not only monitors critical LANDesk services and files, but can also restart terminated services, reset services set to automatic startup, restore files that are pending delete on reboot, and report evidence of file tampering back to the core server.

Read this chapter to learn about:

- [LANDesk Agent Watcher overview](#)
- [Supported device platforms and system requirements](#)
- [Enabling, configuring, and disabling Agent Watcher monitoring](#)
- [About the Configure Agent Watcher settings dialog](#)
- [About the Agent Watcher settings dialog](#)
- [About the Update Agent Watcher settings dialog](#)
- [Using Agent Watcher reports](#)

LANDesk Agent Watcher overview

LANDesk Agent Watcher monitors LANDesk services and files specified by a device's agent watcher settings. Agent watcher settings also determine how often to check the status of agent services and files, whether Agent Watcher remains resident on devices, and whether to check for changes to the applied agent watcher setting itself.

By default, LANDesk Agent Watcher is turned off. You can enable LANDesk Agent Watcher with an agent configuration or, at a later time, with a separate Update Agent Watcher settings task. In other words, you don't have to enable Agent Watcher during a device's initial configuration. It can be done at any time directly from the console for one or more managed devices.

When monitoring services and files, agent watcher performs the recuperative actions listed below.

Monitoring LANDesk services and files

The following LANDesk agent services can be monitored:

- Local scheduler
- LANDesk Antivirus
- LANDesk Remote Control
- LANDesk Software Monitoring
- LANDesk Targeted Multicast
- LANDesk USB Monitor

Services you're not deploying should not be selected for Agent Watcher monitoring

When configuring agent watcher settings, don't select services you don't intend to install on target devices. Otherwise, the core server will receive alerts for services not being installed that weren't installed on purpose. However, note that even if a service that isn't installed is selected to be monitored, alerts are not sent saying that the service can't be restarted or that its startup type can't be changed.

When monitoring agent services, LANDesk Agent Watcher:

- Restarts services when they shut down (one time)
- Changes the service's startup type back to automatic when the startup type is changed
- Sends alerts to the core server when services are not installed
- Sends alerts to the core server when services cannot be restarted
- Sends alerts to the core server when a service's startup type cannot be changed back to automatic

The following LANDesk files can be monitored:

- Ldiscn32.exe
- Vulscan.dll
- Vulscan.exe
- Sdclient.exe
- Amclient.exe
- Usbmon.exe
- Usbmon.ini

When monitoring files, LANDesk Agent Watcher:

- Removes files from the registry that are scheduled for deletion upon reboot
- Sends alerts to the core server when the files are scheduled for deletion upon reboot
- Sends alerts to the core server when the files have been deleted

Supported device platforms and system requirements

LANDesk Agent Watcher supports most of the same platforms supported by Security and Patch Manager, including the following operating systems (listed with minimum software and hardware requirements):

- **Microsoft Windows XP 64 Bit Professional**
(Intel Pentium 64 Bit processor or compatible; 128 MB of RAM, more recommended; 72 MB available on HDD to install)
- **Windows 2000 Professional**
(SP2 and higher; 133 MHz Intel Pentium processor or compatible; 64 MB of RAM, 96MB recommended; 50 MB available on HDD to install)
- **Microsoft Windows XP Professional**
(Microsoft Internet Service Pack 2.0 or higher; 300 MHz Intel Pentium processor or compatible; 128 MB of RAM, more recommended; 72 MB available on HDD to install)

Enabling, configuring, and disabling Agent Watcher monitoring

The LANDesk Agent Watcher utility is installed with the standard LANDesk agent, but it is turned off by default. Agent watcher can be activated through the initial device agent configuration, or at a later time via an Update Agent Watcher settings task.

To enable LANDesk Agent Watcher during agent configuration

1. In the console, click **Tools | Configuration | Agent Configuration**.
2. Click the **New Windows** toolbar button.
3. After specifying your desired settings for the agent configuration, click **Agent watcher** to open that page on the dialog.
4. Check **Use Agent Watcher**.
5. If you want to check for changes to the applied agent watcher settings in order to ensure the target device's settings are current, select **Check for changes in selected configuration**, and then specify a time interval. This option automatically compares the current version of the selected Agent watcher settings with the one deployed to target devices (at the interval specified below). If the setting has been modified during that time span, the new agent watcher setting is deployed and Agent Watcher is restarted with the new settings.
6. Select an agent watcher setting from the available list to apply it to the agent configuration you're creating. You can create a new setting or edit an existing setting by clicking the **Configure**. The applied agent watcher setting determines which services and files are monitored and how often, and whether the Agent Watcher executable remains resident in memory on monitored devices.
7. Finish specifying settings for the agent configuration and then click **Save**.

If you want to activate Agent Watcher (or update settings) at a later time, you can do so for one or more managed devices directly from the console.

You can also disable Agent Watcher for one or more devices with the Update Agent Watcher task.

To enable LANDesk Agent Watcher (or update settings) as a separate task

1. In the console, right-click one or more devices, and then click **Update Agent Watcher settings**.
2. Check **Use Agent Watcher**.
3. If you want to check for changes to the applied agent watcher settings in order to ensure the target device's settings are current, select **Check for changes in selected configuration**, and then specify a time interval.
4. Select an agent watcher setting from the available list to apply it to the agent configuration you're creating. You can create a new setting or edit an existing setting by clicking the **Configure**. The applied agent watcher setting determines which services and files are monitored and how often, and whether the Agent Watcher executable remains resident in memory on monitored devices.
5. Click **OK**.

Once the **OK** button is selected, all the selected target devices are updated with the new settings, and a status message appears.

To disable LANDesk Agent Watcher

1. In the console, right-click one or more devices, and then click **Update Agent Watcher settings**.
2. Make sure the **Use Agent Watcher** checkbox is cleared
3. Click **OK**.

About the Configure Agent Watcher settings dialog

Use this dialog to manage your agent watcher settings. Once configured, you can apply agent watcher settings to managed devices through an agent configuration or a change settings task.

Agent Watcher allows you to create multiple settings that can be applied to devices or device groups.

This dialog contains the following options:

- **New:** Opens the Agent watcher settings dialog where you can configure the options.
- **Edit:** Opens the settings dialog where you can modify the selected agent watcher setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename.
- **Delete:** Removes the selected setting from the database.
- **Close:** Closes the dialog, without applying a setting to the task.

About the Agent Watcher settings dialog

Use this dialog to create and edit an agent watcher setting.

Agent watcher settings determine which services and files are monitored and how often, as well as whether the utility remains resident on the device. (The agent watcher can also be configured to automatically check for new settings by enabling the **Check for changes in selected configuration** option with an agent configuration.

This dialog contains the following options:

- **Name:** Identifies the setting with a unique name.
- **Alert watcher remains resident:** Indicates whether the LDRegwatch.exe (Agent Watcher executable) remains resident in memory all of the time. If you don't check this option, LDRegwatch.exe remains in memory only long enough to check the selected services and files at the scheduled time.
- **Monitor these services:** Specifies which critical LANDesk agent services will be monitored with this agent watcher setting.
- **Monitor these files:** Specifies which critical LANDesk agent services will be monitored with this agent watcher setting.
- **Interval to check:** Specifies how often you want Agent Watcher to monitor the selected services and files. The minimum setting for this interval is 30 seconds.

Services you're not deploying should not be selected for Agent Watcher monitoring

When configuring agent watcher settings, don't select services you don't intend to install on target devices. Otherwise, the core server will receive alerts for services not being installed that weren't installed on purpose. However, note that even if a service that isn't installed is selected to be monitored, alerts are not sent saying that the service can't be restarted or that its startup type can't be changed

About the Update Agent Watcher settings dialog

Use this dialog to update agent watcher setting changes on target devices, and to enable/disable the LANDesk Agent Watcher utility on target devices.

If Agent Watcher is not active on the selected workstations, check the **Use Agent Watcher checkbox**, configure the Agent Watcher settings, and then click **OK**. Agent Watcher will be activated after the configuration is pushed down to the selected devices. To change which files or services are monitored, click the **Configure** button to display the **Agent Watcher Settings** dialog.

With the Update Agent Watcher Settings dialog you can also deactivate the Agent Watcher by unchecking the **Use Agent Watcher** checkbox and clicking **OK**.

This dialog contains the following options:

- **Use Agent watcher: Enables the Agent watcher service on target devices.**
- **Check for changes in selected configuration:** Automatically compares the current version of the selected Agent watcher settings with the one deployed to target devices (at the interval specified below). If the setting has been modified during that time span, the new agent watcher setting is deployed and Agent Watcher is restarted with the new settings.
- **Interval to check:** Specifies the time period of the recurring comparison.
- **Choose an agent watcher setting:** Specifies which setting is used for the task. Select a setting from the drop-down list, or click **Configure** to create a new setting.

Once the **OK** button is selected, all the selected devices are updated with the new settings, and a status message appears.

Using Agent Watcher reports

Agent Watcher alerts that are sent from managed devices can be accessed via the **Reports** tool in the Management Suite console. Click **Tools | Standard Reports | Agent Watcher**.

All the Agent Watcher reports include the hostname of the workstation, the monitored service or file, the status of the alert (either found or resolved, and the date the event was discovered).

Agent Watcher saves the state of the alerts so that the core will only get one alert when the condition is found and one alert when the condition is resolved. Multiple alerts may occur when Agent Watcher is restarted in order to reboot the system, or when a new configuration is pushed or pulled down to the workstation.

Reports can also be generated for a given category based on different time intervals, such as: today, last week, last 30 days, or another specified interval.

Agent Watcher alert data automatically removed after 90 days

All Agent Watcher alerts over 90 days old are automatically removed from the database. Alert data is used to generate Agent Watcher reports.

Agent watcher reports

The five Agent Watcher reports are listed below:

Failed to change the service type

This report lists all the Agent Watcher alerts from workstations that are unable to change the startup type of a monitored LANDesk service.

LANDesk required services not install

This report lists all the Agent Watcher alerts from workstations where a monitored service has been uninstalled.

LANDesk required services not started

This report lists all the Agent Watcher alerts from workstations where a monitored service cannot be restarted by the Agent Watcher.

LANDesk files not found on clients

This report lists all the Agent Watcher alerts from workstations where monitored agent files have been deleted.

Pending delete files found on client

This report lists all the Agent Watcher alerts from workstations where the monitored agent files have been scheduled to be deleted upon reboot. Agent Watcher also automatically removes these files from the Windows registry so they will not be deleted.

Connection control manager

Connection control manager monitors and restricts I/O devices and network connections. You can restrict the network IP addresses that devices are allowed to connect with, and you can also restrict the use of devices that allow data access to the device, such as ports, modems, drives, and wireless connections.

For connection control manager (CCM) to function on a device, you must have the local scheduler agent and the standard LANDesk agent deployed on that device. Every time the device initiates a network/device connection or makes changes to a network/device connection, the connection control manager agent applies configuration rules. These rules include terminating connections that aren't allowed and sending alerts to the core server.

Unsupported platforms

Connection control manager is not supported on managed devices running the 64-bit version of Windows XP or Windows Vista

Use **Connection control configurations** to manage network connections. You can configure network restrictions in two general ways: by specifying which network addresses are allowed or by specifying which network addresses are blocked.

Use **Device control configurations** to manage USB, modem, I/O port, CD/DVD drive, PCMCIA, and network connections. You can configure USB restrictions by either generically blocking a whole class of USB devices, such as storage devices, or by using advanced settings to restrict certain USB devices based on information you specify.

Each connection control configuration that you define is saved and can be applied to the managed devices that you specify. You can save multiple configurations and apply them to different devices as needed. When you create a configuration, you must deploy it to devices for it to take effect. Connection control manager supports devices running Windows 2000, Windows Server 2003, and Windows XP.

Connection control manager is a component of LANDesk Security Suite

Connection control manager isn't available unless you have a LANDesk Security Suite license.

Read this chapter to learn about:

- "Using connection control configurations to restrict network access" on page 518
- "Using device control configurations to restrict USB device access" on page 521
- "Configuring advanced USB settings" on page 526
- "Deploying configurations" on page 528
- "Troubleshooting CCM" on page 529

Using connection control configurations to restrict network access

Use the connection control configurations to help limit networks on which a workstation may reside. The network connectivity may be disabled if a workstation does not reside on an allowed network.

A connection control on a managed device monitors connections through the network and connections using I/O devices. The connection control applies rules based on the items selected for the connection control configuration. These rules include terminating connections that are not allowed and sending alerts to the core server.

You can create multiple configurations and apply them to different managed devices. However, a managed device can have only one network configuration applied to it at a time.

Network restrictions are configured in two general ways:

- By specifying which network addresses are allowed. In this case, the device can only receive IP addresses that are within the range of addresses that are explicitly allowed.
- By specifying which network addresses are blocked. In this case, if any network device receives an IP address that is within the range of blocked addresses, the device is disabled.

I/O device restrictions can be applied in conjunction with the network restrictions that are selected. These restrictions can be placed on devices that allow data access, such as ports, modems, drives, and wireless connections. When a restriction is in effect, the device is disabled in Windows and cannot be accessed.

To create a connection control configuration

1. Click **Tools | Security | Connection control manager**.
2. In the lower pane, from the **Connection control configuration** option's shortcut menu, click **New connection control configuration**.
3. Enter a **Configuration name**.
4. Check **Limit connections to listed networks** and list the network addresses that are allowed. If devices can be connected to other networks when not connected to restricted network addresses, check **Allow unlisted networks if not connected**.

OR

- Check **Block connections to listed networks** and list the network addresses that aren't allowed.
5. Enter a range of IP addresses and click **Add**. Repeat as needed. To remove a range of IP addresses, select it from list and click **Remove**.
 6. To verify that a core server is running on the network that the device is connecting to, check **Verify core server existence on the network**. This option applies only if **Limit connections to listed networks** was selected.
 7. If you want, select a device control configuration that you want applied during connections to listed or unlisted networks.
 8. Click **Save** when done.

Verifying the core server's existence on a network

A range of IP addresses can sometimes be used by more than one network. For added security in restricting network access, you can ensure the core server is running on a network before a device is allowed to connect to that network.

Check the **Verify core server existence on the network** option to implement this added security. If no core server is found on the network being accessed, the connection will be disabled. Leave this option clear if you're confident that the network addresses in the access list are trusted, or if you prefer to reduce traffic on the network by not sending pings to the core server.

Allowing unlisted networks if not connected

Check the **Allow unlisted networks if not connected** box if you want to allow a device (such as a laptop to connect to an unlisted network) while it isn't connected to a network on the restricted list. Connection control manager ensures that the device only connects to listed networks or only to unlisted networks, but does not connect to both at the same time. The next time the device is connected to the network where the core server is running, an alert is sent from the device to the core server to notify the core server that a connection was made outside of the listed IP addresses.

If this option isn't checked, the device can connect only to listed network addresses.

Applying device configurations to network connections

You can apply device configurations to both listed and unlisted network connection types. If you check **Apply device configuration while connected**, you can select a configuration that connection control manager will apply to the managed computer. If you also check the **Allow unlisted networks if not connected** option, the configuration can apply to both listed and unlisted network connections, as long as you don't use the **Apply another configuration while on unlisted networks** option.

If you check both the **Allow unlisted networks if not connected** and the **Apply another configuration while on unlisted networks** options, you can specify a different configuration that only applies to computers that are connected to an unlisted network. You can specify configurations at the bottom of the **Connection control configuration** dialog. The options there are available once you check **Apply device configuration while connected** and/or **Apply another configuration while on unlisted networks**.

If you leave the configuration to apply at **None**, connection control manager won't apply a device control configuration while connected to the network. This means even if a device control configuration was active before a network connection, once a network connection happens, no device control configuration will be active, and all device access will be unrestricted.

If you select a configuration from the list, once a matching network connection is made, connection control manager will change the device control configuration on the computer to match your selection.

Device control configurations applied through a connection control configuration are applied to the computer, not the user. An active user-based device control configuration outranks a computer-based device control configuration. When there's an active user-based device control configuration, the device control configuration applied through a connection control configuration won't take effect. If you always want the device control configuration specified in a connection control configuration to be applied, make sure there aren't any user-based device control configurations on the computer.

Selecting a device control configuration to apply in the **Connection control configuration** dialog doesn't deploy that device control configuration to computers. Device control configurations and connection control configurations are deployed independently. Make sure you've deployed device control configurations that a connection control configuration refers to. If the configuration isn't available on a computer, the computer sends a Configuration Error Alert to the core server. You can see these alerts in the AMS alert log (**View | Alert history**).

About the Connection control configuration dialog

This dialog has these options:

- **Name:** The name for this configuration. This name appears in the main connection control manager window.
- **Limit connections to listed networks:** Only allows connections to the listed IP address ranges.
 - **Allow unlisted networks if not connected:** Allows connections to unlisted networks, but only if the device isn't already connected to a listed network.
 - **Apply device configuration while connected:** Applies the configuration you specify at the bottom of the dialog when users connect to a network.
 - **Apply another configuration while on unlisted networks:** Applies a different configuration when users connect to an unlisted network. Unlisted network connections must be allowed for this option to be available.
- **Block connections to listed networks:** Blocks connections to the listed IP address ranges.
- **Starting IP address:** The starting IP address for the range you want to control.
- **Ending IP address:** The ending IP address for the range you want to control.
- **Add:** Adds valid IP address ranges to the controlled list.
- **Remove:** Removes the selected IP address range from the controlled list.
- **Verify core server existence on the network:** A range of IP addresses can sometimes be used by more than one network. For added security in restricting network access, you can ensure that the core server is running on a network before a device is allowed to connect to that network. Check this option to implement this added security. If no core server is found on the network being accessed, the connection will be disabled.
- **Device configuration to apply while on listed networks:** If you checked **Apply device configuration while connected**, you can specify the configuration you want to apply.
- **Device configuration to apply while on unlisted networks:** If you checked **Apply another configuration while on unlisted networks**, you can specify the configuration you want to apply.

Using device control configurations to restrict USB device access

Connection control manager configurations can have two parts. The first part is the connection control configuration, where you limit network access. The secondary part, a device control configuration, is optional. The device control configuration service, usbmon, runs on managed devices, where it monitors and restricts USB and specified device connections.

Device control configurations are standalone, and you can deploy a device control configuration without deploying a connection control configuration.

By default, device control configurations can restrict the various types of devices. You can use the advanced USB settings to restrict any USB device or class of devices that you specify. Among the devices you can restrict are:

- USB devices such as drives, keyboards and mice, printers, and scanners
- RIM Blackberry*, Pocket PC*, and Palm* handheld devices
- Network volumes
- Bluetooth* Personal Area Networks
- Wireless 802.11x networks
- Modems
- PCMCIA* devices
- Serial, parallel, infrared, and FireWire 1394 ports
- Floppy and CD/DVD drives

The usbmon service can:

- Prevent the use of unauthorized USB and PCMCIA devices.
- Prevent the use of unauthorized removable storage devices.
- Trigger an external program or script when it detects an unauthorized device.

To create a device control configuration

1. Click **Tools | Security | Connection control manager**.
2. In the lower pane, from the **Device control configuration** option's shortcut menu, click **New device control configuration**.
3. Enter a **Configuration name**.
4. Select whether you want the profile to apply to the current **User** or all users on the **Computer**. For more information, see "Understanding profiles" on page 524.
5. Customize the options you want. For more information, see the next section that describes the options on the Device control configuration dialogs.
6. Click **Save** to save your profile.

Connection control manager stores device control configurations in the core server's LDLogon\usbmon folder. Device control configurations are .INI files named with the configuration name you specified.

About the Device control configuration dialog's General settings page

- **Name:** The name for this configuration. This name appears in the main connection control manager window.
- **Apply configuration to:**
 - **User:** Applies the configuration only to the user logged on at the time of deployment. For more information, see "Understanding profiles" on page 524.
 - **Computer:** Applies the configuration to all users on the device.
- **Commands:** Allows you to configure commands that run when an unauthorized device is detected. For more information, see "Configuring commands that run when an unauthorized device is detected" on page 527.

About the Device control configuration dialog's USB devices page

- **Make USB storage read only:** Specifies that users can read from but not write to a USB storage device with this configuration.
- **Use encryption:** Deploys a program (EncArchive.exe) that enables file encryption on target devices. Files are encrypted when written to a device and decrypted when read from the device. Access is allowed only with the correct password. You can use this encryption feature to provide additional protection for devices that contain confidential data.
- **Percentage of USB storage device to use for encryption:** Specifies the percentage of total space of a USB storage device that can be used for encrypted files.
- **Block USB devices: Allow the following:**
 - **Keyboard and mice:** Checking this allows USB keyboards and mice, and adds Service=hidusb to the USB rules list. For more information on the rules list, see "Configuring advanced USB settings" on page 526.
 - **Pocket PC's:** Checking this allows devices to sync with Pocket PC handhelds, and adds Service=wceusbsh to the USB rules list.
 - **Storage:** Checking this allows USB storage devices, and adds Service=usbstor to the USB rules list.
 - **Printers:** Checking this allows USB printers, and adds Service=usbprint to the USB rules list.
 - **Palm devices:** Checking this allows devices to sync with Palm handhelds, and adds Service=PalmUSB to the USB rules list.
 - **Scanners:** Checking this allows USB scanners, and adds Service=usbscan to the USB rules list.
 - **RIM Blackberry:** Checking this allows RIM Blackberries, and adds Service=RimUsb to the USB rules list.
 - **Biometric fingerprint reader:** Checking this allows biometric fingerprint readers, and adds Service=TcUsb to the USB rules list.

- **Allow password override of blocked devices:** Checking this option allows temporary access for a blocked device. Once the checkbox is checked, you can enter the password twice to confirm.

To access the password dialog on the client: In order to display the password dialog on a client, you must press the **CTRL + SHIFT + UP ARROW** key sequence on the client keyboard. You can then enter the password. If the password matches the one specified in the device control configuration, the blocked USB devices are now allowed access. To terminate access and restore the original access restriction, press the **CTRL + SHIFT + UP ARROW** key sequence again, and then click **End session**.

- **Notify user when unauthorized USB devices are detected:** Checking this displays a message box when a user connects an unauthorized USB device. For more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 527.
- **Advanced USB settings:** Displays the Device control advanced settings dialog, where you can see blocked devices and create your own rules to unblock devices. For more information, see "Configuring advanced USB settings" on page 526.

About the Device control configuration dialog's Volumes and network page

- **Block all unknown volumes:** Blocks access to any volume that wasn't present when the device control configuration was installed. Note that if a device containing a volume was attached when the configuration was installed, the usbmon service will allow that device in the future, even though it may be removable.
- **Notify user when unauthorized volumes are detected:** Checking this displays a message box when the usbmon service detects an unauthorized storage volume. For more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 527.
- **Block Bluetooth Personal Area Networks (PAN):** Blocks access to Bluetooth networks.
- **Block wireless LAN 802.11X:** Blocks access to wireless 802.11X networks.
- **Block wireless LAN 802.11X only when a wired connection exists:** Blocks access to wireless 802.11X networks when a wired connection exists.

About the Device control configuration dialog's Other devices page

- **Block modems:** Blocks modems.
- **Block PCMCIA devices, allow the following:**
 - **Network cards:** Checking this allows PCMCIA network cards.
 - **Storage:** Checking this allows PCMCIA storage cards.
- **Block all ports:** Checks/clears all blockable port options.
 - **Serial:** Blocks serial ports.
 - **Parallel:** Blocks parallel ports.
 - **Infrared:** Blocks infrared ports.
 - **FireWire 1394:** Blocks FireWire 1394 ports.
- **Block all drives:** Checks/clears all blockable drive options.
 - **Floppy:** Blocks floppy drives.

- **CD/DVD:** Blocks CD/DVD drives.
- **Make CD/DVD writers read-only:** Configures an internal or external CD and DVD writing/recordable device so that data can be read from it but not written to it.

Understanding profiles

The Device control configuration dialog has an **Apply configuration to** option, where you can select whether the configuration applies to either a **User** or the **Computer**. It's important to understand what is happening when you select each option:

- **User:** The current configuration will be applied to the logged in user. All previous configurations to other users and the device will stay the same.
- **Computer:** All users without a private user configuration will get this current configuration. If a particular user already had a configuration, the previous configuration stays active.

Unauthorized device handling

Device control configurations use the usbmon service on managed devices. When the usbmon service receives notification from the OS that a new USB or PCMCIA device has been inserted, the usbmon service applies a number of custom defined rules to decide whether or not the device is allowed. You can set up simple rules to allow only certain types of devices such as keyboards and mice, printers, and scanners. More complex rules might allow only secure storage devices of a given manufacturer, or exclude devices of a given manufacturer.

When an unauthorized device is detected, the usbmon service will:

- Remove the device from the Windows Device Manager so Windows won't see it any more. Any drivers for the device remain installed.
- In the case of an unauthorized USB device or volume, optionally display a configurable message to the user (for more information, see "Creating custom messages when unauthorized devices/volumes are detected" on page 527).
- Optionally load an external program (For more information, see "Configuring commands that run when an unauthorized device is detected" on page 527). For example, the external program can be a script that sends an alert to a central console.
- Send a "Disabled device activated" AMS alert to the core server. The alert message includes the device name.

Removable storage device handling

Usbmon is the name of the service on managed devices that restricts USB connections. When a new volume is mounted, the usbmon service receives notification from the operating system. The usbmon service then uses the GetDriveType() API call to check the type of drive that was mounted. If the OS describes the drive as "removable" or "fixed drive", the usbmon service will take action. The usbmon service also checks for removable volumes at boot time. If an unauthorized volume is found at boot time, the same actions are taken as when the volume is mounted later.

Drives that are considered removable include (but are not limited to) USB storage devices. CD drives (read-only or read/write) are not considered removable storage.

The OS doesn't consider hard drives as removable. The `GetDriveType()` call describes them as "fixed drive" even if they are attached via USB or some other external port. To allow removable hard drives to be handled the same as other removable storage devices, the usbmon service records the list of hard drives at the time the service is installed. For example, if a device has two hard drives (C: and D:) at the time the usbmon service is installed, the usbmon service will consider those drives as fixed and will not check them. But if at some later time a hard drive with drive letter E: is found, the usbmon service will consider it a removable device.

The usbmon service keeps the list of "fixed drives" in the registry at `HKLM\Software\LANDesk\usbmon\FixedDrives`. This list is created at the time the service is installed. The **Block all unknown volumes** option blocks access to any volume that wasn't present when the device control configuration was installed. Note that if a device containing a volume was attached when the configuration was installed, the usbmon service will allow that device in the future, even though it may be removable.

When a removable storage device is detected, the usbmon service will:

- Lock the volume. Users who attempt to access the volume will get an "access denied" error.
- Optionally display a configurable message to the user.
- Optionally load an external program. For example, the external program can be a script that sends an alert to a central console.
- Send a "Disabled device activated" AMS alert to the core server. The alert says a volume was activated, but additional information about the volume isn't available.

Blocking all unknown volumes works for Windows XP or Windows 2003 only

In Windows 2000, the operating system reports that the volume is blocked when it really isn't blocked. LANDesk recommends that for Windows 2000 you block specific devices in order to prevent the addition of new volumes.

What if a support person needs to use a USB memory stick?

If you're an IT support person and you want to use a USB storage device on a user's computer, there are several things you can do:

- The most convenient method of allowing access to a USB device on a temporary basis is to enable the password override option when defining and deploying a device control configuration to your managed devices. For more information, see the "About the Device control configuration dialog's General settings page" on page 522.

You can try the following methods if the device control isn't configured with the password override feature:

- Log on with admin rights and temporarily disable the usbmon service.
- Log on with admin rights, run the usbmon GUI and add the device to the list of authorized volumes.
- Use profiles. A device that is not allowed for the end user might be allowed when you log in on the same computer with your support account because you have a different usbmon profile.

Configuring advanced USB settings

Once connection control manager is installed on a device, the agent stores information about the last ten USB devices that it blocked access to. The inventory scanner sends this information to the core database. Information about these blocked devices then appears in the **Advanced USB settings** dialog. You can use this information to create advanced rules that allow or block specific USB devices. These advanced rules allow you to control more than just the basic device categories you see in the **Device control configuration** dialog.

In the **Advanced USB settings** dialog, you can base a rule on any of the six columns. Right-click on a value in the column and click **Allow** to create a rule that allows devices based on that attribute. The keywords created for each of the columns are the following:

```
DeviceDesc
HardwareID
Service
Mfg
LocationInformation
Class
```

These are the same names that are used in the registry under the HKLM\System\CurrentControlSet\Enum\USB key.

The most useful field to base rules on is usually **Service**. This corresponds to a Windows driver. For example, the driver for USB ActiveSync connections to Windows CE PDAs is called wceusbsh (see HKLM\CurrentControlSet\Services\wceusbsh). Any of the six columns can be used to base a rule on, however, it is up to you to decide which rules make sense for your situation.

Wildcards

You can use wildcards in rules, for example, the following would allow any device that has the string "floppy" in its device description:

```
DeviceDesc=*floppy*
```

Whitelist vs. Blacklist rules

All the rules illustrated so far have been whitelist rules, where devices are forbidden unless they satisfy at least one of the rules. The usbmon service also supports blacklist rules. Rules prefixed by a minus sign are blacklist rules. For example:

```
Service=usbstor
-DeviceDesc=*floppy*
```

The first rule allows USB storage devices. The second rule blacklists devices that have the string "floppy" in their device description.

If both whitelist and blacklist rules are defined, the usbmon service first checks devices against the whitelist rules. If there are no whitelist rules that allow the device, the device is forbidden. If there is at least one whitelist rule that allows the device, then the usbmon service checks the device against the blacklist rules. If the device satisfies none of the blacklist rules, it is allowed. Otherwise it is forbidden.

If only whitelist rules exist, a device is forbidden unless it satisfies one of the whitelist rules. If only blacklist rules exist, a device is allowed unless it satisfies one of the blacklist rules.

Composite rules

All the rules illustrated so far have been simple rules, where a single field is tested. Usbmon also supports composite rules, as in the following example:

```
Service=wceusbsh,DeviceDesc=*iPAQ*
```

This rule allows only Windows CE devices that have the string IPAQ in their device description.

Composite blacklist rules are also possible. Example:

```
Service=wceusbsh  
-Service=wceusbsh,Mfg=*iPAQ*
```

The above two lines allow Windows CE devices, except those that have the string IPAQ in their manufacturer field. The above lines are equivalent to the following single line:

```
Service=wceusbsh,-Mfg=*iPAQ*
```

Creating custom messages when unauthorized devices/volumes are detected

In the **Device control configuration** dialog, you can customize the message text that the user sees when unauthorized devices/volumes are detected. In the message text, you can use these placeholders to show information about the unauthorized volume or device:

- %vol%: volume serial number
- %desc%: description
- %service%: service
- %hwid%: hardware ID
- %mfg%: manufacturer
- %loc%: location
- %class%: class

Configuring commands that run when an unauthorized device is detected

When the usbmon service detects an unauthorized volume or device, it can execute external programs. You can include one or two placeholders in the commands:

- %1: will be replaced with either "volume" or "device", depending on whether an unauthorized volume or an unauthorized USB device was detected.
- %2: will be replaced with either the volume serial number of the unauthorized volume, or with the identification string of an unauthorized USB device.

For example, when a command such as the following is given:

```
wscript myscript.vbs %1 %2
```

This might cause the following command to be launched:

```
wscript myscript.vbs volume "1234ABCD"  
wscript myscript.vbs device "Y-E Data USB Floppy: Vid_057b&Pid_0000"
```

Usbmon guarantees that only one instance of the script will be running at the same time.

To configure commands

1. In a device control configuration, click **Commands**.
2. Enter the commands you want.
3. Click **OK**.

Configuring alerts

Connection control manager configurations use the alert management system for alerting (**Tools | Alert settings | Connection control manager**). Connection control manager can trigger alerts on these events:

- Configuration error
- Disabled device activated
- Restricted network connection attempted
- Unlisted network connection attempted
- Unlisted network session detected

Viewing the unauthorized device list

On each computer, connection control manager stores a list of the ten most recent unauthorized devices that were connected. You can view this information from the **Network view** by clicking **Inventory** on a device's shortcut menu. Then click **LANDesk Management | Connection control manager | Usbmon alert**.

Deploying configurations

Once you've created a connection control configuration or a device control configuration, you must deploy it to managed devices before it will be active.

To deploy a configuration

1. From the saved configuration's shortcut menu, click **Schedule**.
2. The configuration is added to the **Scheduled tasks** window. In this window, drag devices onto the configuration icon.
3. When all devices have been added, from the task's shortcut menu, click **Properties**. In the tree click **Schedule task**, and configure the scheduling options.

For more information on scheduling tasks, see "Scripts and tasks" on page 136.

When you schedule a device control configuration for deployment, connection control manager does the following:

- It creates an executable distribution package that's named after the source device control configuration. The package's primary file is `usbmon.exe`. Additional files are `usbmon.reg`, `devactalert.exe`, `netres.mrl`, and `<device control configuration name>.ini`.
- If you target users for the device control configuration task, connection control manager uses a public policy-based delivery method called "Usbmon Pull Delivery." If this delivery method doesn't exist, connection control manager creates it. When task targets are users, connection control manager has to use a policy-based delivery method to ensure that the correct user gets the configuration. When target users log on, the policy-based delivery method activates and installs the configuration.
- If you target computers for the device control configuration task, connection control manager uses a public policy-supported push delivery method called "Usbmon Push Delivery." If this delivery method doesn't exist, connection control manager creates it. Since the configuration targets a device, any user that logs into that device will get that device control configuration; it doesn't matter who is logged in when the configuration gets installed. You can use push or policy delivery methods for computers.

Once connection control manager creates the `usbmon` policy or policy-supported push delivery methods, you can customize them. As long as the method name doesn't change, connection control manager will use the modified delivery method.

For more information on creating device control configurations locally on managed computers and deploying those configurations manually, view the `usbmon` help file, `usbmon.chm` in the core server's LDMain share.

Troubleshooting CCM

This section contains information about some possible situations you might encounter with Connection control manager, and how to address them.

- Each new connection control configuration is saved as a configuration file and a script file in the following folders:
 - `ldmain\ccmgr\name.cfg`
 - `ldmain\scripts\name.ini`
- If a script or configuration already exists with the same name that you give a configuration, you'll be prompted to overwrite the existing script or configuration. This can cause an unrelated distribution script of the same name to be overwritten.

- When entering IP ranges for network restrictions, don't restrict access to the network range the core server is on. If clients access a restricted network and connection control manager disables network access, only communication with the core server can restore network access. If devices can't communicate with the core server because of a restriction, network access can't be restored.
- When restricting access to I/O devices, don't restrict I/O devices that host network adapters. If you restrict access to I/O devices that host a network adapter, that client will no longer be able to access the network. For example, restricting USB access prevents any USB network adapters from working. Without network access, you won't be able to update restriction settings for that client.
- If you select the following options in connection control manager, and the core server isn't available on a listed network, clients will have unrestricted I/O device access while on that network:
 - Limit connections to listed networks
 - Allow unlisted networks if not connected
 - Verify core server existence on the network
- If "Allow unlisted networks if not connected" is checked, and the agent can't find the core on a listed network, it will assume that the network is unlisted. At this point, unintended access may be granted to local I/O devices. This can create a security risk. Make sure the core server is available to prevent this from happening.

Asset manager add-on

LANDesk Asset Manager is a complete asset management solution that lets you record, track, and analyze any type of fixed asset within your organization; including IT assets like computers and monitors, office equipment, furniture, and any other valuable item you want to manage; in addition to critical business information such as contracts, invoices, and projects.

Asset Manager includes all the tools you need to configure data entry forms, enter items into the database with those forms, as well as collect and analyze that data with customizable reports.

For two of the predefined asset types, computers and software, Asset Manager also provides the capability to link and update asset data from the scanned inventory and SLM records.

Asset Manager is a Web-based application that runs in the LANDesk Web console. Note that Asset Manager is supported only in the Internet Explorer browser, and that Asset Manager is not accessible in the main Windows console.

Asset Manager is a separately licensed add-on component

Asset Manager is a separately purchased add-on product that integrates seamlessly with your current LANDesk network. If you haven't purchased or installed a LANDesk Asset Manager license, the user interface and the capabilities described here are not on your core server and will not be available from the Web console.

For information about purchasing an Asset Manager license, visit the LANDesk Web site.

For information about installing and activating the Asset Manager add-on product, refer to "Installing add-ons" in the *Installation and Deployment Guide*.

Read this chapter to learn about:

- [Asset Manager overview](#)
- [Using role-based administration with Asset Manager](#)
- [Accessing Asset Manager in the Web console](#)
- [Managing assets](#)
 - [Working with computer assets](#)
 - [Working with software assets](#)
- [Managing contracts](#)
- [Managing invoices](#)
- [Managing projects](#)
- [Managing global lists](#)
- [Using subgroups to organize types](#)
- [Creating new types](#)
 - [Using a details summary](#)
 - [Adding details](#)
 - [Adding detail tables](#)
 - [Managing detail templates](#)
 - [Adding detail templates](#)
 - [Organizing details in sections](#)
- [Using an item list](#)

- [Adding items to the database](#)
- [Using asset alert dates](#)
- [Associating items](#)
- [Importing items](#)
- [Exporting items](#)
- [Searching for items](#)
- [Using Asset Manager reports](#)

Asset Manager overview

Asset Manager adds easy-to-use features to the Web console that let you proactively manage all types of fixed (non-scannable) assets across your enterprise throughout the entire asset life cycle. In addition to physical assets, you can manage other relevant information such as contracts, invoices, and projects. If implemented and maintained properly, this type of information management can provide the security, access, and control of important data necessary to not only make informed business decisions and planning, but improve the productivity and efficiency of your organization's everyday business operations.

In short, Asset Manager helps you get the most out of your IT investments.

Linked data from the core database (for computers and software)

With Asset Manager, you can leverage existing data for computers and licensed software products that has already been scanned (via the inventory scanner or entered manually into your core database.)

Import and export capabilities

You can also use Asset Manager to import and export asset data to use with other data tracking and management applications and databases. The import and export features support both CSV (comma-separated value) and XML formatted files.

Other features and benefits

In addition to the features mentioned above, with Asset Manager you can:

- Use predefined types (i.e., data entry forms) or create your own custom types that are used to add items to the database.
- Store asset management data in a single repository; the core database. A single database simplifies data management, ensures data accuracy and integrity, and allows multiple users to enter asset data and generate reports at the same time.
- Associate assets with each other and with other related information, such as invoices, users, service histories, etc.
- Set up alert dates to automatically notify you when an asset's pre-established deadline expires.
- Use predefined asset management reports or create your own custom reports.

- Reconcile recorded asset data with actual physical inventories.
- Track asset data history.

Understanding Asset Manager types and details

Asset Manager uses types and details to describe the kinds of items (and their inherent properties) that can be added into the database. A *type* simply represents a specific kind of asset, contract, invoice, project; and so on. And a *detail* represents specific information about that type. To understand this concept in practical terms, it's probably helpful to think of a type as essentially a data entry form (made up of details for a particular kind of item), and each detail as an individual data field on the form.

Asset Manager has several predefined asset types, contract types, invoice types, project types, and global list (i.e., universally applicable) types, each defined by its own unique combination and arrangement of details. However, you're not limited to these types or details. With Asset Manager, you can also create and modify your own custom types, details, detail tables, and detail templates in order to meet your asset management requirements and goals. You're able to determine the content and layout of a data entry form, what type of information is being asked for, whether a data field is required, and more.

Ultimately, the purpose of asset types and details is to give you a way to configure data entry forms that you then fill out in order to add items to the database.

Using role-based administration with Asset Manager

Role-based administration is LANDesk's access and security model that lets LANDesk Administrators restrict access to tools and devices. Each user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see *Using role-based administration in the Users Guide*.

Role-based administration can also be implemented to control access to features in the Web console, including the Asset Manager tool. To learn more about how role-based administration works for the basic Web console interface and tools, see *Using the Web console in the Users Guide*.

Asset Manager introduces three new roles and corresponding rights to role-based administration. An administrator assigns these rights to other users with the Users tool in the main console (see the *Users Guide* for details). In order to see and use the various Asset Manager features in the Web console, a user must be assigned the necessary Asset Manager right, as described below.

Note: In addition to users that have only one of the rights below, a user could have both the Asset Data Entry and Reports rights. Since Asset Configuration gives full access to Asset Management, any combination with it would be redundant.

Asset Configuration

The Asset Configuration right is an administrator-level right that provides users the ability to:

- See and access all the Asset Management links in the Web console: Assets, Contracts, Invoices, Projects, Global Lists, Detail Templates, and Reports.
- See and access the new Asset Access link. Administrators can control user access to view and edit asset information by creating filters based on global list types and their details.
- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset Data Entry

The Asset Data Entry right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global Lists links in the Web console.
- Browse types and details (can't add, edit or delete them)
- Add items to the database by filling in data entry forms
- Edit items that have been added to the database

Reports

The Reports right for asset management-specific reports is the same Reports right that allows users to generate and view all other reports in the main console. This right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, Global Lists, and Reports links in the Web console.
- Browse types, details, and items (can't add, edit or delete them)
- Run predefined Asset Manager reports
- Create and run custom asset reports
- Edit all report configurations
- Print all reports

Asset management workflow

The following steps provide a quick summary outline of the typical processes involved in implementing an asset management strategy on your LANDesk network. Each of these tasks is described in detail in the appropriate sections of this chapter.

Basic steps in implementing and using asset management:

1. Managing types (viewing, organizing, editing, and deleting with the Assets, Contracts, Invoices, Projects, and Global Lists pages.)

2. Creating types (i.e., data entry forms with the Add new type page.)
3. Creating details (i.e., data fields for types with the Add details page. Also, adding detail tables and detail templates to types.)
4. Adding items to the database by filling out data entry forms.
5. Importing and exporting asset items.
6. Using predefined and custom reports to collect and analyze asset data.

Accessing Asset Manager in the Web console

Asset Manager is a browser-based application that is accessed through the Web console (note that Asset Manager is supported only in the Internet Explorer browser). Asset Manager features and interface do not appear at all in the main Windows-based console. In order to use Asset Manager, you must already have the Web console software installed on either your core server or on another Web server on your network.

For more information about the Web console

For information on installation prerequisites and procedures for the Web console, see *Installing the Web console* in the *Installation and Deployment Guide*.

For more information on logging in to the Web console and using the default Web console features, see *Using the Web console* in the *Users Guide*.

Users with a valid Web console account can access Asset Manager in the Web console from any Windows-based computer running Internet Explorer* 5.5 or later.

To access Asset Manager in the Web console

1. From a networked computer, open Internet Explorer.
2. In the Address field, enter the URL to the site hosting the Web console pages. Normally the URL is: `http://webservername/remote`.
3. Once you authenticate, an Asset Manager link appears in the left navigation pane. Clicking on this link will open Asset Manager in its own browser window, with features displayed based on the user's role based administration rights.

What's next?

Now that you have a basic understanding of what you can do with Asset Manager and have logged into the Web console, you can click any of the Asset Management links and start using the features introduced in this overview section.

Online help

From any page in the Web console, including Asset Manager pages, click the Help link in the upper right corner to access online context-sensitive help for that page.

Managing assets

The Assets page shows all the asset groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Assets are defined as IT items or property that can't be scanned by the inventory scanner into the core database but that you want to track and manage, such as printers, monitors, phones, desks, supplies, etc. The exception to this definition are the computer and software types (see below for an explanation about these two special asset types). There's no limit to the number or variety of IT assets you can record with Asset Manager.

Asset *types* represent the data entry forms used to enter asset items into the database. You can use the predefined asset types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as [by global lists](#).
- Create, edit, and delete subgroups by clicking the [Manage subgroups](#) link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- [Search for types](#) in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its [details summary page](#).
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- [Create new types](#) in a subgroup by clicking the **Add Type** link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- [View a list of all the items](#) that have been added to the database for a particular type by clicking the type name.
- [Add items to the database](#) by clicking the plus sign (+ **Add** link) and filling out the data entry form.

The predefined asset groups and types include:

Miscellaneous

- Chair
- User

Office Equipment

- Copier
- Digital Camera
- Fax
- Mobile Phone
- Phone
- Projector
- Television

Technology

- Computer
Important: Computer is a special asset type because it contains linked data that can be updated and synchronized with inventory data in the core database. The computer asset type can't be deleted or renamed. For more information, see [Working with computer assets](#).
- Monitor
- PDA
- Printer
- Router
- Scanner
- Software
Important: Software is a special asset type because it contains linked data that can be updated and synchronized with inventory data. The software asset type can't be deleted or renamed. For more information, see [Working with software assets](#).
- Switch

Working with computer assets

The computer type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated computer type details are linked to a scanned device's hardware inventory (a scanned or managed device is one on which the product inventory scanner has been run). The other asset type with linked details that can be updated with information from the core database is the software type.

You can use linked details to populate linked data fields for computers that have already been scanned and have an inventory record. For computers that aren't yet connected to your network or haven't yet been scanned by the inventory scanner, you can manually add computer items in Asset Manager (using a valid MAC addresses or serial number provided by the manufacturer), and populate the other linked data fields after the machines have been scanned.

The computer asset type can't be deleted or renamed.

Linked details for computers

Only designated computer details are linked and can be updated from a scanned computer's hardware inventory. These details are identified by the linked-chain icon. Linked details can't be deleted, and you can't create your own linked details.

The following computer details are linked:

- Device ID

Important: The Device ID linked detail can be thought of as the master link because it is used to definitively identify each specific computer asset in the hardware inventory, ensure there are no duplicate records, and synchronize the appropriate linked data for each computer asset. Device ID is listed as a Hidden information type in the computer details summary page, and only its Default value and Summary fields can be edited manually.

- Machine name
- Manufacturer
- MAC address
- Serial number
- Model
- Asset tag
- Domain name
- Description
- Notes
- Last hardware scan date
- Primary owner (the user who has logged in to a device the most times within a specified number of logins. The default number of logins is 5.)

All other details for the computer type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with inventory information. Once a computer's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the inventory as many times as you like.

Non-linked data fields can always be edited in Asset Manager. Non-linked data does not appear in a scanned device's inventory tree.

Updating linked data for computers

You can update all of your scanned computers at once from the computer item list page (this may take a long time depending on how many managed devices you have in the core database). Or, you can update linked data for an individual computer from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see [Using the asset inventory update utility](#).

To update the computer item list

1. From the Assets page, open the **Technology** subgroup, and then click **Computer** to view all the computer assets currently recorded in the database.
2. Click the **Refresh asset data** link located above the computers list.

Scanned devices that do not have a corresponding computer item on this page are added to the list, with their linked data fields filled in. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

If a corresponding computer item already exists on this page, its linked data is refreshed/updated from the scanned device's inventory. If the information has changed in the inventory, the new information replaces the value in the linked data field. Only linked data fields are updated.

To update linked data for one computer item

1. From the computer item list page, edit the computer by clicking its pencil icon.
2. Click the **Refresh asset data** link located above the details list.

The computer's linked data is updated with information from the corresponding scanned device's inventory. This process rewrites any manually entered or changed value in a linked data field with the current value in the inventory. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

From a specific computer's page, you can also click the **Open inventory data** link located above the details list to view the scanned device's entire inventory tree.

Note: If the Open inventory data option is not available on a computer's page, it indicates the corresponding device has been deleted from the hardware inventory. When a device is deleted from the inventory, its asset record is not removed from Asset Manager.

Using the asset inventory update utility

When you install the Asset Manager add-on, an utility executable is copied to the LDMain folder on the core server (the LANDesk\ManagementSuite folder). This utility provides the convenience of being able to refresh all of the computer and software license asset data that currently resides in the core database at once, either manually or as a scheduled task at a specific time. In other words, you don't have to perform this task via the computer or software item list pages in the Web console's Asset Manager pages.

The name of the executable file is:

LANDesk.ManagementSuite.AssetManagement.InventoryUpdate.exe

You can run this utility by any of the following methods:

- Double-click the executable file
- Run the executable from a command line interface
- Create a Windows Scheduled Task that runs this executable. Note this is NOT a LANDesk Scheduled Task.

To create a Windows Scheduled Task to update refresh computer and software asset data

1. At the core server, click **Start | Programs | Accessories | System Tools | Scheduled Tasks**.
2. Click **Add Scheduled Task** to open the Scheduled Task wizard, and then click **Next**.
3. Use the **Browse** button to locate and select the utility executable (named above in the ManagementSuite folder), and then click **Next**.
4. Enter a name for the task, select the frequency when the task should be performed, and then click **Next**.
5. If necessary, select the time and day when the task should be performed, and then click **Next**.
6. Enter the user name and password for a valid LANDesk Administrator user, and then click **Next**.

7. Click **Finish**. The task should appear in the Scheduled Tasks window. (You can right-click a task to run it, delete or rename it, or to modify any of the task's basic or advanced settings.)

Working with software assets

The software type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated software type details are linked to license file information for your licensed software products. The other asset type with linked details that can be updated with data from the core database is the computer type.

You can use linked details to populate linked data fields for software that has a license file recorded in Software License Monitoring (SLM) in the main console or in the Compliance section in the Web console. For more information about the SLM tool, refer to the *Users Guide*.

The software asset type can't be deleted or renamed.

Linked details for software

Only designated software details are linked and can be updated from SLM. These details are identified by the linked detail icon. Linked details can't be deleted, and you can't create your own linked details.

The following software details are linked:

- Product name
- Version
- Publisher
- Product Link ID

Important: The Product Link ID linked detail can be thought of as the master link because it is used to definitively identify each specific software asset in SLM, ensure there are no duplicate records, and synchronize the appropriate linked data for each software asset. Product Link ID is listed as a Hidden information type in the software details summary page, and only its Default value and Summary fields can be edited manually.

- License number
- License type
- Quantity
- Serial number
- Purchase date
- Unit price
- Order number
- Reseller
- Owner
- Location
- Note

All other details for the software type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with SLM information. Once a software product's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the product information in SLM as many times as you like.

Non-linked data fields can always be edited in Asset Manager.

Updating linked data for software

You can update all of your software products that have a valid license file at once from the software item list page. Note that not all of your licensed software products in SLM necessarily have a license file. Only those licensed products with an actual license file will be updated. Or, you can update linked data for an individual software product (that has a license file) from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see [Using the asset inventory update utility](#).

To update the software item list

1. From the Assets page, open the Technology subgroup, and then click **Software** to view all the software assets currently recorded in the database.
2. Click **Refresh asset data** link located above the

Software products (with a license file) that do not already have a corresponding software item on this page are added to the list, with their linked data fields filled in. If there is no data the field is left blank, and can't be edited.

If a corresponding software item already exists on this page, its linked data is refreshed/updated from the license file information in SLM. If the information has changed in SLM, the new information replaces the value in the linked data field. Only linked data fields are updated. If there is no data the field is left blank, and can't be edited.

To update linked data for one software item

1. From the software item list page, edit the software product by clicking its pencil icon.
2. Click **Refresh asset data** link located above the details list.

The software product's linked data is updated with information from the corresponding product's license file information in SLM. This process rewrites any manually entered or changed value in a linked data field with the current value in SLM. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

Managing contracts

The Contracts page shows all the contract groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Contracts can be any sort of document pertaining to the formal business relationships you have with service providers, partners, and vendors that you want to record and manage. Record critical information about the contract such as names, effective dates, status, contract numbers, terms and conditions, relationships, etc., and then associate the contract with the assets it covers. For example, you could enter data about a lease agreement for a group of printers, and then associate the lease with the printers.

Adding contract information to the database not only helps you keep track of valuable assets but also the important information you need for negotiating terms and conditions for future contracts.

Contract *types* represent the data entry forms used to enter contract items into the database. You can use the predefined contract types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as [by global lists](#).
- Create, edit, and delete subgroups by clicking the [Manage subgroups](#) link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- [Search for types](#) in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its [details summary page](#).
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- [Create new types](#) in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- [View a list of all the items](#) that have been added to the database for a particular type by clicking the type name.
- [Add items to the database](#) by clicking the plus sign (+ Add... link) and filling out its data entry form.

The predefined contract groups and types include:

Standard

- Consulting Agreement
- Escrow
- Lease

Managing invoices

The Invoices page shows all the invoice groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Invoices are documents pertaining to the purchase, acquisition, or payment of products and services. With Asset Manager, you can enter and store relevant information about an invoice and associate it to the corresponding asset.

Invoice *types* represent the data entry forms used to enter invoice items into the database. You can use the predefined invoice types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as [by global lists](#).
- Create, edit, and delete subgroups by clicking the [Manage subgroups](#) link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- [Search for types](#) in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its [details summary page](#).
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- [Create new types](#) in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- [View a list of all the items](#) that have been added to the database for a particular type by clicking the type name.
- [Add items to the database](#) by clicking the plus sign (+ Add... link) and filling out its data entry form.

The predefined invoice groups and types include:

Standard

- Invoice
- Purchase Order

Managing projects

The Projects page shows all the project groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Large, complex projects typically involve the purchase and use of a variety assets and related materials. With Asset Manager, you can enter specific project information into the database, associate the project with any other recorded item, and then generate custom reports to help you track and manage the project.

Project *types* represent the data entry forms used to enter project items into the database. You can use the predefined project types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as [by global lists](#).
- Create, edit, and delete subgroups by clicking the [Manage subgroups](#) link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- [Search for types](#) in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its [details summary page](#).
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- [Create new types](#) in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- [View a list of all the items](#) that have been added to the database for a particular type by clicking the type name.
- [Add items to the database](#) by clicking the plus sign (+ Add... link) and filling out its data entry form.

The predefined project groups and types include:

Miscellaneous

- Ad hoc

Standard

- Capital Expenditure
- Sustaining

Managing global lists

The Global Lists page shows all the global list groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Global lists refer to lists of standard information, such as locations, companies, and users, that can be applied globally to describe assets throughout your organization. By defining these global lists in one place, and using them to add standard data to other types, you can ensure consistent usage in all your asset management records. For example, if you need to update data in a global list, such as a department's name or company's address, the new information propagates automatically to all other items that include that standard global list data.

Global List *types* represent the data entry forms used to enter global list information into the database. You can use the predefined global list types and create your own custom global list types.

On a data entry form, an Expand/Collapse icon next to a data field's text box identifies it as a global list type that can be used to select a detail from a list of that global list type's available details. Whereas, an Expand/Collapse icon next to a data field name, where there is no text box, indicates a table detail.

Using global lists to add a detail to a type

Global lists are different from the asset, contract, invoice, and project types because you can use a global list type to add a standard detail (or data field) to any of the other types. For example, let's say you're adding a detail to a new asset type; choosing "Global List" opens a new dialog where you can select the global list type called "Locations" (and, if you want to specify a default value, you can also select a specific location from the drop-down list of available locations). In this way, global list types are truly global, meaning they're available for all other types, and provide standard, consistent information across the database's asset records.

As previously mentioned, if a detail in a global list type is changed, the change is reflected in any recorded item that uses that detail.

Using global lists to create filters that control user access to asset information

You can also use global list types to control user access to asset information.

First you create a filter based on a global list and then assign a detail from that global list to the user so that they will see only those assets that match.

You can change your global list filter at any time.

To create a global filter and assign it to users

1. From the main Asset Manager page, click **Asses Access**. (This link is available only if the logged in user has administrator rights.)
2. Select the global list you want to server as the filter.
3. Click **Submit** to save the global filter setting in the database. You can come back and change the filter at any time.
4. In the LANdesk console, click **Tools | Administration | Users**.
5. Click the **Asset** tab.
6. Select the detail you want to assign to the user as the filtering criterion. The user will see only the assets whose detail for the global list filter matches the detail selected here.
7. Click **OK**.

Using global lists to organize and view types

Global lists serve another unique purpose in Asset Manager. They can be used as parent groups to view lists of asset, contract, invoice, and project types. From any of the type pages, you can click the **Group by** drop-down list and select a global list (predefined and custom) by which to arrange the types on that page.

For example, if you want to view computer asset types by location, select the "location" global list. Each current location appears as a parent group that can be expanded to show the types (in their subgroups) with matching location data. Types that do not contain location data are listed under the "No Information" parent group. If there aren't any types in the "location" global list type, the "No Information" parent group displays, containing all the page's subgroups and types.

If you select **None** from the Group by menu, subgroups and types are listed without a parent global list group. None is the default setting.

As with other type pages, from the Global Lists page you can:

- View types in subgroups. (Grouping by global list types is not supported on the global lists page).
- Create, edit, and delete subgroups by clicking the [Manage subgroups](#) link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- [Search for types](#) in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its [details summary page](#).
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded).
- [Create new types](#) in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- [View a list of all the items](#) that have been added to the database for a particular type by clicking the type name.
- [Add items to the database](#) by clicking the plus sign (+ Add... link) and filling out its data entry form.

The predefined global list groups and types include:

Default

- Company
- Cost Center
- Department
- Location
- Vendor

Displaying large global lists

The more items you place in a global list, the longer it takes for a page containing that global list to display. For example, when a global list is included in a specific type's definition, that type's Add Items and Edit Items data entry pages take longer to display. Also, selecting a global list that contains a large number of items in the Group By drop-down list may take longer to display.

Creating new types

Use the Add new type page to create your own custom types for assets, contracts, invoices, projects, and global lists.

As a reminder, it might be helpful to consider types as data entry forms comprised of specific details that define an item. Types are divided into the following five major categories in order to facilitate tracking and reporting: Assets, Contracts, Invoices, Projects, and Global Lists. For example, a printer is an asset type, a lease is a contract type, and a location is a global (i.e., generally applicable) type. To continue the example, a printer asset type could be comprised of details (data fields) specifying the printer's manufacturer, model, description, service history, warranty type, cost, and so on. A type is used to add items to the database.

Asset Manager comes with several predefined types that can be used to add common items to the database. You also have the flexibility to create as many additional custom types as you like to accommodate all of the IT assets and critical information you want to manage.

The first step in creating a new type is to define the type's key detail. After the key detail is defined you can add as many other details as you like. All types are created by the same procedure, described below.

To create a new type

1. From any Asset Manager type page (Assets, Contracts, Invoices, Projects, Global Lists), click the **Add type** link next to the group where you want to add the type.
2. In the **Type name** field, enter a unique name for the type.
3. In the **Key name** field, enter a name for the key detail. Every type must have one (and only one) detail designated as the "key" so that it can be tracked in the database. When you initially create a new type, you're required to specify the name of its key detail. If the key detail is the only detail for a type, it must also be a unique and required value. Once a type is created you can't delete its key detail. Additionally, once designated you can't change a type's key detail to be another detail.
4. From the **Type** drop-down list, select the type of information you want this type's key detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), and Alert Date (calendar date; for more information, see [Using asset alert dates](#)). **Note:** Static List and Global List are not valid information types for the key detail. However, they can be used when creating additional details. For more information, see [Adding details](#).
5. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.

6. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (# represents a number). For the actual character a, use the /a exception. For the actual pound character (#, use the /# exception). This mask appears on the data entry form so the user knows how to enter data for the field. **Note:** Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask. Extended characters and double-byte characters are NOT supported.

7. If you want to specify a value that will automatically appear in the key detail's data field on a data entry form, enter that value in the **Default Value** field. You can enter a default value for any type of information. This field is optional. (To enter a default date value, use the calendar control). **Note:** Any default value specified here can be changed when filling out the actual data entry form.
8. Click **Save** to save the type and its key detail, and to return to the Details for... page.

At this page you can continue to configure the type by adding more [details](#), [detail tables](#), or [detail templates](#). You can also change the subgroup where this type resides with the **Belongs to** drop-down list.

Important: When you're done configuring the type, you must also click **Save Details** on the Details for... page in order to save all the details you've added to that type.

Once a custom type is created, you can:

- [Edit a type's details](#) by clicking the pencil icon.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded).
- [Add items to the database](#) by clicking the plus sign (+ **Add** link and filling out the data entry form).

Using a details summary

This page provides a summary view of all the details that make up the type named at the top of the page. A type's details are what appear on a data entry form for that type.

Each type's details summary page is unique, depending on the details that have been used to define that type. However, the tasks you can perform from any details summary page are the same.

From any details summary page, you can:

- View all the details that define the selected type.
- [Edit existing details](#) by clicking the pencil icon next to the detail name.
- Create new details for a type by clicking the [Add detail](#) link.
- Create an [alert date](#) detail for a type.
- Add a group of details to a type at once by clicking the [Choose template](#) link.

- Add a table data field to a type by clicking the [Add table](#) link.
- Delete a detail by clicking the X icon.
- Organize details in configurable sections by clicking the [Manage sections](#) link.

Important note on saving changes to details:

In order to preserve any changes you've made to details in the details summary list (including changes to detail templates and detail tables), you must always click **Save Details** on this page. If you add, modify, or delete one or more details and then click **Cancel** on this page, none of your changes will be saved.

Understanding the detail icons

The details summary page includes a legend with icons that indicate different characteristics for the detail. Detail icons appear here in a details summary list, as well as on an item page and on data entry forms next to data fields.

The legend shows the following icons:

- **Key:** Indicates the detail is the key identifying detail for this type. Each type must have one, and only one, key detail in order to be saved. Key details are automatically unique and required. A key detail can't be deleted or changed.
- **Unique:** Indicates the detail must have a unique value entered when filling out the data entry form. If you enter a duplicate entry (the same value already exists in that data field for another item), an error message displays. Unique details are automatically required. Types can have multiple details that ask for unique data.
- **Required:** Indicates the detail must have valid data entered when filling out the data entry form. A required detail may or may not be unique. For example, if a detail is marked required but not unique, you can enter the same data in that field on data entry forms for different items.
- **Summary:** Indicates the detail will appear as a column heading on an item list page.
- **Linked:** (Applies only to the computer and software asset types) Indicates the detail is linked to corresponding scanned device data, or entered software license data, in the core database. The linked characteristic applies to only some of the details for the computer and software asset types, not all of their details. The linked characteristic does not apply to any details for any other asset type. You can't create your own linked details.

Asset Manager lets you update and synchronize linked data by using the computer or software asset's Refresh feature. Computer assets are updated with the current device inventory data that has been scanned into the core database by the inventory scanner. Software assets are updated with the licensed software products data you've entered into the core database.

Adding details

Use this page to add a new detail, or edit an existing detail, for an asset type.

Details represent the data fields on an item's data entry form. When you fill out a data entry form, that item is added to the core database and can be tracked and managed with Asset Manager.

To edit an existing detail, click the pencil icon next to the detail name. For a description of what information you can and can't edit on a saved detail, see [Rules for editing details](#) below.

To add a new detail

1. From any details summary page, click the **Add detail** link.
2. In the **Name** field, enter a unique name for the detail.
3. From the **Type** drop-down list, select the type of information you want this detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), Alert Date (calendar date; for more information, see [Using asset alert dates](#)), Static List (lets you create a predefined list of values; see the Static List step below), and Global List (lets you select any of the current global list types; see the Global List step below).
4. The **Key** option is not available because this is not the initial detail. The key detail is defined when you initially create the type, and it can't be changed or removed.
5. Select the **Unique** option if you want to indicate on the data entry form that this detail (data field) on the form needs to be filled in with a unique value. In other words, duplicate entries among recorded items won't be allowed in this data field. If you select the Unique option, the Required option (below) is automatically selected as well. This is because a data field that asks for a unique value is considered a required field by default.
6. Select the **Required** option if you want to indicate on the data entry form that this detail (data field) must be filled in with valid data. A required field is indicated by the red "i" icon on a data entry form. A required data field does not necessarily have to be filled in with unique data.
7. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.
8. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (# represents a number). For the actual character a, use the /a exception. For the actual pound character (#), use the /# exception. This mask appears on the data entry form so the user knows how to enter data for the field. **Note:** Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask; extended characters and double-byte characters are not supported.

9. If you want to specify a value that will automatically appear in this detail's data field on a data entry form, enter that value in the **Default Value** field. This option applies to all the information types and is not required. All default values on a form can be edited. (To enter a default date value, use the calendar control.)
10. If you want this detail to appear on the item list page for the type you're configuring, select the **Summary** option. This option is checked by default. If you clear the Summary option, this detail does not appear on the item's list page.

11. If you want to configure a controlled list of valid data entry values for this detail, select **Static List** type. A new dialog appears to the right that lets you add values to the static list. The values you add to this list will be available for this detail in a drop-down list on the data entry form. To add values to the static list, simply enter a value in the **Add Values** text box and click the plus sign (+). To set a value as the default value (automatically appears in the detail's data field on a data entry form), select the value and then click **Set Default**. To remove a value, select it and click **Remove**.
12. If you want to use a global list type to define this detail, select **Global List** type. A new dialog appears to the right that lets you choose from the current global list types (see [Managing global lists](#)). The values that have been added to the database for the selected type will be available for this detail in a drop-down list on the data entry form. Global lists contain general information that is standard throughout your organization, such as vendors, users, and locations. To use a global list type to define this detail, first select the subgroup that includes the global list type you want from the **Select Group** drop-down list, and then select the global list type from the **Select Type** drop-down list. If you want to assign a default value to this detail (data field on the form), select a value from the **Select Default Value** drop-down list. Keep in mind that if no data has been entered into the database for that type yet, this list will be empty.
13. When you're done configuring the settings and values for the detail, click **Return to form** to save the detail and return to the details summary page. Or, click **Cancel** to exit without saving the detail.
14. If you want to place the detail in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see [Organizing details in sections](#).

Important: You must also click **Save Details** on the details summary page to save any details you've added or modified.

Rules for editing details

After a type has been saved, you can edit only some of the information fields for the details that define that type.

Remember that a type must have at least one detail, called the key detail. In addition to its key detail, a type can have any number of additional details that help define that type and help you track and manage your IT assets.

Non-editable fields

For both key and non-key details, AFTER the detail is saved you can't edit any of the following information fields on the Edit Detail page:

- Name
- Type
- Key
- Unique
- Required

Editable fields

Whether the other information fields can be edited is different for key and non-key details, as described below.

For key details:

For a key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary
String	Yes	Yes	Yes	No
Integer	No	No	Yes	No
Date	No	No	Yes	No
Decimal	No	No	Yes	No
Alert Date	No	No	Yes	No

For non-key details:

For a non-key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary	Static List Values	Global List Default Value
Integer	No	No	Yes	Yes	No	No
String	Yes	Yes	Yes	Yes	No	No

Information Type	Length	Input Mask	Default Value	Summary	Static List Values	Global List Default Value
Date	No	No	Yes	Yes	No	No
Decimal	No	No	Yes	Yes	No	No
Alert Date	No	No	Yes	Yes	No	No
Static List	No	No	Yes	Yes	Yes	No
Global List	No	No	No	Yes	No	Yes

Adding detail tables

Use this page to add a detail table to the selected type. A detail table consists of one or more details and appears as an expandable table data field on a data entry form, each detail represented by a separate column in the table.

On a data entry form, an Expand/Collapse icon next to a data field name (without a text box) identifies a detail table. In contrast, an Expand/Collapse icon next to a data field with a text box identifies a global list type.

One example of a table data field on a form is a service history table, that consists of details such as cost, service date, technician, vendor, and so on.

When filling in a form, users can add as many entries as they like into a table data field by clicking the **Expand** icon, clicking the **Add** link, filling in the fields, and then clicking the **Add to table** link. This process can be repeated as many times as you want to add entries to the table.

Some predefined types (and their associated data entry forms) include predefined detail tables. You can also create your own custom tables and add them to types. A table is specific to the type to which it was added (i.e., it can't be shared with other types).

To add a detail table to a type

1. From any details summary page, click **Add table**.
2. In the **Details for** field, enter a unique name for the table.
3. Click **Add detail** to define an individual detail that appears as a column in the table. A table must include at least one detail (data field) on the form .

4. You can also click **Choose template** to select from a list of existing detail templates that will add several details at once to the table. Each detail appears as a single column in the table.

Details in a table display in the order in which they were entered and can't be moved.

5. When you're done configuring the table, click **Save Details** to save the table. The new table appears in the details list as a Table type. Details display in the list in alphabetical order unless they belong to a specific section.
6. If you want to place the detail table in a specific section on the form, click **Manage sections**, select the section in which you want the table to appear, click **Edit**, and move the table to the **Current Details** box. For more information, see [Organizing details in sections](#).

Important: Click **Save Details** again (this time from the details summary page) in order to save the changes you've made.

Once a table is configured, you can:

- [Edit a table's details](#) by clicking the pencil icon.
- Delete an existing table by clicking the X icon.

Managing detail templates

Use the Detail Templates page to view, create, edit, and delete detail templates. Detail templates are sets or groups of details that make it easy and convenient to add several details at once to a type.

Note: You add a detail template to a type from the type's details summary page, not from the Detail Template page. You can also add a detail template to a table from the table's details summary page.

Asset Manager includes a few predefined detail templates, and lets you create as many new detail templates as you want in order to facilitate the creation of custom types and detail tables.

To create a detail template

1. From the Asset Management menu in the Web console, click **Detail templates**.
2. Click **Add template**.
3. Enter a unique name for the template in the **Details for** field.
4. Add as many details as you want to the template by clicking **Add detail**.
5. When you're done adding details to the template, click **Save Details** to save the template and return to the templates list.

Note: When you add a details template to a type, all of the details contained in that template are added as individual details, not grouped as a template. In other words, a details summary list does not indicate in any way whether details came from a template.

To edit a detail template, click the pencil icon next to the template name.

To delete a detail template, click the X icon next to the template name.

To rename a detail template, click the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)

Adding detail templates

Detail templates are sets or groups of details you can use to add several details at once. You can add detail templates to a type's details summary list or to a detail table.

Detail templates are not specific to a type or table; you can view and add currently available templates from any details summary page.

To add a detail template

1. From any details summary page (for either a type or a table), click **Choose template**. All of the existing detail templates appear in a list, and show all of the details in each template.
2. Find the template you want to add to the details summary, and click **Add template**. All of the details contained in the template you just added appear as individual details in the details summary. They're not grouped or identified as coming from a template.
3. If you want to place any of the newly added details in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see [Organizing details in sections](#).

Important: You must also click **Save Details** on the Detail for... page to save any details you've configured.

Using an item list

The item list page provides a summary view of all the items recorded in the database for the type named at the top of the page. To see a type's item list page, click the name of the type on the Assets, Contracts, Invoices, Projects, or Global Lists pages.

The information that displays in the columned table on an item list page is determined by the details that have the Summary option checked. In other words, if Summary is checked then the detail appears on the item list page. You can click the column headings to sort by that detail (data field).

To add items to the database, click the **Add** link, and then fill in the data entry form. For more information, see [Adding items](#).

To edit an item's recorded data, click its **pencil icon**, and then enter new data. When editing, the item's data entry form includes a few extra options. For more information, see [Editing an item](#).

To delete an item from the list (and from the database), click its **pencil icon**, and then click **Delete**.

Additional item list tasks

From an item list page, you can also perform the following tasks:

- [Associate items](#) with other items and related information.
- [Import data](#) for items of the selected type.
- [Export data](#) for items of the selected type.

From the item list page for two asset types, computer and software, you can also:

- Update designated linked details (data fields) with scanned inventory and SLM information from the core database. For more information, see [Working with computer assets](#) and [Working with software assets](#).

Adding items to the database

This page is the data entry form for the type named at the top of the page. Asset Manager includes several predefined asset, contract, invoice, project, and global list types, and provides the ability for you to create as many custom types in each of those categories as you like.

When you enter and save the information on a data entry form, the item is recorded in the database.

A slightly different version of this page appears when you're editing an item. For more information, see [Editing an item](#) below.

The contents and layout of a data entry form are defined by the type's details and sections. For more information, see [Using the details summary](#) and [Organizing details in sections](#).

Adding assets and other important information such as contracts, users, and projects to the database is *the* central task of someone who wants to gain all the benefits of proactive asset management for their organization. Asset Manager provides the tools necessary to configure asset types and the detail elements that define them, to track that data, and ultimately to analyze and share that data through custom asset reports. However, the benefits of asset management to your business, in real terms, depends on the recorded data itself. If most of the fields in a well-designed and thorough data entry form are left blank, there is very little to track, and running reports will be of minimal value. The recorded data is the key, and hence, data entry should be considered the most important step in implementing an effective asset management solution.

Although the information asked for on data entry forms can vary, the process of adding data is the same, as described below:

To add an item to the database

1. From any item list (accessed by clicking the name of a type on either the Assets, Contracts, Invoices, or Projects page), click **Add**. Or, you can access the same page by clicking the plus sign (+ **Add** link) next to the item type. You can expand or collapse the sections of a form by clicking the section name. Also, refer to the Legend at the top of the form to understand the icons next to certain data fields. Detail icons are explained in [Understanding the detail icons](#).

2. Fill in the data fields. When adding or editing a detail, you can only enter data compatible with the field type (i.e., only an integer in an integer field, a text string in a string field, a date in a date field, etc.).
3. To save the item and continue adding more items, click **Save and add another**.
4. To save the item and return to the item list, click **Save and return to list**. The new item appears in the item list.

Editing an item

If you're editing an item that has already been added to the database, this page displays the following additional options:

- **Associate items:** Opens the [Associate items](#) page where you can create associations between the selected item and other items recorded in the database.
- **Delete:** Removes the item from the item list and from the database. When you delete an item, any association to or from the item is also removed. This data can't be retrieved unless you've exported it beforehand to a CSV file.
- **Print preview:** Opens a print-friendly version of this page in a separate window that can be printed from the browser.
- **Last edited by:** Lets you view (at the bottom of the page) the user who most recently modified this item, their core server, and the time.

Using asset alert dates

Asset Manager includes an alerting feature that lets you create and enable alert dates for any of the IT assets you add to your database. Asset alerting uses the standard product Alert Management System (AMS) and its accompanying Alert Settings tool (**Configure | Alert Settings**) where you can configure the precise alert action you want to notify you when an asset's specified alert date is reached.

About the Alert Management System (AMS)

This section describes how to create and enable alert dates for the assets you record and track with Asset Manager. For more detailed and complete information on the Alert Settings tool, see [Using alerts](#).

Alert dates are a convenient way for you to be automatically notified when a predefined deadline for a particular asset item is reached. For example, you can set an alert date to notify you when a lease expires, a contract needs to be renewed, a project milestone is scheduled, or when a computer should be upgraded. You can use alert dates for any purpose to help remind you of important asset-related tasks that need to be performed by a certain date.

In order to use asset alert dates, an asset must first have an alert date detail as part of its type definition. You can use existing alert date details that are already included with most of the predefined asset types, or you can create your own new alert date details. Then, when adding items of that type to the database by filling out its data entry form, the alert date detail must be enabled and a date specified. You also need to decide how you'll be notified by AMS by configuring the alert action in Alert Settings.

Important: Notification actually occurs during the next scheduled Inventory Service Alert Check AFTER the specified alert date is passed.

To learn more about each of these steps, read the sections below:

- [Creating alert date details](#)
- [Enabling and specifying alert dates](#)
- [Configuring the asset alert in Alert Settings](#)

Creating alert date details

Most of the predefined asset types have an alert date detail, but not all. You can create additional alert date details for any of the predefined asset types. For new custom types that you create, you can also add alert date details. A custom type's key detail can be an alert date. An asset can have more than one alert date defined.

Alert date details are listed with all other details on a type's details summary page. They appear as data fields on the type's data entry form.

To create an alert date detail

1. From any Asset Manager type page (Assets, Contracts, Invoices, Projects, Global Lists), click the pencil icon next to the type that you want to create an alert date detail for. The type's details summary page displays.
2. Click the **Add detail** link.
3. In the **Name** field, enter a unique name for the alert date detail.
4. From the **Type** drop-down list, select **Alert Date**.
5. The **Key** option is available only if you're creating a new custom type. For more information, see [Creating new types](#).
6. Select the **Unique** option if you want to indicate on the data entry form that this detail (data field) on the form needs to be filled in with a unique value. In other words, duplicate entries among recorded items won't be allowed in this data field. If you select the Unique option, the Required option (below) is automatically selected as well. This is because a data field that asks for a unique value is considered a required field by default.
7. Select the **Required** option if you want to indicate on the data entry form that this detail (data field) must be filled in with valid data. A required field is indicated by the red "i" icon on a data entry form. A required data field does not necessarily have to be filled in with unique data.
8. If you want to specify a date that will automatically appear in the alert date's data field on the data entry form, enter that value in the **Default Value** field. Click the calendar button, and then select the date you want in the calendar window. You don't have to specify a default value, and any default value can be edited on a data entry form. If you specify a default value, the alert date data field will be enabled on the data entry form.
9. If you want this detail to appear on the item list page for the type you're configuring, select the **Summary** option. This option is checked by default. If you clear the Summary option, this detail does not appear on the item's list page.
10. When you're done configuring the settings and values for the detail, click **Return to form** to save the detail and return to the details summary page. Or, click **Cancel** to exit without saving the detail.
11. The new alert date detail appears on the details summary page in alphabetical order with all the other details.
12. If you want to place the detail in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see [Organizing details in sections](#).

Important: You must also click **Save Details** on the details summary page to save any details you've added or modified.

Your alert date detail has been added to the type. The next time you add an item of this type by filling out its data entry form, you can enable the alert date data field, and then specify the date you want to be notified.

Enabling and specifying alert dates

As stated previously, alert dates (without a specified default value) are disabled by default. If you want to set an alert date for an item you're adding to the database, you must enable the alert date field on the asset's data entry form and then select the date.

To enable and specify an alert date for an item

1. From any item list (accessed by clicking the name of a type on either the Assets, Contracts, Invoices, or Projects page), click **Add**. Or, you can access the same page by clicking the plus sign (+ **Add** link) next to the item type.
2. Fill in the required data fields.
3. For any alert dates you want to enable, clear the **Disable Alerts** check box. (Alert dates with a default value are already enabled. You can select a different date if you prefer, or you can disable the alert date.)
4. Click the calendar control button, and then select the date for which you want to be notified. **Important:** Notification actually occurs during the next scheduled Inventory Service Alert Check AFTER the specified alert date is passed, by the action specified in Alert Settings.
5. To save the item and continue adding more items, click **Save and add another**.
6. To save the item and return to the item list, click **Save and return to list**.

The new item appears in the item list, with its alert date enabled.

Note: You can enable and/or disable alert dates, and modify the specified date, for any item that has already been added to an item list by clicking its pencil icon and making the changes you want.

Configuring the asset alert in Alert Settings

For assets that are being tracked by Asset Manager, the only valid alert event or condition that can be used to trigger an alert is a date (i.e., a specified date being reached). However, the asset date alert is only one of many alerts offered for various tools and services.

As with other alerts, you need to configure the notification method or action for the asset alert in Alert Settings (**Configure | Alert Settings**). The alert you need to configure is called "Asset alert date has been reached." This alert is located under the **LANDesk Inventory Server** object.

Available alert actions include: broadcast messages, Internet mail, SNMP trap, event log, and more.

For step-by-step instructions on how to configure each of these alert actions, see [Configuring alert actions](#).

Adding the description field to an Internet mail action

If you choose to be notified via the Internet mail method, you must manually add and define the Description field to the alert message when configuring the alert action. The purpose of this field is to provide the recipient of the alert message with helpful information regarding the type, nature, and source of the alert. You can enter any text you want.

To define the Description field for the Internet mail alert action

1. At the console, click **Configure | Alert Settings**.
2. Open the **LANDesk Inventory Server** object.
3. Right-click **Asset alert date**, and then click **Configure**.
4. Select **Send Internet Mail**, and then click **Next**.
5. Select the core server you want to be notified, and then click **Next**.
6. Fill in the address, subject line, and SMTP mail server fields, and then click **Next**.
7. Move the **Description** parameter from the Alert Parameters list to the Alert Message list.
8. Enter any text you want in the **Description** field, and then click **Finish**.

Associating items

This page allows you to view, create, and delete associations between the item named on this page and any other item recorded in the database.

Through associations, you can establish and track relationships between any of your fixed assets and their supporting items such as contracts, locations, users, projects, and so on. For example, you may want to associate printers with their lease agreement contract; or PDAs with their users; or phones with their users, locations, and service contracts; and so forth. Associations provide another level of asset management.

Creating associations:

You can create associations only from an actual item page, not from the item list page.

Associations exist between actual items in the database, not between item types. Associations are bidirectional. In other words, if you create an association from a printer to a contract, the same association also exists from the contract to the printer in that specific contract's page.

You can associate the following item types with each other:

- Assets
- Contracts
- Invoices
- Projects

To create an association

1. From any item page, click **Associate Items**. (This is also the way to view an item's associations.) **Note:** The Associated Items page refers to the selected item by its key detail.

2. Use the **Search** tool to locate items that you want to associate with the selected item. From the search results list, check the items you want to associate, and then click **Add to list**.
3. Click **Save** to save the associations and return to the item page.
4. Click **Cancel** to exit without saving.

To delete an association, click the X icon next to the association in the list. Deleting an item also removes all of its associations from the database.

Associated item information can be included in Asset Manager reports.

Importing items

Asset Manager provides the ability to import items for asset, contract, invoice, project and global list types. For example, if you have information for all your printers in a single spreadsheet, you could import printer data into the item list for the printer asset type. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're importing items of a particular type, the **Import** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

Supported file formats

Asset Manager's import and export feature supports both CSV (comma-separated value) as well as XML formatted files. You import data from a CSV or an XML file into an existing type. These file formats are compatible with other data management tools such as Microsoft* SQL Server, Oracle*, Microsoft Access*, and Microsoft Excel*.

Understanding the structure of the import file

The file you want to import must be organized in such a way as to accommodate all the details (data fields) used to define the type.

Each line in the import file represents a single item and therefore corresponds to an item row on the item list page. Furthermore, each line must contain the data for that individual item, separated by commas. Each comma-separated value corresponds to a column on the item list page. A line must include a value for every detail in the type. For example, if the type is defined by ten details, then each line in the import file must have ten values (a value can be empty as long as it's separated by commas). Furthermore, the data in each value must match the data type specified for that data field (i.e., integer, string, date, etc.), or the import fails.

It is a requirement that the first line of the import file contain the names of the details (that match the column headings on an item list page), separated by commas.

It might be helpful to envision the import file as basically being in the same format and layout as an item list page; a table listing where each column represents a detail and each line represents an individual item.

Importing items

To import items into an existing type

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to import items into.
2. On the item list page, click **Import**.
3. Enter the full path, including the filename, to the file you want to import in the **File path** field. You can click **Browse** to locate and select the file you want to import.
4. Click the **Valid column names** link to see a list of all the details used to define the selected type. A details summary window opens showing all of the type's details by name and other characteristics in a column list. **Important:** Your import file's structure and contents must be compatible with the columns in this list (each column representing a detail). For more information on the correct structure of an import file, see [Understanding the structure of the import file](#) above.
5. To ignore duplicate data, click **Ignore**. Or, to update duplicate data, click **Update**.

Duplicate data is identified as such by the value of an item's key detail. If two items have the same value for their key detail, both items in their entirety (i.e., their key detail and any other details) are considered duplicate data. You can choose what the import procedure does with any occurrences of duplicate data like this with the **Duplicate handling** feature, as described below:

If you click **Ignore**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database is NOT imported. The item in the import file is ignored and the existing item is preserved. If you click **Update**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database IS imported. The item in the import file replaces the existing one.

6. Click **Import now**.

If the import file is formatted correctly, the data is added to the database and the items appear on the item list page.

Exporting items

Asset Manager provides the ability to export data for asset, contract, invoice, project, and global list types. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're exporting items of a particular type, the **Export** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

When you export a type, all of the items currently recorded in the database for that specific type are exported. However, you can customize the data to be included in the export file by selecting which of the type's details you want exported. The selected details will be exported for all the items currently recorded in the database. You can also save a customized list of selected details as an export configuration for future use. Export configurations are specific to the type for which they are created.

Supported file formats

Data can be exported as either a CSV (comma-separated value) formatted file or as an XML formatted file. These file formats are compatible with other data management tools such as Microsoft SQL Server, Oracle, Microsoft Access, and Microsoft Excel.

Understanding the structure of the export file

As stated in the [Importing items](#) section, the structure or layout of this exported file essentially matches the layout of an item list page, where each line in the file represents a distinct item record, and each comma-separated value in a line represents a detail (data field) for that item.

Export file names

All items for the selected type are exported in a single file (typename.csv). If the type has table data fields, then each table is exported as a separate file (typename-tablename.csv).

Exporting items

To export items

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to export.
2. On the item list page, click **Export**.
3. To use an existing export configuration, select it from the **Configurations** drop-down list.

Or, to manually specify the data you want included in the export file, clear the details you don't want exported. All details are checked by default. If you want to save your selected details as a new export configuration for this type, enter a name in the **Configurations Name** field, and then click **Save**. The export configuration is added to the drop-down list and can be used at any time by this specific type.

4. Click **Export now**. The Export window opens displaying the files (and formats) that can be exported. You can export one or both of a file's two formats: CSV and XML. **Note:** If you're exporting one or more table details for the type, each table detail must be exported as a separate file represented in the Export window by a unique file whose name corresponds to the table name.
5. Click the file you want to export.
6. At the browser's File Download dialog, click **Save**, choose a destination on the local machine, and then click **Save** again.
7. At the Download Complete dialog, click **Close**.

8. You can continue saving other export files from the Export window, and simply click **Close Window** when you're finished.

Using Asset Manager reports

Asset Manager includes a reporting tool that lets you collect and analyze the asset management data you've entered into the database.

The reporting tool includes several predefined asset management-specific reports that you can use to analyze the data you've entered for assets, contracts, invoices, and projects. These predefined reports provide examples of how you create and configure your own custom reports.

To view and edit a report's configuration, click the pencil icon.

To run a report and view the results, click the report name.

To delete a report, click the X icon.

Rights required to use asset reports

A user must have either the Asset Configuration right (which is equivalent to an administrator role) for Asset Manager features and implies all Asset Manager rights or the Reports right to be able to see and use the Reports link and features in Asset Manager. If a user has only the Asset Data Entry right, they won't even see the Reports link in the left navigation pane of the Web console. On the other hand, if a user has only the Reports right, they will see the Assets, Contracts, Invoices, Projects, and Global Lists links, but they can only browse those pages and can't create, edit, or delete any types, details, or actual items. For more information about the specific abilities provided by these asset management rights, see "[Using role-based administration with Asset Manager.](#)"

Note: A user with only the Reports right does not count against your total number of user licenses for Asset Manager.

Rights are assigned to users by one with the Administrator right via the Users tool in the main console.

The Reports right for Asset Manager is the same Reports right that is used to provide access to the reporting tool in the console. Note that none of the Asset Manager reports are available in the main console's Reports tool (even for users with the Reports right). Asset Manager reports are only accessible via the Web console.

Using predefined Asset Manager reports

Asset Manager includes several predefined reports that generate information about the assets, contracts, invoices, projects, and related information recorded in the database. Some of the predefined asset reports are listed below. You can use these reports as examples or templates of what you can do with the Reports tool in Asset Manager.

- Ad-Hoc Projects Completed in Last 30 Days
- Ad-hoc Projects Started in Last 30 Days

- All Computers and Associated Items
- All Consulting Agreements
- All Leases and Associated Items
- All Mobile Phones
- All PDAs
- All Purchase Orders and Associated Items
- Computers by Cost Center Location
- Computers by Requested Date
- Computers Installed in Last 30 Days
- Leases by Business Code
- Leases by Cost Center Location
- Leases Expired in Last 30 Days
- Leases Expiring in Next 30 Days
- Purchase Orders by Cost Center Location
- Purchase Orders by Vendor
- Software by Cost Center Location
- Software by Request Date
- Software Installed in Last 30 Days

Creating and running custom reports

You can create, edit, run, and print your own custom reports. There are three types of custom reports:

Date report: Provides information for a specific type's recorded items, grouped by one of its date details. For example, you could create a custom date report that gathers information about an asset based on its purchase date, or a contract based on its signature date. The results of a date report are determined by a specified timeframe (range of days) for the date detail. You can customize the additional details that are included in the report.

Summary report: Provides information for a specific type's recorded items, grouped by any one of its details. Summary reports always show a count number and at least one of the item's details. You can customize the additional details that are included in the report.

List report: Provides information for a specific type's recorded items, in a flat list. You can customize the additional details that are included in the report.

Use the procedure below to create and run a custom report:

To create and run a custom report

1. From the Reports page, click the **Add report** link for the type of report you want ; date, summary, or list.
2. In the **Report name** field, enter a unique name for the report.
3. From the **Run report on** drop-down list, select whether to report on an asset, contract, invoice, or project type.

4. From the **Select type** drop-down list, select the specific type for whose recorded items you want to gather information. This list includes all the currently available types for the selected category.

If you're creating a list report, skip to step 7.

5. For a **date report**:

First, from the **Group by detail** drop-down list, select the date detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the date detail from its submenu. (The drop-down list includes the currently available *date* details for the selected type, plus any global list types whose date details the selected type uses.) Then, in the **Timeframe** field, enter the number of days (before or after today) whose dates you want to include in this report. For example, 0 (zero) indicates today, -30 indicates 30 days before today (including today), and 30 or +30 indicates 30 days after today (including today). The date report will include all of the type's recorded items whose specified date value matches a date within this timeframe.

6. For a **summary report**:

First, from the **Group by detail** drop-down list, select the detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the detail from its submenu. (The drop-down list includes *all* the currently available details for the selected type, plus any global list types whose details the selected type uses.) Then, if you want the summary report to include only the detail selected above and an item count, clear the **Details** check box. If you clear this option, the Shows columns and Related details options are dimmed and can't be selected. However, if you want to configure additional information to appear in the summary report, make sure **Details** is checked (the default setting), which allows you to select the other information options.

7. Specify the columns (that display details) on an item's page you want to include for each item in the report with the **Show columns** option. You can choose to include just the key detail, the summary details, or all details.
8. Specify additional information you want to include for each item in the report with the **Related details** option. You can choose to include none, table details, or associated items.
9. Click **Save and run** to save this report configuration and generate the report's results. A separate browser (pop-up window) opens and displays the report, which you can view and print.
10. Or, click **Save** to save the report configuration and return to the Reports page without running the report.

If you selected either of the two save options, the report is added to the alphabetical list on the Reports page.

As with predefined reports, you can view and edit a custom report configuration by clicking the pencil icon, and run a custom report by clicking the report name.

You can print a report from the report's pop-up window, according to the browser's Print settings.

Monitoring with alerts

Using alerts

Alerting and monitoring features make your work more efficient by giving you immediate notice of hardware, software, and application events on the devices you manage. When events occur that indicate a need for action or a potential problem, alerts can initiate the process of solving the problem in different ways, such as logging the event, sending an e-mail or pager message, running an application, or powering off the device.

An *alert* is a unique ID that represents an event. You can specify an *alert action* that is performed automatically when the event occurs, such as automated e-mail, applications, or power options. An alert combined with an action is referred to in this product as an *alert rule*. Some alerts can be combined with specific *performance monitoring rules* that specify the condition that triggers an event. For example, you can define a monitoring rule for available free space on disk drives, so that when a drive is 90% full a warning alert is generated.

By defining *alert rulesets* you decide which events require immediate action or need to be logged for your attention. A ruleset contains a collection of alert rules, each of which has a corresponding alert action. When you define an alert ruleset you can deploy it to one or more devices to monitor the items that are important for that kind of device.

This chapter includes information about:

- [Understanding alerts, actions, and performance monitoring](#)
- [Events that can generate alerts](#)
- [Severity levels for events](#)
- [Using alert actions to receive notifications](#)
- [Process for deploying alert rulesets](#)
- [Process for configuring custom alert rulesets](#)
- [Alert storm control](#)
- [Migrating alerts from previous versions of LANDesk Management Suite](#)

Related topics include:

- [Configuring alert rulesets](#)
- [Deploying alert rulesets](#)
- [Viewing alert rulesets for a device](#)
- [Viewing the alert log](#)

Understanding alerts, actions, and performance monitoring

To generate alerts for a managed device, the alerting agent must be deployed to that device. A default alerting agent is deployed to every managed device when you add the device to your list of managed devices. That agent follows the rules defined in the alert rulesets for that device.

By default every managed device has a standard alert ruleset. When you have defined a custom ruleset you can deploy it to devices to monitor items specific to that type of device. You can deploy multiple rulesets to devices, although you should be aware that conflicts could occur between similar rules in different rulesets.

When you install an additional Win32 console on a device, no agent is installed on that device. Even though you can manage other devices from that console, the console device itself can't generate alerts, either as a core or as a managed device, unless you also install management agents on it.

Events that can generate alerts

This product has an extensive list of events that can generate alerts. Some events are problems that need immediate attention, such as component failure or system shutdown. Other events are configuration changes that provide useful information to a system administrator, such as changes that affect a device's performance and stability or cause problems with a standard installation.

Examples of the types of events you can monitor include the following:

- **Hardware changes:** A component such as a processor, memory, a disk drive, or a network card has been added or removed.
- **Application added or removed:** A user has installed or uninstalled an application on a device. This can be useful in tracking licenses or employee productivity. Applications registered in Windows Add or Remove Programs are monitored, and the application name used in Add or Remove Programs is the name that appears in the alert notification.
- **Service event:** A service has started or stopped on the device.
- **Performance:** A performance threshold has been crossed, such as for drive capacity, available memory, etc.
- **IPMI event:** An event detectable on IPMI devices has occurred, including changes to controllers, sensors, logs, etc.
- **Modem usage:** The system modem has been used, or a modem has been added or removed.
- **Physical security:** Chassis intrusion detection, power cycling, or another physical change has occurred.
- **Package installation:** A package has been installed on the target computer.
- **Remote control activity:** Remote control session activity has occurred, including starting, stopping, or failures.





To view a record of alerts for configuration changes, review the alert log on the device's server information console (see [Viewing the alert log](#) for details).

Alerts can only be generated when devices are equipped with the appropriate hardware. For example, alerts generated from sensor readings only apply to devices equipped with the correct sensors.

Hardware monitoring is also dependent on the correct configuration of the hardware. For example, if a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, alerts will not be generated from S.M.A.R.T. drive monitoring.

Severity levels for events

Device problems or events can be associated with some or all of the severity levels shown below. In some parts of the product interface, these states are noted with a numeric value as well as an associated icon. Numeric values are in parentheses.

-  **Informational (1)**: Supports configuration changes or events that manufacturers may include with their systems. This severity level does not affect device health.
-  **OK (2)**: Indicates that the status is at an acceptable level.
-  **Warning (3)**: Provides some advance warning of a problem before it reaches a critical point.
-  **Critical (4)**: Indicates that the problem needs immediate attention.
- **Unknown**: The alert status cannot be determined or the monitoring agent has not been installed on the device.

Depending on the nature of the event, some severity levels don't apply and aren't available. For example, with the Intrusion detection event, the device's chassis is either open or closed. If it is open, an alert action can be triggered, but only with a severity of Warning. Other events, such as Disk space and Virtual memory, include three severity levels (OK, Warning, and Critical) because different states can indicate different levels of concern to the administrator.

You can choose the severity level or threshold that will trigger some alerts. For example, you can select one action for a Warning status and a different action for a Critical status for an alert. The Unknown status can't be selected as an alert trigger but simply indicates that the status cannot be determined.

Using alert actions to receive notifications

This product can notify you when monitored events occur by doing any of the following:

- Adding information to the log
- E-mailing a notice or sending a message to a pager
- Running a program on the core or an individual device
- Sending an SNMP trap to an SNMP management console on the network
- Rebooting or shutting down a device

See [Configuring alert rulesets](#) for detailed information about configuring alert actions.

Process for deploying alert rulesets

This product includes predefined alert rulesets that can be deployed to managed devices. Note that each managed device must have a management agent installed before you can deploy an alert ruleset to the device and before it can send alerts to the core server.

When the monitoring agent is installed to a managed device, a default ruleset of alerts is included by default to provide health status feedback to the console. This default ruleset includes alerts such as:

- Inventory scanner alerts

- Connection control manager actions
- LANDesk Antivirus status
- Network access control status
- Client database utility
- Security and Patch Manager alerts

You can modify these standard alert rulesets to include the alerts you want to monitor. See [Configuring alert rulesets](#) for detailed information.

The general process for deploying alert rulesets to managed devices is as follows:

- Create or edit the ruleset
- Target the devices you want to deploy the ruleset to
- Schedule a deployment task to the targeted devices

For complete instructions on deploying rulesets to devices, see [Deploying alert rulesets](#).

Notes

You can deploy multiple rulesets to a device, and you can select devices in other ways than by targeting them.

You can remove all rulesets from one or more devices in the same way that you deploy rulesets: target the devices and, in the list of alert rulesets, right-click and select **Remove all rulesets**.

Process for configuring custom alert rulesets

In addition to the default rulesets, you can configure and deploy custom alert rulesets. You can include custom alert actions to respond any combination of events. For example, you may want to define one set of actions for events on managed desktop devices (such as sending an e-mail to the hardware support team) and a different set of actions for managed servers (such as sending a pager message to the admin).

The overall process for creating and deploying an alert ruleset is as follows:

1. Create your custom alert ruleset. This includes selecting alerts to include and associating alert actions with them. (See [Configuring alert rulesets](#) for more information).
2. Select the devices to which you will deploy the ruleset and click **Target** to add them to the **Targeted devices** list.
3. Deploy the ruleset to the targeted devices. (See [Deploying alert rulesets](#) for more information).

Alert storm control

Some alert rules assigned to groups of devices can simultaneously generate a large number of responses. For example, you can include an alert rule for computer configuration changes and associate it with an e-mail action. If a software distribution patch is applied to many devices with this alert rule, it would generate a number of e-mails from the core server equal to the number of devices to which the patch was applied, potentially flooding your e-mail server with a "storm" of alert notifications.

This product's alert storm control feature automatically limits the number of times an alert action occurs for an alert. If an alert triggers an action 5 times in 5 minutes, the alert action is discontinued but alerts are still written to the core log file. The administrator is notified of the alert storm with an automated e-mail. When the alert stops occurring and does not occur again for one hour, the alert storm control is reset for that alert. Alert actions will again be triggered if that alert occurs again later.

Migrating alerts from previous versions of LANDesk Management Suite

Previous versions of LANDesk® Management Suite included alerting functionality with the Alert Management System (AMS) feature. Beginning with version 8.8, alerting is based on a new set of alert handlers, even though some alerts are based on AMS alerts. Your alert rulesets for managed devices will need to be created using the new alerting feature.

To help you migrate alerts from previous versions, this product includes a utility that extracts information about your AMS alerts and writes the data to a text file, which you can refer to as you create new rulesets. To use this utility:

1. In the \utilities directory of the LDMAIN share, run `alertexp.exe`.
To show help information about using the utility, type `alertexp.exe /?` at the command line. You can optionally specify the path to the `iaobind.dat` file and a path and filename for the output file.
2. Open the `iaobind.txt` file to view a summary of existing AMS alerts.

You can use the information about your existing alerts to create new alert rulesets. The text file lists the name of each alert with the associated action and severity, along with the application that triggers the alert and parameters associated with it.

Configuring alert rulesets

The **Alert rulesets** page displays all the alert rulesets that you can deploy to managed devices. There are four rulesets that appear by default, and you can create custom rulesets to apply specific types of monitoring to different kinds of devices.

The four alert rulesets that appear by default on the **Alert rulesets** page are:

- **Core alert ruleset:** This ruleset ensures that alerts originating on the core server are handled. This ruleset is installed on the core server but can't be installed on other devices, and you can only have one core alert ruleset. You can edit the ruleset but can't delete it from the core server. This ruleset contains a predefined group of alert types, including Device Monitor, Intel vPro (Intel AMT) alerts, and Serial Over LAN Session alert types.
- **Default ruleset:** This ruleset is deployed by default to all LANDesk Server Manager and System Manager managed devices and contains a number of alert types that are of general use for most network administrators. You can edit this ruleset to add other alert types and change the settings for the default alert types.
- **LDMS default ruleset:** This ruleset is deployed by default to all LANDesk Management Suite managed devices. It includes alerts for security features included in Management Suite, such as access control, connection control manager, inventory scanner, and Security and Patch Manager alerts.

- **Provisioning ruleset:** This ruleset contains alerts related to provisioning tasks, such as task begin and end, section completed, and wrong OS pre-boot environment. When a device is provisioned, this ruleset is used to send alerts related to the progress of the provisioning task. You can edit this ruleset to change the actions associated with the provisioning alerts (for example, to be notified by e-mail when a provisioning task is complete).

In addition to these rulesets you can create custom rulesets to apply to targeted groups of managed devices. You can deploy rulesets by scheduling a deployment task, or you can include rulesets when you deploy agents to devices using agent configuration. While the default rulesets are available to be deployed with agents, you can choose not to deploy the rulesets when you define the agent configuration.

Notes

- When you create a custom ruleset for a device, be aware that if a default ruleset has already been deployed to the device you may have overlapping or conflicting alerting rules. If you deploy the default ruleset when you configure the managed device, and then deploy a custom ruleset, both rulesets will be executed on the device. For example, if both rulesets generate alerts for the same alert type but take different actions, you may have duplicate or unpredictable alert actions as a result.
- Every alert that you create rules for automatically has a "Log handler configuration" rule so that every alert is logged at the core server. When you create a new alert rule, a second rule with the Log handler configuration action is created by default. This default rule must always be in the ruleset: you can't delete it unless you delete all rules for that particular alert. In other words, if you have three rules for an alert, you can't delete the default rule unless you delete all three rules, but you can delete either of the other two rules for that alert.

Important: To use the ruleset editing feature in LANDesk® Management Suite, you must install the Web console as part of the Management Suite installation process. If the Web console is not installed you will not be able to create or edit alert rulesets.

Process for configuring a ruleset

Rulesets contain a collection of associated alerts, actions, and time filters. As you configure a ruleset, you'll define multiple action tasks and time filters that can be reused. The general procedure for configuring a ruleset includes the following steps:

1. [Create a ruleset](#)
2. [Add new alert rules to a ruleset](#)
3. [Define alert actions to use in rules](#)
4. [Define time filters to use in alert rules](#)
5. [Edit alert rules in a ruleset](#)
6. [Include rulesets within other rulesets](#)
7. [Publish a ruleset](#)

To create an alert ruleset

1. Click **Tools | Configuration | Alerting**.

2. Click the **New alert ruleset** button on the toolbar. Type a name in the **Name** field, type a description of the alert in the **Description** field, then click **OK**.
3. To change the ruleset's name or description, right-click it in the **Alert rulesets** list and select **Properties**.
4. To make a copy of a ruleset that you can make minor changes to, right-click the ruleset in the list and select **Copy**. Type a new name and description and click **OK**.

To add new alert rules to a ruleset

1. In the **Alert rulesets** list, select the ruleset and click **Edit** on the toolbar.

The **Rules summary** page lists each alert in the ruleset with its associated actions and time. Each combination of an alert, action, and time is listed as a separate item on the **Rules summary**.

2. Click **Alerts** in the left column to add an alert rule to the ruleset.
3. In the right column, click **Rules | New**. Three "wells" are displayed at the bottom of the page to associate alerts, actions, and time rules. Locate an alert in the list and drag it to the **Alerts** well at the bottom of the page.

Alerts are listed in two groups, **Standard** and **Monitor**. Click an item under one of those groups to view a group of associated alerts. If you click the **All alerts** folder, all alerts are listed alphabetically.

4. To find a particular alert, type a search string in the **Rules filter** text box at the top right of the page. All alerts containing the string you type are displayed in the list.
5. Click **Actions** to associate an alert action with the alert you added. By default, every alert has a **Log handler configuration** action associated with it, which logs the alert at the core server. To add another action, drag it to the **Actions** well at the bottom of the page.

The **Standard** folder contains predefined actions. To use another type of action, you need to define the action first (see steps below).

6. Click **Time** to specify how frequently the alert should be monitored. Drag a time rule (for example, **Always**) to the **Time** well at the bottom of the page.

Three time rules are available by default. To use a different time rule, you need to define it first (see steps below).

7. When you have at least one alert with associated action and time tasks, click the **OK** button at the bottom of the page to add the alert rule to the ruleset. Click **OK** again, then click **Rules summary** to view the updated ruleset with the new alerts.

With a list of alerts in the ruleset, you can edit each item to change the associated action and time. You can also choose which severity levels to apply to the alert and you can specify whether that alert should contribute to the device health. See the steps below for more information about editing a rule.

If you are using LANDesk® Management Suite, you will not see all available alerts unless you also have LANDesk® System Manager installed on the core server (or if you have a dual installation of Management Suite and Server Manager). The alerts listed under the Monitor folder are only available when Server Manager or System Manager are installed on the core server.

To define alert actions to use in rules

1. In the left column of the **Alert ruleset** page, click **Actions**.
2. Select an action group (for example, **Send e-mail**), then click **Tasks | New** in the right column.
3. Add information in the fields as needed, then click **Save**.

The action is listed under the group you selected and is available to associate with alerts. Details about the fields in the different actions types are explained below.

Run on core/Run on client

This action starts an executable file on either the core server or the managed device.

- **Name:** the identifying name for the action. Be specific so you can easily distinguish between actions.
- **Path and filename:** the full path and filename for the executable to be run on the core server or the managed device. When the alert is triggered, the alerting agent will issue a command to run this file.

When you select either action, note that programs may not display as expected on the desktop. When the program is run, it is started as a service in Windows and so is not displayed as a regular application would be. Programs that are run in this way should not contain a user interface that requires interaction. To definitively determine if the program executed, check the processes in the Windows Task Manager.

Send e-mail

This action sends an e-mail message using the SMTP server you specify.

- **Name:** the identifying name for the action. Be specific so you can easily distinguish between actions.
- **To:** the full e-mail address of the person you want to receive the e-mail notification.
- **From:** any valid e-mail address, preferably one that indicates that the e-mail is an alert notification. If this is not a valid e-mail address the message will not be sent.
- **Subject:** a descriptive subject for the e-mail notification.
- **Body:** a message to accompany the alert notification.
- **SMTP server:** the location of an SMTP server from which the e-mail can be sent.
- **Set credentials:** click to specify a username and password that can be used to log on to the SMTP server.

The e-mail will be sent from the core server.

You can send e-mail messages to multiple recipients, and you can use the following variables in the Body field:

- %% = %
- %D = Description
- %N = Computer name
- %S = Severity
- %T = Time (UTC)

Send SNMP trap

This action sends an SNMP v1 trap when the alert is triggered.

- **Name:** the identifying name for the action. Be specific so you can easily distinguish between actions.
- **Host name:** the name of the SNMP host that will receive the trap.
- **Community string:** a v1 community string that is used by the host to receive traps.

Severity levels for alerts are reported in the Specific Trap Type field of the trap. Values are 1 = Unknown, 2 = Informational, 3 = OK, 4 = Warning, and 5 = Critical.

To define time filters to use in alert rules

1. In the left column of the **Alert ruleset** page, click **Time**.
2. Click **Tasks | New** in the right column.
3. In the **New filter** dialog, enter data in the fields (described below).
4. Click **Save**.

The time filter appears in the list and is available to associate with alerts. Details about the fields in the **New filter** dialog are explained below.

- **Filter name:** the identifying name for the filter.
- **Schedule:** select **Specific time** for a filter that limits the time and days when the alert is monitored. Select **Anytime** to monitor the alert continually.
- **From/To:** select a beginning and ending time during the day when the alert is monitored.
- **On these days of the week:** select the days that you want the alert monitored. Selected day icons are darker than unselected days.

To edit an alert rule

You can edit individual alert rules in the **Rules summary** page. Changes you can make include selecting a different action or time filter, selecting which severity levels are in effect, and specifying whether the rule contributes to the device's health status.

1. Click **Rules summary** to view the alert rules in the current ruleset.
2. Click the alert rule you want to edit and click **Rules | Edit** in the right column.
3. To change the associated action or time, select a new option from the drop-down lists.
4. To receive an alert notification only for particular severity levels, click the severity level icons. A dimmed icon indicates that alerts for that severity level will be ignored.
5. To include the alert rule as an indicator of device health, check the **Health** check box.
6. Click **OK** to save your changes.

Each alert rule can have only one associated action and one time filter. If you want to create additional rules for an alert, click **Clone** in the right column to create a duplicate of the rule, then edit the duplicate.

To include rulesets within other rulesets

One way to make ruleset creation more flexible is to create smaller rulesets that you then combine for different uses. To do this, you can include rulesets within other rulesets.

1. At the bottom left of the **Alert ruleset** page, click the **Includes** button.
2. In the left column, click **Includes**.
3. In the right column, click **Includes | New**.
4. In the **Available rulesets** dialog, select one or more rulesets to include in the current ruleset, then click **OK**. Use Ctrl+click or Shift+click to select multiple rulesets.

The rulesets are added to the **Includes** list.

5. If you want to remove a ruleset from the **Includes** list, select it and click **Includes | Delete** in the right column.
6. To see which other rulesets include the current ruleset, click **Included by** in the left column.

When you include rulesets, each individual ruleset is maintained as an individual XML file. The XML files are not combined, but they reference each other

To publish an alert ruleset

After you have added and edited rules in a ruleset you need to publish the ruleset. This creates an XML file with the ruleset data that is referenced by the alerting agent as it works.

1. On the top left of the **Rules summary** page, click the **Publish** button.

A success message will indicate that the ruleset has been published.

The XML files with published ruleset data are stored in the Idlogon share on the core server, in the alertrules folder.

When you publish a ruleset, the alerting service is notified to reload the updated rulesets. When you have updated a ruleset that you have already deployed to managed devices, each of those devices will automatically update their rulesets with the modified rules the next time the alerting agent runs on those devices. If you don't publish a ruleset, there will be no signal to the alerting service to reload the ruleset, so there will be no automatic update of the ruleset on devices that already have the ruleset. It is strongly recommended that you publish rulesets every time you make any changes to them.

Deploying alert rulesets

To install an alert ruleset on one or more devices, you can schedule a deployment task for the ruleset.

In order to deploy a ruleset to a managed device, you must first have a management agent installed on that device. When you deploy the standard management agent, the default ruleset is installed on the device by default, but you can select this or any other available rulesets to be installed on the device with the management agent. After the agent setup is complete you can update the default ruleset or deploy new rulesets by scheduling an alerting task.

To deploy an alert ruleset

1. Click **Tools | Configuration | Alerting**.
2. In the **Alert rulesets** list, click the ruleset you want to deploy.
3. On the toolbar, click the schedule icon and select **Distribute rulesets**.
4. Type a task name for the alerting task.
5. To add the ruleset to devices and keep any existing rulesets on those devices, click **Add selected rulesets**.

To add the ruleset to devices and remove any existing rulesets on those devices, click **Replace any existing rulesets**.

If you have previously deployed the ruleset and want to update it on the same devices, check the **Resend to devices with the selected rulesets** check box.

6. To deploy other rulesets in the same task, click the **Add** button and select the rulesets.
7. Click **OK**.

Notes

To remove all existing rulesets from targeted devices (without deploying any new rulesets), click the schedule icon and select **Remove all rulesets**.

You can deploy rulesets to devices as part of an agent configuration. When you define an agent configuration you can select the rulesets you want to deploy.

Viewing alert rulesets for a device

To view the alert rulesets that have been assigned to a managed device, open the full inventory view for the device. This displays the name of the ruleset and the date it was last installed or updated on the device.

To view the alert rulesets installed on a device

1. In the **All devices** view, right-click the device and select **Inventory**.
2. In the tree view, expand **LANDesk Management** and click **Alert Ruleset Installed**.
3. If there is more than one ruleset, select a ruleset in the tree view to display its details.

You can also create a query that returns all devices that have a particular alert ruleset installed. In the query components list, follow the same path as described in the inventory list above.

Viewing the alert log

Use the **Alert log** page to view alerts sent to the core (the global alert log) or to managed devices. The log is sorted by Time (GMT), the most recent alert being at the top of the log.

The alert log contains the following columns:

- **Alert name:** The name associated with the alert, as defined in the **Alert configurations** page.
- **GMT Time:** The date and time the alert was generated.
- **Status:** The severity state of the alert, which can be one of the following:
 - **Unknown:** The status cannot be determined.
 - **Informational:** Supports configuration changes or events that manufacturers may include with their systems.
 - **OK:** Indicates that the status is at an acceptable level.
 - **Warning:** Provides some advance warning of a problem before it reaches a critical point.
 - **Critical:** Indicates that the problem needs your immediate attention.
- **Device name:** The name of the device on which the alert was generated. This should be a fully qualified domain name. (Global alert log only).
- **IP address:** The IP address of the device on which the alert was generated. (Global alert log only).

If the device name does not appear as a fully qualified domain name, it is because this product was unable to resolve the fully qualified domain name for the device.

To view the global alert log

1. Click **Tools | Reporting/Monitoring | Logs**.
2. To sort entries by column, click a column heading.
3. To view a more detailed description of an alert, double-click the entry in the **Alert name** column.
4. To list log entries by name, status, or instance, select the filter criteria in the **In column** drop-down list. For example, select **Alert name** and type a complete name (such as Performance) or a partial name with the * wildcard (such as Remote*) in the **Find** box. To search by date, select **Enable date filtering**, enter a range with a start date and end date. When you have added filter criteria, click **Search** on the toolbar.
5. To delete a log entry, right-click the alert and select **Delete**.

Handheld Manager

LANDesk® Handheld Manager provides extensive inventory management and software distribution for handhelds devices. Unify desktop, server, and mobile device management in a single solution.

Handheld Manager provides:

- Asset management
- Software distribution
- Bandwidth throttling and checkpoint restart
- Automated file backup
- Automated update and device maintenance

Optimized for the low-speed, intermittent connections characteristic of handhelds and embedded devices, Handheld Manager integrates comprehensive handheld management with enterprise-level task control.

Handheld Manager provides handhelds with the same detailed inventory and software distribution capabilities that LANDesk provides for desktops, servers, and laptops. A lightweight inventory scanner catalogs detailed hardware and software attributes and stores them in the central inventory database. That enables robust license tracking, reporting, and change control, as well as easy targeting for software deployments.

Handheld Manager's seamless integration with LANDesk means you can manage handhelds right alongside your desktops and laptops. Use the same familiar querying tools to track inventory, and the same powerful task scheduler to distribute software. There's no need to learn specialized tools to support handheld devices.

Easily distribute software packages and updates to both wired and wireless Windows CE devices using LANDesk's familiar task scheduler. This enables IT to establish standards and ensure that the right tools are available to your mobile workforce—wherever they may be at the moment—so they spend their time working, not configuring their handhelds.

Handheld Manager supports these features:

- Palm: Inventory only
- Windows CE*: Inventory, software distribution, and handheld file exchange
- Blackberry/RIM: Inventory only

Note: This product installs with Management Suite automatically. It only needs to be activated.

Read this chapter for more information on:

- [Installing Handheld Manager](#)
- [Using Handheld Manager](#)
- [Working with BlackBerry* devices](#)

The following table indicates which features are supported on each client:

	Pocket PC 2003 SE	Mobile 5 Pocket PC	Mobile 6 Professional	Palm	Blackberry	HPT5220 ce5	Neoware ce5
Hardware inventory scan	X	X	X	X	X	X	X
Software inventory scan	X	X	X			X	X
Software distribution	X	X	X			X	X
Transfer files from core to client	X	X	X			X	X
Transfer files from client to core	X	X	X			X	X
Agent update (wceagent.ext)	X	X	X			X	X

Installing Handheld Manager

Handheld Manager has these system requirements

Palm system requirements

- LANDesk Management Suite 8.7 inventory and software distribution agents on host computers that handhelds are connected to (required for Palm handheld agent installation, optional for Windows CE host computers)
- Palm OS 4.0 or greater
- About 25 KB of memory

Windows Mobile system requirements

- Pocket PC 2003 Second Edition or Windows Mobile 5.0
- The device must be running on the X-Scale ARM processor platform
- About 80 KB of memory (program file storage requires about 1 MB)

Blackberry system requirements

- Blackberry Platform OS 4.0, 4.1, and 4.2
- BlackBerry Enterprise Server on your network

Installing Handheld Manager on devices

Handheld Manager stores agent installation files on the core server. Handheld Manager supports two types of agent installations:

- Windows CE users can use a Web browser to directly run the installation .CAB file from the core server's LDLogon share. For example, <http://mycore/ldlogon/hh-mobile5.cab>.
- Both Windows CE and Palm users can receive client agents through a "push" installation. This method uses a standard software distribution script to deploy the Handheld Manager client agents to the handheld host computer. The next time the handheld synchronizes with that computer, it receives the handheld agent.

Because of platform differences between Windows CE devices, there are multiple Windows CE configurations you may have to manage. For Pocket PC 2002 devices, the .CAB filename is hh-ppc2002.cab. For Pocket PC 2003, 2003 Second Edition, or Windows Mobile 5.0 devices, the .CAB file name is hh-mobile5.cab.

Before deploying agents to Windows CE devices, you must create the handheld agent configuration .CAB files. This isn't necessary for Palm devices. The Windows CE agent configuration window is only available from the Management Suite console on the core server. Additional consoles won't display this window.

To create the agent configuration .CAB files

1. Click **Tools | Handheld | Windows CE agent configuration**.
2. In the left pane, click the configuration that matches the device you'll be deploying the agent to.
3. Click the **Create new agent CAB file** toolbar button.
4. Handheld manager copies the compiled cab files to the core server's LDLogon share.

Palm, Pocket PC, and Windows Mobile 5 devices use the steps below to remotely install device agents.

To remotely install handheld device agents using the software distribution method

1. Click **Tools | Distribution | Distribution Packages**.
2. Expand **My Distribution Packages**.
3. From the **SWD Package** short menu, click **New SWD package**.
4. Enter a name and description. Enter the path to the primary installer file for the handheld platform you're distributing to. The installer file must be saved in a null session share to use the UNC path. The installer file is saved by default at \\<core server>\LDLogon\. You can enter in the http path for this file to use this location (<http://<core name>/ldlogon>) followed by the name of the cab installation file:
 - For Windows CE devices, insert **LANDesk Windows Mobile 5 ActiveSync Client.exe** or **LANDesk Pocket PC 2002 ActiveSync Client.exe**
 - For Palm handhelds, insert **ldscnpalm-8.1-5.exe**
5. Click **Save**.
6. Click **Tools | Distribution | Scheduled Tasks**.
7. From the **My tasks** shortcut menu, click **Create software distribution task** for distributing the installer file.
8. Enter a task a name.
9. On the **Distribution package** page, select the distribution package you created previously.
10. On the **Delivery method** page, select the delivery method (you can select either a push-based distribution or a policy-based distribution) and then click **Save**.

11. Target the host computers individually or by using a query that returns the desired computers as its results.
12. Run the task.

After the job runs successfully, the next time the handheld synchronizes with the targeted host computer, the host will install the Handheld Manager agents. Note that you can create a query that returns computers with handhelds attached to them. You can then use this query as the target for a client agent distribution script.

- For Palm handhelds, query on **PDA | Palm OS | Version**, and select 4.0 or greater.
- For Windows CE devices, query on **PDA | Windows CE | Device Processor**, and select equals Arm.

Understanding Windows CE client agent installation

On Windows CE agent installations, Handheld Manager setup copies a .CAB file to the computer that a Windows CE device synchronizes with. The contents of this .CAB are installed on the Windows CE device the next time it synchronizes. The .CAB contains these files:

- **setup.dll**: Handles the install/uninstall events and custom installation for the agent.
- **wcetrigger.exe**: The scheduler runs every hour, by default. It launches programs in `ldlaunch.ini` based on their individual schedules.
- **wceagent.exe**: The auto-update agent that communicates with the core server.
- **wcescn.exe**: The inventory scanner runs once per day (based on the default settings within `ldlaunch.ini`). The scanner places the scan file, `ldcescan.txt`, in the LANDesk client folder on the device.
- **wcesdclnt.exe**: Software distribution agent that communicates with the core server. By default this checks with the core server for distribution jobs once an hour (based on the default settings within `ldlaunch.ini`). This component also handles importing and exporting registry settings.
- **wcedwnld.dll**: Used by `wcesdclnt.exe` and handles the file download.
- **ldlaunch.ini**: Text file that contains programs `wcetrigger.exe` should launch. By default, this file contains references to `wceagent.exe`, `wcescn.exe`, and `wcesdclnt.exe`. It also includes the launch frequency and the next launch time.
- **ldcfg.txt**: Text file that contains the fully-qualified domain name for the core server.
- **pkey.0**: This file contains the public key that is used to authenticate with the core server.

For handheld devices, these files are stored in the handheld's `\Program Files\LANDesk` folder.

Understanding Palm client agent installation

Palm handhelds only support inventory scans. Unlike Windows CE devices, Palm handhelds don't communicate with the core server directly. Palm handhelds have a small inventory scanner program on them that uses a HotSync conduit to pass inventory scan data to the computer the Palm handheld HotSyncs with. The Palm inventory scanner runs on each HotSync. The Management Suite inventory scanner includes the handheld inventory scan file when the host computer sends an inventory scan to the core server.

Handheld Manager Setup makes these changes to computers hosting Palm handhelds:

- Setup installs a HotSync conduit, ScannerConduit.dll. When the Palm device synchronizes with the desktop, the desktop inventory scanner uploads the scan file to the core server, where the Inventory service adds them to the database.
- Setup configures the Palm inventory scanner, Idscanpalm.prc, so that it gets installed to the handheld on the next HotSync.

Once Idscanpalm.prc is installed, it stores inventory data in palmscan.scn. During each HotSync, the Handheld Manager conduit copies this file to the host computer's C:\Program Files\LANDesk\LDClient\Palm\Transfer folder. The desktop inventory scanner looks here for scan files to send to the core server. This file gets overwritten each HotSync.

Using Handheld Manager

Once the agents are on handhelds, you can:

- Query handheld inventory data
- Distribute programs to Windows CE devices
- Transfer files to and from Windows CE devices

Querying for handheld inventory data

The Management Suite inventory scanner stores handheld inventory information in two places:

- Under the PDA attribute: This attribute contains handheld inventory data from computers that host handhelds. This information is limited, since it doesn't come directly from the handheld.
- In the standard device attributes: The handheld inventory scanners put inventory data in the normal device attributes. For querying on this data, use the same attributes you would use to query for computer data. Don't look for handheld inventory scanner data under the PDA attribute.

Distributing software to Windows CE devices

Handheld Manager software distribution to Windows CE devices supports these Management Suite distribution features:

- **Checkpoint restart:** Restarts interrupted distribution downloads at the point the download was interrupted.
- **Bandwidth throttling:** Controls the file transfer speed to limit the amount of network and handheld bandwidth used.
- **Packet sleep options:** Adjusts the interval between distribution network packets. Higher intervals slow down the packet rate, using less bandwidth.
- **Feedback options:** For .CAB installations, you can select whether files install silently or with whatever UI the .CAB was configured to show (typically a progress bar).

You can distribute programs or .REG registry files. After the file is on the handheld, Handheld Manager executes the .CAB or .EXE file, or it imports the registry file.

The \Program Files\LANDesk\Management Suite\LDHM\softdist folder on the core server is a read-only Web share that any client can access. Software distribution uses this folder to store files that you have scheduled for distribution to Windows CE devices. When you schedule a handheld distribution job in the Management Suite console, the console copies programs you're distributing to this share. The handheld distribution agent will retrieve the program from this share on the core server. You can't host files you want distributed to handhelds in a different location.

To access this web share directly, use the following URL: `http://<core-server>/ldhm-softdist/`.

Create a handheld distribution job from **Tools | Distribution | Scheduled tasks** in the Management Suite console. There's a **Schedule handheld task** button in this window that launches the handheld script wizard.

Before you can distribute software to handhelds, they must have the Handheld Manager client agents on them. Once they return an inventory scan, you'll be able to make Windows CE devices distribution job targets. Don't target the handheld host computer for handheld distribution jobs. You only need to target the host computer for initial handheld agent installation.

When you schedule a handheld distribution job, the job status reports "Working," and the result changes to "Policy has been made available." The next time `wcesdclnt.exe` is executed on the handheld device, it will check with the core server for available jobs, see the job you have scheduled, and start downloading the program. By default, `wcesdclnt.exe` runs once per hour (specified in `ldlaunch.ini`).

When the job finishes, the job status changes to "Done."

To distribute software to a Windows CE device

1. Copy the program you want to install to a Web share. The default share location on the core server is \Program Files\LANDesk\ManagementSuite\LDHM\Packages. This corresponds to the following Web share: `http://<core server>/ldhm-packages`.
2. Click **Tools | Distribution | Scheduled tasks**, and click the **Schedule handheld task** button. Browse to the program you want to install and click **Next**.
3. Enter a **Script name** and click **Next**.
4. Adjust the download options you want and click **Next**.
5. Finish the wizard.
6. From the network view, drag handheld clients that you want to receive the package to the task you created in the **Scheduled tasks** window.
7. From the task's shortcut menu, click **Properties** and configure the task or select **Run now**. Once the start time arrives, the job status will change to **Working** and the job results will change to **Policy has been made available**, indicating that the file has been made available to the handheld the next time the handheld distribution agent runs (the default is once an hour). You can force the agent to run by running `wcesdclnt.exe` on the handheld.

Understanding distribution options

When you create a handheld distribution script, the wizard includes a **Download options** page that has the bandwidth throttling options below. The defaults normally work fine since handheld packages tend to be small. If you want to adjust the bandwidth used, adjust these options:

- **Dynamic bandwidth throttling:** Specifies that the network traffic a client creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage** at 0, once the client initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops.
This option forces a full download of the file into the client's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted.
- **Minimum available bandwidth percentage to use on client:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the client. For example, if there were one other application consuming network bandwidth on the client during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the client application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.
- **Delay between packets (source):** Specifies the delay between the package source and client destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

Distributing registry files to Windows CE devices

You can send .REG registry files directly to Windows CE devices. The format of these files matches the standard Windows registry export format with two exceptions. Instead of the normal Windows registry format header, the first line of Windows CE-based .REG files must start with one of the following strings:

- **LDHM Generic Registry File:** Installs to all Windows CE devices
- **LDHM Handheld Registry File:** Installs only to handheld Windows CE devices
- **LDHM <DeviceType> Registry File:** Installs only to the device type specified.

The string you specify affects which devices the registry file will be applied to. If you distribute a registry file to a device that isn't covered by the header you specify, the device will ignore the registry file and delete it.

The second exception is that binary data in a file to be imported by wcesdclnt.exe must all be on the same line, as opposed to the standard desktop registry file that puts eight or sixteen bytes per line.

Here is a sample registry file:

```
LDHM Registry File

[HKCU\Software\LANDesk]
"Test String"=sz:"This is a test"
"Another"=sz:This is a test
"Test DWORD"=dword:00000400
"Test Binary"=binary:3c,4a,88,f0,00,00,45
```

Transferring files to and from Windows CE devices

Handheld Manager's file exchange feature lets you transfer files from Windows CE devices to the core server. To send files to Windows CE devices, you must first package them into a .CAB file and distribute the .CAB file to the devices.

Sending files to Windows CE devices

Before sending files to Windows CE devices, Handheld Manager bundles them in a standard .CAB format, which then gets installed on the Windows CE device. The .CAB includes the file and the path on the Windows CE device the file should be installed to. Any existing files in the same path with the same name are overwritten.

Sending files to Windows CE devices requires two steps:

- Create a .CAB file containing the files you want sent
- Distribute the .CAB file to the Windows CE devices that need it

To create a .CAB

1. Click **Tools | Handheld | Windows CE CAB creator**.
2. In the **Windows CE CAB creator** window, click the **Launch CAB creation wizard tool** toolbar button.
3. Enter the .CAB name.
4. Select a file to include by browsing for it or typing in the path and filename.
5. Enter the destination path on the Windows CE device. Don't include the filename.
6. Click the **Add** button to add it to the .CAB.
7. Repeat steps 4-6 for each file you want the .CAB to install.
8. Click **Create** when you're done adding files to the .CAB.
9. The CAB file is created on the core server at \Program Files\LANDesk\ManagementSuite\LDHM\Packages. This corresponds to the following Web share: http://<core server>/ldhm-packages.

Once you've created a .CAB, distribute it as described in "[Distributing software to Windows CE devices](#)". **Retrieving files from Windows CE devices**

Handheld Manager's file exchange feature allows you to retrieve files from Windows CE devices. The **Configure handheld file exchange** dialog manages the file list. There is only one backup list and it applies to all Windows CE devices. Any changes you make are immediately applied once you click **Apply** or **OK**. Windows CE devices send the files you specified to the core server when they do their next scheduled inventory scan.

When you use handheld file exchange to retrieve files from the Windows CE device, they're copied to this location on the core server:

- \Program Files\LANDesk\ManagementSuite\LDHM\filex\<letter of alphabet>\<login name>\<GUID>

Handheld Manager creates an alphabetical directory structure under the `..filex` folder. Each letter contains a subfolder matching the login name for the user logged in when the device uploaded files. If the login name isn't available, there's a `<GUID>` folder that contains folders named with the Windows CE device's Windows GUID (Globally Unique Identifier).

When saving Windows CE device files on the core server, Handheld Manager resets the file date and time to match the time it was created on the core server. By default, Handheld Manager will keep backup versions of files for three days. Backups are renamed with a `.bak.0001`, `.bak.0002`, `.bak.0003`, and so on extension. The most recent backup will have the `.bak.0001` extension. Backup files are not deleted until there are 9999 of them, where the oldest gets deleted upon each new file being saved.

To retrieve files from Windows CE devices

1. Click **Configure | Handheld file exchange**.
2. To add a file, enter its path and filename on the Windows CE device and click **Add**.
3. To remove an existing file, select it in the list and click **Remove**.
4. Change the delay and buffer size if necessary. These options control the amount of network bandwidth Windows CE devices use to transfer files.
5. Click **OK** when you're done.

Working with Windows CE agent configurations

The Windows CE agent configuration window (**Tools | Handheld | Windows CE agent configuration**) helps you create `.CAB` agent configurations. The file list in this window corresponds to the folder structure under this path on the core server:

- `\Program Files\LANDesk\ManagementSuite\LDHM\clients`

These folders contain the Handheld Manager agent configuration files for each platform. Files in these folders are synchronized with managed devices when the `wcesdclnt.exe` agent runs. If you add additional files to these folders, those files will be copied to the default installation path on managed devices. You can't change the path that additional files will be placed in. If you want to place files in these folders but you don't want them copied to devices, you can add filenames to `exclude.txt` in the same folder.

Additional files won't be made part of the agent installation `.CAB` file unless you also modify the device `.INF` installation file in the same folder.

Changing the Windows CE inventory scan frequency

The `wcetriggr.exe` file launches programs based on their individual schedules defined in `ldlaunch.ini`. The scheduler interval, by default, is set to run every hour. You can change the scheduler interval by changing this registry key:

- `HKLM\Software\LANDesk\Handheld Manager\Schedule Interval (Minutes)`

This key uses a numeric `DWORD` value for the number of minutes between `wcetriggr.exe` checks. Note that reducing the amount of time between checks will increase battery power consumption.

The ldlaunch.ini file contains one application (and path) per line with its run-time parameters that will get executed by the wcettrigger.exe. The line containing wcescn.exe controls the inventory scanner, and the line containing wcesdclnt.exe controls the software distribution agent.

The file format is as follows:

- `\Program Files\landesk\wceagent.exe|daily|6/4/2004`
- `\Program Files\landesk\wcescn.exe|daily|6/4/2004`
- `\Program Files\landesk\wcesdclnt.exe|hourly|6/4/2004 14:00`

Each line is broken up into three parts; the executable, modifier, and next scheduled date/time.

- The executable can be any application (.exe) on the device. You must use the full path to the file.
- The modifier specifies how often to run this application. The modifier can be one of the following: hourly, daily, weekly, monthly, and yearly. It can also be a numeric value indicating the number of hours or minutes between each execution. Including an 'm' after the number will indicate minutes (requires the scheduler interval registry change described earlier).
- The next scheduled date/time value denotes the earliest time that the application can run again. This value is automatically updated by the trigger each time it is run. If you leave this value empty, the program will run at the next interval.

Here are some more examples:

```
\myapp.exe|2|12/05/2005 15:00
```

This will execute myapp.exe every two hours. It will run again the first time the trigger runs after 3:00 PM on 12/05/2005. If it runs successfully, the trigger will update the next scheduled date/time value to 17:00. If it isn't successful the trigger will run it again every time the trigger itself runs, until it is successful.

```
\myapp.exe|15m|12/05/2005 15:30
```

This will execute myapp.exe every fifteen minutes.

```
\myapp.exe|hourly|12/05/2005 15:00
```

This will execute myapp.exe every hour.

```
\myapp.exe|daily|12/05/2005
```

This will execute myapp.exe every day, only once.

Note: When changing an application to run more frequently than once per hour, you must set the registry value described above.

When customizing the ldlaunch.ini file with your own programs, each application is responsible to check if a network connection is available on its own. The trigger runs on its schedule regardless of network connectivity. If a non-zero return value is received by the application being run, it will be run again every time the trigger runs until successful.

Working with BlackBerry devices

Handheld Manager can do inventory scans on BlackBerry devices that run Platform 1.6 or 1.7. The scanner reports the device type, version, OS, battery info, network connection, display type and resolution, installed software, and other data.

Handheld Manager's BlackBerry support requires that your network have a BlackBerry Enterprise Server (BES). The BES allows BlackBerry devices to communicate with the Management Suite core server.

The BlackBerry agent consists of three files in the ldhm-packages share on the core server:

- com_Landesk_LdBbScanner.cod
- com_Landesk_LdBbScanner.jad
- com_Landesk_LdBbScanner.alx

The easiest way to have clients install the scanner is to send them an e-mail such as the following:

```
Please click on the following link to install the LANdesk Inventory
Scanner for BlackBerry/RIM devices:
http://<coreserver>/ldhm-packages/com_Landesk_LdBbScanner.jad
Once the scanner installs, open the LANdesk Inventory Scanner from the
ribbon bar.
From the scanner's menu, select Configure Scanner and do the following:
Enter <your core server name> in the Core Server field.
Enter your name in the Owner Name field.
Select Scan Device from the main menu.
```

You can also have users install the scanner from the BlackBerry Desktop Manager. Use the application loader and browse for \\coreserver\LDMain\LDHM\Packages\com_Landesk_LdBbScanner.alx. Finish the wizard to install the scanner.

Once users install the scanner, it appears in the device's ribbon bar. Users must enter the core server name and owner name for the scanner to work. The scanner can run without any other information.

If users don't enter configuration information or the scanner can't contact the core server, the next time the scanner runs it will display the configuration screen and prompt for updated configuration information.

Scanned BlackBerry devices appear in the network view. Their device name is the BlackBerry 7-digit PIN. To preserve battery, the inventory scan does not run automatically. It must be manually run from the device.

Handheld Manager for hybrid phone/pda devices

LANdesk Handheld Manager is the combination of software embedded in the standard LANdesk Management Suite install and the enhanced LANdesk Handheld Manager which is available for download. This feature is designed specifically to synchronize with hybrid phone/PDA devices. Once the handheld agents are deployed by the enhanced Handheld Manager, the following functionality is added to the console:

- **Handheld Management** toolbox entry: This button will be added to the Handheld subheading in the Toolbox and links directly to the online LANDesk Handheld Manager console.
- **Right-click functionality:** You can right-click any supported handheld device in the LDMS console's network view

LANDesk Application Virtualization

LANDesk Application Virtualization is a LANDesk Management Suite add-on product that is sold separately by LANDesk Software. LANDesk Application Virtualization uses Thinstall technology to virtualize an application, storing it in a single self-contained executable with the application and .DLL/device driver dependencies.

When run, virtualized applications run in an isolated environment without making changes to the Windows installation they're run on. Virtualized applications even run on locked-down devices without requiring additional privileges.

For more information, see the documentation that accompanies LANDesk Application Virtualization. When you use LANDesk Application Virtualization with Management Suite, you can deploy and manage virtualized applications.

Read this chapter to learn more about:

- [Distributing virtualized applications](#)
- [Using inventory and software license monitoring with virtualized applications](#)
- [More information on virtualized applications](#)

Distributing virtualized applications

Virtualized applications generally consist of one or more executable files. You can use software distribution to deploy these virtualized application executables to managed devices. You can use any of the software distribution delivery methods with virtualized application packages, including run from source. When you deploy a run from source virtualized application package, managed devices use a application shortcut icon to run the virtualized application executable over the network.

To create a virtualized application package

1. Use LANDesk Application Virtualization to create your virtualized application executable.
2. Click **Tools | Distribution | Distribution Packages**.
3. From the shortcut menu of the package group you want, click **New distribution package | New virtualized application package**.
4. In the **Distribution package** dialog, enter the package information and change the options you want. Note that you must enter the package name, description, and primary file. For more information on each page, click **Help**.
5. The **Shortcut** page is the only page specific to virtualized applications. Enter the shortcut icon **Name**. You can also specify if you want the icon on the **Desktop** and/or in the **Start menu**. If you check Start menu, you also can enter the **Programs folder name** that will contain the shortcut. The folder path you enter appears under **All programs**.
6. Click **OK** when you're done. Your script appears under the tree item for the package type and owner you selected.

When you deploy a virtualized application, software distribution copies the executable(s) to this folder on managed devices:

- %programfiles%\LANDesk\VirtualApplications\

The full virtualized application path includes the software distribution source path to help prevent problems with duplicate filenames. For example, if your distribution source path was vapps\myapp.exe, the path on managed devices would be %programfiles%\LANDesk\VirtualApplications\vapps\myapp.exe.

You can change the default virtualized application path if necessary in the **Agent configuration** dialog's **Software distribution** page.

Some virtualized applications require multiple executables. If that's the case, you can create a separate distribution package for these additional virtualized application executables. Then, when you create a distribution package for the main virtualized application executable, you can then include any additional dependent executables packages as dependencies. That way, if the dependent executables aren't already there, they'll be installed automatically.

Dependent executables need to be in the same shared folder when the distribution packages are created. This ensures that the dependent packages are distributed to the same folder on the managed device. If the dependent executables aren't in the same folder on the managed device they won't run.

The first time someone runs a virtualized application on a device, the "Thinstall runtime license agreement" dialog appears. Users need to click **Continue** to run the virtualized application. Users should only have to do this once.

Using inventory and software license monitoring with virtualized applications

Virtualized application executables created with LANDesk Application Virtualization have additional property information that helps Management Suite inventory and software license monitoring. In Windows Explorer, if you right-click a virtualized application executable and click **Properties**, there is additional version information:

- **ThinstallLicense:** LANDesk Application Virtualization license type and registration e-mail address.
- **ThinstallVersion:** LANDesk Application Virtualization packager version used to create this package.

You can use this information in your inventory queries to find virtualized applications that were scanned by the inventory scanner. Generally, virtualized application executable properties mirror those of the main executable inside the virtualized application. In the inventory view for a device, virtualized applications appear in the **Software | Package** list. Virtualized applications in this list have a "Virtual Application" attribute with a value of "Yes".

However, some applications don't provide version information before they are virtualized. In this case, they won't show up as virtualized applications in inventory even though they are virtualized.

Virtualized application executables will be scanned by the inventory scanner automatically only if you're using MODE=ALL inventory scanning. If you aren't using MODE=ALL and you want virtualized application inventory information in the database, you'll need to manually add the virtualized application executable information to software license monitoring's **Inventory | Files | To be scanned list**. The inventory scanner only sees the virtualized application executable. It doesn't scan within the executable.

Software licence monitoring will automatically discover virtualized applications and include them in the **Product definitions | Autodiscovered** list. Software license monitoring's automatic application discovery doesn't use the inventory scanner. Software license monitoring does this by detecting the Start menu or desktop shortcut to the application.

A discovered virtualized application in the **Automatically discovered** list will only have the single virtualized application executable in its files list, but the product definition will still be based on the product within the virtualized application executable. Software license monitoring doesn't look inside the virtualized application executable and so it can't include other files that might normally be assigned to a product when it is installed without virtualization.

More information on virtualized applications

Virtual application sandbox

By default, virtualized applications create temporary files necessary for them to run under this folder:

- Documents and Settings\

The inventory scanner doesn't scan this folder to prevent false reports of applications on the system.

Using non-LANDesk versions of Thinstall

The LANDesk Application Virtualization version of Thinstall has customizations that are specific to Management Suite. Other versions of Thinstall virtualized applications may not work correctly with software license monitoring or the inventory scanner.

LANDesk Inventory Manager

LANDesk Inventory Manager is a version of LANDesk Management Suite 8 that contains only these inventory-related features:

- Inventory scanning and inventory-related console features
- Custom data forms
- Software license monitoring
- Unmanaged device discovery
- Reports for the above features

The Inventory Manager installation on a core server contains all LANDesk Management Suite 8 components, but when you activate a core server with an account that is licensed for Inventory Manager, the non-Inventory Manager features aren't applicable or visible in the Management Suite and Web consoles.

If you're using Inventory Manager, refer to the sections that correspond to the list of features above. Typically, you can recognize the information that doesn't apply in each chapter because those sections refer to Management Suite features like software distribution and remote control that aren't part of Inventory Manager.

Appendix A: Additional inventory operations and troubleshooting

LANDesk uses an inventory scanner utility to gather hardware and software information for the devices on your network. For information on inventory scanner basics, see the "Managing inventory" on page 114 and "Reports" on page 123 chapters. This chapter provides additional information about inventory scanning, as well as some troubleshooting tips.

Read this chapter to learn about:

- "Scanning custom information" on page 595
- "Specifying the software scanning interval and history" on page 596
- "Scanner command-line parameters" on page 597
- "Scanning standalone devices with a floppy disk" on page 599
- "Adding inventory records to the core database" on page 599
- "Adding BIOS text strings to the core database" on page 599
- "Creating MIF files" on page 600
- "Scanning NetWare servers" on page 601
- "Editing the LDAPPL3.TEMPLATE file" on page 602
- "Troubleshooting the inventory scanner" on page 604

Scanning custom information

The Windows inventory scanner utility (for Windows 95/98 and Windows NT/2000/2003/XP) automatically scans the device's registry for custom information. When you configure a device, the following keys are installed into the registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\INTELLANDESK\INVENTORY\CUSTOM FIELDS

The inventory scanner always scans the registry for the Custom Fields key and picks up any information it finds under that key. It then enters the custom information into Custom fields in the core database. The information content doesn't matter. When you view this data in the console, it displays under Custom fields.

The inventory scanner reads two data types:

- REG_SZ
- REG_DWORD

Custom field subkeys

The inventory scanner doesn't scan for any subkeys below Custom fields.

Custom fields string length

ASCII character strings must be no longer than 255 characters. Multi-byte character set (MBCS strings must be between 127 and 255 characters).

Configuring the scanner to scan registry keys

The inventory scanner can scan for registry keys you specify and add their values to the core database. This can be useful for customized software, asset information, or other information stored in the registry that you want to include in the core database.

To use registry key scanning, add a section at the very beginning of the LDAPPL3.TEMPLATE file with this format:

```
[Registry Info]
KEY=HKLM, Software\Intel\LANDesk, version, MyData - LANDesk - Version
```

Change the values after KEY= to match the registry key you're looking for. In the example above, notice that each registry key element is separated by commas.

When the inventory scanner retrieves the registry key data, you can view it in the path specified by the last parameter. Each level is separated by " - " (space dash space). To force the scanner to use a 64-bit hive, append 64 to the hive name. For example, HKLM64.

Specifying the software scanning interval and history

You can specify when to scan a device's software and how long to save the inventory changes history log on the core server. These intervals apply to every device.

Note: A device's *hardware* is scanned every time it boots and is connected to the network.

To specify the software scanning settings

1. In the console's network view, click **Configure | Services | Inventory | Software**.
2. Specify the frequency of software scanning.
3. Specify the number of days to save the history.

The core server and software scanning

This feature affects only devices. It doesn't affect the core server, which is always scanned daily.

Scheduling an inventory scan task

If the device is running the LANDesk agents, you can schedule a script that triggers an inventory scan on devices.

To schedule an inventory scan

1. Click **Tools | Distribution | Manage scripts**.
2. Click **All other scripts**.
3. From the inventoryscanner script's shortcut menu, click **Schedule**.
4. Configure task targets and the start time in the **Scheduled tasks** window.

The inventory scanner script is located in the \Program Files\LANDesk\ManagementSuite\Scripts directory. The script is a Windows .INI file that you can edit with any text editor. If you need to change the options or parameters within the script, open it and follow the instructions contained within it.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner's (LDISCN32.EXE) shortcut properties to control how it functions.

The following table lists the scanner's command-line parameters:

Option	Description
/NTT=IP	Core server's IP address or DNS name and UDP port. For example, /NTT=123.123.123.123:5007 or /NTT=CORESERVER:5007. The OS/2 scan utility, LDISCAN2.EXE, and DOS scanner utility, LDISCAN.EXE, don't use this parameter.
/UDP	Scanner communicates via UDP instead of TCP. Combine this switch with /NTT=[IP].
/NOUI	Forces the scanner to run with no user interface.
/i=inifile	Provides the path (HTTP, UNC), or a drive letter to the master LDAPPL3 file. LDISCN32.EXE also copies the LDAPPL3 file they find in this location to the device's local LDAPPL3.INI file. The scanners compare the date of the master LDAPPL3 with the local LDAPPL3.INI; if the dates don't match, the master file is copied locally.
/d=directory	Starts the software scan in the specified directory. By default, the scan starts in the root directory of each local hard drive.
/L	Sends the scan to the core server the device was configured from. When you use /L, the /NTT parameter isn't necessary.
/sync	Forces a full scan, including a complete software scan. Full scan files can be several megabytes in size.
/n	Doesn't search subdirectories.

Option	Description
/v	Verbose mode.
/Z=retry count	How many times the scanner tries to resend the scan.
/W=wait in seconds	Have the scanner wait the number of seconds specified before starting a scan.
/? or /h	Displays the command-line syntax help.
/s=servern ame	Specifies the core server to store the inventory data on.
/f	Forces a software scan regardless of the software scan interval set at the console. Specify /f- to disable a software scan regardless of the software scan interval set at the console.
/t=[path]fil ename	Copies the contents of the specified file to the core database. Use this option to enter inventory data from standalone devices or from separate inventory files.
/o=[path]fil ename	Writes inventory data to the specified output file.
/m	Creates a non-unicode LDISCAN.MIF file in the C:/DMI/DOS/MIFS directory. This file contains the inventory data discovered during the scan.
/muni	(LDISCN32.EXE only) Creates a unicode LDISCAN.MIF file in the directory found in LDAPPL3.INI file's MIFPATH. This file contains the inventory data discovered during the scan.
/do16	Enables the 16-bit inventory scanner (inv16.exe) on managed devices.

Scanning standalone devices with a floppy disk

To scan a standalone device

1. Copy the proper inventory scanner utility and a software description file (usually LDAPPL3.INI) to a floppy disk. (You may also need to copy ELOGAPI.DLL, YGREP32.DLL, LOC16VC0.DLL, INV16.EXE, LOC32VC0.DLL, LTAPI.DLL, and LDISCN32.EXE.)
2. Run the scan with the **/O= parameter** specifying the path and filename of the output file.
3. At the command-line prompt, enter a **unique name** for the device. This name is saved in the LDISCAN.CFG file on the device's local drive. This name also appears in the Description field in the core database. For example:

```
ldiscn32.exe /f /v /o=c:\%computername%.scn
```

Adding inventory records to the core database

You can add inventory information from a standalone device or separate inventory files by running the inventory scanner from the operating system command line.

To add inventory records from a file to the core database

- Run the scan utility with the **/S=**, **/T=**, and either the **/NTT** or **/NTI** parameters.

Adding BIOS text strings to the core database

There is a section in the LDAPPL3.TEMPLATE file called [BIOS Info]. This section provides the capability to search for information inside the BIOS of a computer. You can add one or more entries to the [BIOS Info] section. These entries define new keys in the core database and provide parsing instructions to the inventory scanner. The parsing instructions identify where to look in the LDBIOS.TXT file for a specific string. Using these instructions, the inventory scanner populates the core database with the strings from the LDBIOS.TXT file.

The inventory scanner uses a parsing method to locate BIOS information. This allows you to search for information one or more lines away from a specified text string. Such a search would enable you to locate random letter and number combinations assigned to computer hardware.

Text strings in LDBIOS.TXT

If you run the inventory scanner with the **/do16** command line parameter, during an inventory scan, the text strings available in the BIOS are exported to a text file called LDBIOS.TXT. This hidden file is stored in the same location as the LDISCAN.CFG file, which is by default the root of the C: drive. LDBIOS.TXT stores all of the strings that are created by the scanner. If you want to store this information in the database, you can store it as a configuration file by using the CFGFILES parameter in LDAPPL3.INI.

Sample of BIOS entries in the LDAPPL3.TEMPLATE file

Here is an example from the [BIOS Info] section in the LDAPPL3.TEMPLATE file:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell
[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*\ (AMI|American Megatrends\ )
[BIOS - Dell]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \ (A.+)\ ::\1
Value = BIOS Version: \ (A.+)\ ::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*Dell|[Cc]opyright.*Dell
```

Understanding BIOS entries

Entries in the [BIOS Info] section consist of the following:

- **[Section name]:** Identifies a new component in the core database.
- **StringLength=:** Specifies the minimum length of the strings to search for.
- **Key=:** Identifies the class and attribute name of the information returned from searching the LDBIOS.TXT file.
- **Parameters=:** Specifies the search criteria that tells the scanner where and how to search for values associated with a specific key.
- **Value=:** Specifies the value that is searched for in the BIOS. A value has three main sections, each separated by a double colon character (:). The strings identified in the value entry are case-sensitive. All characters in the value, even spaces, are included in the search unless they are an operator.

Creating MIF files

If you need a MIF file that stores a device's inventory information, you can create one by running the appropriate scanner at the command line.

To create a unicode MIF file, use the /MUNI option. To create a non-unicode MIF file, use the /M option.

To create MIF files

- Enter this at a DOS prompt:
LDISCN32/MUNI /V

Scanning NetWare servers

LANDesk uses LDISCAN.NLM to scan NetWare servers for hardware and software information. The command-line syntax for LDISCAN.NLM is:

```
LOADLDISCAN[.NLM]INV_SERV=servername
NTI=IPXaddressFILE=path[TIME=#][SCANNOW][MIF]
```

The following table lists the command-line parameters that you can use with the NetWare scanner.

Option	Description
INV_SERV = serenade	Directs the results of the scan to the specified server. The specified server must be running the inventory service.
NTT = IP address	Gives the IP address of the core server to send the inventory information to.
FILE = path	Lists the path to the LDAPPL3.INI file.
TIME = #	Sets the time of day for the server hardware scan in whole hours. The clock is in military time, so 0 = midnight and 23 = 11 p.m. Configure software scans in Options Software Scanning. The default is 8 p.m.
SCANNOW	Forces an core server scan at the time the NM is loaded.
MIF	Creates the LDISCAN.MIF file for the core server. The .MIF file contains the inventory information gathered from the server.

To load LDISCAN.NLM on a NetWare server

- From the server console, enter the proper syntax at the LDISCAN.NLM command line.

For example, to scan a server daily and record its inventory data in the core database on "Server1," enter:

```
LOADLDISCANINV_SERV=SERVER1TMEWORK
NUMBER:NODEADDRESS:SOCKETFILERS:MONEYCHANGER
```

To unload LDISCAN.NLM from a server, enter:

```
UNLOADLDISCAN
```

Scheduling NetWare server scans

LDISCAN.NLM scans recur every day as specified by the TIME=# parameter. The TIME parameter is set in military time, so 0 is midnight and 23 is 11 p.m. The default is 8 p.m.

To change the time for server scans

- Add the TIME = # parameter to the load LDISCAN.NLM entry of LD_AUTO.NCF.

Editing the LDAPPL3.TEMPLATE file

Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3 file to identify a device's software inventory.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in this directory on the core server:

- \Program Files\LANDesk\ManagementSuite\LDLogon

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
Mode	<p>Determines how the scanner scans for software on devices. The default is Listed. Here are the settings:</p> <ul style="list-style-type: none"> • Listed: Records the files listed in LDAPPL3. • Unlisted: Records the names and dates of all files that have the extensions listed on the ScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network. • All: Discovers files with extensions listed on the ScanExtensions line.
Duplicate	<p>Records multiple instances of files. Set the value to OFF to record only the first instance, or ON to record all detected instances. The default is ON.</p>
ScanExtensions	<p>Sets the file extensions (.EXE, .COM, .CFG, etc.) that will be scanned. Use a space to separate the file extensions. By default, only .EXEs are scanned.</p>

Option	Description
Version	Is the version number of the LDAPPL3 file.
Revision	Is the revision number of the LDAPPL3 file; helps ensure future compatibility.
CfgFiles 1-4	<p>Records the date, time, file size, and contents of the specified files. You can leave out the drive letter (for example, c:) if you want to search all local drives. You can specify more than one file on each of the four lines, but the line length is limited to 80 characters.</p> <p>Separate path names on the same line by a space.</p> <p>The scanner compares the date and size of the current file with that of the previous scan. If the date and size don't match, the scan records the contents of the file as a new revision.</p>
ExcludeDir 1-3	Excludes specific directories from a scan. You can leave out the drive letter (for example, c:) if you want to exclude all local drives. Enumeration must start at 1 and be continuous. You can use environment variables in this format: "%varname%". You can use a wildcard (*) in a "begins with" form only (ExcludeDir=%windir%\\$NtUninstall*). You must end each line with "\".
MifPath	Specifies where MIF files are stored on a device's local drive. The default location is c:\DM\DOS\MIFS.
UseDefaultVersion	If set to TRUE, the scanner reports a match when a file matches an exact filename and file size entry in LDAPPL3 on filename only (the version will be reported as EXISTS). This can cause some false positives for applications that share a common filename with an unknown application. In the as-delivered LDAPPL3.TEMPLATE file, this parameter is set FALSE; that is, only add an entry if the match is exact. If the parameter is missing, it defaults to TRUE.
SendExtraFileData	If set to TRUE, sends extra file data to the core server. The default is FALSE. This means that by default, only path, name, and version are entered into the core database.

To edit the LDAPPL3.TEMPLATE file

1. From your core server, go to the LDLogon directory and open LDAPPL3.TEMPLATE in Notepad or another text editor.
2. Scroll down to the parameter you're interested in updating and make your changes.
3. Save the file.
4. In the console, click **Tools | Reporting/Monitoring | Software License Monitoring**.
5. Click the **Make Available to Clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Troubleshooting the inventory scanner

This section describes common inventory scanner problems and possible solutions.

The inventory scanner hangs

- Make certain that you aren't including the old /DELL or /CPQ options on the command line. These options are no longer supported.
- Scan to a file using the /O= parameter. This may show a conflict with the network card or the network.

A device's hardware scans correctly, but its software doesn't

- Verify that the core database is configured to do a software scan now, and use the /f parameter to force a software scan.
- Scan to a file using the /O= parameter. This should list all of the software at the end of the file.
- Verify that the device is not trying to scan in a binary file in LDAPPL3.TEMPLATE's CfgFiles parameter.

The network view provides inventory data for only some devices

To view device information, ensure that your devices have been scanned into the core database. Devices appearing without information haven't been scanned into the core database.

To view a device's inventory data in the network view

1. Configure the device.
2. Scan the device into the core database.

For more information about configuring devices

Refer to "Configuring device agents" on page 86.

For more information about scanning devices

Refer to "Managing inventory" on page 114.

Specifying the number of days to keep inventory scans

By default, the core server keeps inventory scans for devices until you delete them. You can have the core delete inventory scans for devices if the device hasn't submitted a scan for the number of days you specify. Doing this can remove devices that are no longer on your network.

To specify the number of file revisions to keep in the core database

1. Click **Configure | Services | Inventory**.
2. Specify the **number of days** you want to keep inventory scans.
3. Click **OK**.

Changes to the way the inventory scanner gathers BIOS information

Beginning with LANDesk Management Suite 8.7 SP3, the inventory scanner no longer uses the 16-bit inventory scanner to gather some BIOS information. By default, the scanner no longer reports on motherboard bus number, motherboard bus device attributes, and the size of attached floppy drives. Also, the inventory scanner no longer creates a hidden LDBIOS.TXT file on managed devices containing a list of BIOS strings.

If you want the inventory scanner to once again report on these options and create the LDBIOS.TXT file, you can run the inventory scanner with the /do16 switch.

Appendix B: Additional OS deployment and profile migration information

The chapter provides supplemental information about LANDesk's OS imaging and profile migration capabilities.

Read this chapter to learn about:

- "Creating an imaging boot disk" on page 606
- "Adding application package distributions to the end of an OSD script" on page 607
- "Using CSVIMPORT.EXE to import inventory data" on page 607
- "Creating custom computer names" on page 608
- "Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values" on page 609
- "Using images in mixed uniprocessor and multiprocessor environments" on page 609
- "Adding network adapter drivers to the DOS boot environment" on page 610
- "Adding network adapter drivers to the Windows PE boot environment" on page 612
- "Using the LANDesk imaging tool for DOS" on page 613
- "Using the LANDesk imaging tool for Windows" on page 616
- "Understanding the Windows PE preboot environment" on page 619

Additional OS deployment procedures

Creating an imaging boot disk

LANDesk OS deployment (OSD) includes a boot disk creation utility that allows you to easily create a disk you can use to boot devices into a managed state in LANDesk network. You can use this boot disk to continue OSD jobs on devices that do not have an operating system or that failed a job for some reason and are no longer bootable. Once you boot a device with this boot disk, you can schedule a job for it.

Note: A user must have administrator rights on the core server if they want to create an OSD boot disk (even if they already have the OS Deployment right).

Boot disks are associated with the core server where they were created. If you have multiple core servers, use a boot disk created from the core server you want the device to report to.

To create an imaging boot disk

1. Click **Tools | Distribution | Manage Scripts**.
2. In the Manage Scripts window, click the **Create Boot Floppy** toolbar button to open the Create Imaging Boot Disk dialog.
3. Insert a 1.44 MB diskette into the floppy disk drive and make sure the destination floppy drive is correct.

Note: All data on the diskette will be erased.

4. Select the network adapter you want this boot floppy to support. Each floppy can only support one adapter because of disk space limitations.
5. Click **Start**. The Status box indicates the progress of the disk creation.
6. When finished, click **Close** to exit the dialog.

Adding application package distributions to the end of an OSD script

You can easily make an Enhanced Software Distribution (ESWD) application package distribution part of your OS deployment script.

To add ESWD packages to an OS deployment script

1. Open your package script in the LANDesk/ManagementSuite/Scripts directory and copy the REMEXECx= package distribution lines.
2. Edit your script by right-clicking it in the Manage Scripts window and clicking **Advanced edit**.
3. Paste the ESW REMEXEC commands at the bottom of your script, changing the REMEXEC numbering so that the numbers are sequential.
4. Insert a line before the ESWD lines you pasted in for LDSLEEP, similar to below. This allows time for the OS to finish booting before starting the package installation.

```
REMESECxx=LDSLEEP.EXE 120
```

Replace xx with a unique sequential number.

Using CSVIMPORT.EXE to import inventory data

LANDesk includes a command-line utility that allows you to import inventory data into the core database. This can be useful if you're installing new devices and you have information like MAC addresses available. You can use CSVIMPORT.EXE to import this data to the core server so you can target devices ahead of time for OS deployment jobs.

CSVIMPORT.EXE requires a template file describing the field contents and what columns in the core database the data should go in. CSVIMPORT.EXE also requires the .CSV file containing the data matching the template file you specify. CSVIMPORT.EXE creates miniscan files that you can then copy to the LANDesk/ManagementSuite/LDScan directory so they get added to the core database.

Sample template file:

```
Network - NIC Address = %1%  
Network - TCP/IP - Adapter 0 - Subnet Mask = 255.255.255.0  
BIOS - Serial Number = %2%  
BIOS - Asset Tag = %3%  
Display Name = %4%
```

Note that you can include custom data in the files. The entries %1, %2, and so on refer to the first, second, and so on columns. The subnet mask in this case will be applied to all entries as 255.255.255.0. The template file can't have any header text other than the actual template information.

Sample .CSV file:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1
0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2
0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3
0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4
0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5
0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Run CSVIMPORT with these three parameters: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. If you want the output to be entered in the core database immediately, specify your LANDesk/ManagementSuite/LDScan directory for output.

Creating custom computer names

The **Assign naming convention for target computers** page of the OS Deployment/Migration Tasks wizard lets you create computer names based on MAC addresses, text you enter, and counters (nnn...). You can also create names based on inventory data for asset tags, serial numbers, and login names by creating a COMPUTERNAME.INI file.

COMPUTERNAME.INI syntax:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

The values returned by the .INI file substitute for the \$MAC token in the wizard's naming convention page.

You can only use the above three inventory values in the file. OS deployment checks the options in the numeric tok<x> order. All three of the above tokens don't have to be in the file. The first tok<x> option found that has an equivalent database entry substitutes for the \$MAC token for the device being imaged. For example, in the case above, if there were no asset tag or serial number entries in the database, but there was a login name, the login name would be used for the \$MAC token. If none of the options match, the MAC address is used for the \$MAC token.

The login name option returns the login name returned by the most recent inventory scan.

Using the nnn computer name token

The **Assign naming convention for target computers** page of the OS Deployment/Migration Tasks wizard includes an nnn option that substitutes for a 3-15 digit number, depending on how many n characters you specify. For each computer name template you use in the wizard, OS deployment keeps a running counter of the numbers used. This way, subsequent jobs continue where the last job left off.

Every unique template has its own counter. If you always use the same template, the counter will span jobs. If you change your template after deploying some devices and later decide to go back to the template you originally used, the counter remembers where you left off for that template and continues counting.

Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values

The SYSPREP.INF contains a [RunOnce] section that specifies programs to run after the device boots for the first time. If you add your own programs to that section, you can include database tokens on the program command line if they're useful to the program you're running. OS deployment substitutes the token you specify with corresponding information from the core database.

Sample tokens:

```
%Computer - Device Name%
%Computer - Login Name%
%Computer - Manufacturer%
%Computer - Model%
%Computer - Type%
%Computer - BIOS - Asset Tag%
%Computer - BIOS - Service Tag%
%Network - TCPIP - Address%
%System - Manufacturer%
%System - Model%
%System - Serial Number%
%Processor - Processor Count%
%Computer - Workgroup%
%Computer - Domain Name%
```

You can chain multiple tokens together. For example, to separate two tokens by a colon: %Computer - Workgroup%:%Computer - Device Name% could return MyWorkgroup:MyComputer.

Note: You should only use tokens that return a single value.

Using images in mixed uniprocessor and multiprocessor environments

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP images. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

Note: The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's UNATTEND.TXT file for more details. Generally, you need to remember the following when sharing uniprocessor and multiprocessor images: **Both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.**

To configure multiple processor information

1. In the Sysprep file information page of the OS Deployment/Migration Tasks wizard, select **Configure advanced multiprocessor options** and then click **Next**.
2. In the Configure multiprocessor information page, select whether you're deploying a **Windows 2000** or a **Windows XP** image.
3. Select whether the image you're using was created on a **Uniprocessor** or **Multiprocessor** device.
4. Your source and target devices have the same HAL. If your image was created on an APIC ACPI device, select **APIC**. If your image was created on a non-ACPI APIC device, select **MPS**.

Adding network adapter drivers to the DOS boot environment

There are three network adapter driver detection phases that occur during on OS deployment job, as follows:

Phase 1 occurs in Windows:

NICINFO.EXE detects PnP drivers in Windows 2000/XP. It also detects Windows 9x if IE 4.02 or higher is installed. NICINFO.EXE writes the detected vendor and device ID to DOSNIC.INI on the virtual boot image.

Phase 2 occurs in DOS:

AUTODETE.EXE looks for the DOSNIC.INI left by NICINFO.EXE and reads the vendor and device ID. AUTODETE.EXE then refers to NIC.TXT to find the corresponding driver to load. It copies the driver from c:\Net\Drivers on the virtual boot image to the current RAM drive image (r:\Net by default). AUTODETE.EXE then sets the Microsoft DOS network stack configuration files, SYSTEM.INI and PROTOCOL.INI.

If DOSNIC.INI is empty, AUTODETE.EXE scans all PCI device slots looking for network adapter vendor and device IDs. If the ID found matches an entry in NIC.TXT, AUTODETE.EXE loads that driver.

Phase 3 continues in DOS:

If DOSNIC.INI is empty and AUTODETE.EXE can't match the discovered ID with NIC.TXT, it loads the driver specified in the OS Deployment/Migration Tasks wizard. If this driver doesn't load, the device will be stuck in DOS, and you'll need to reboot it manually. If no driver was specified in the wizard, AUTODETE.EXE saves an AUTODETE.LOG file to the drive root and the device boots back into the original operating system.

NICINFO.EXE and AUTODETE.EXE don't support 16-bit PCMCIA network adapters. You can load the drivers for these network adapters by selecting the appropriate driver in the OS Deployment/Migration Tasks wizard as described in Phase 3. NICINFO.EXE can detect network adapters that support CardBus.

NICINFO.EXE requires PnP support. Windows NT 4 has no PnP support.

Adding network adapter drivers

To add network adapter drivers

1. Edit the **ALTDIVERS.INI** file.
2. Edit the **NIC.TXT** file in the `..\ManagementSuite\OSD\Utilities` directory.
3. Use **COPYFILE.EXE** to insert the .DOS or .EXE driver file into the virtual boot image in `..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG`
4. Use **COPYFILE.EXE** to insert **NIC.TXT** to the virtual boot image.

Editing the ALTDIVERS.INI file

ALTDIVERS.INI is the driver description file.

Sample entry:

```
[Intel PRO/1000 Adapters]
DRIVER=E1000.DOS
PROTOCOL=E1000
```

The description between [] can be anything. This is the text that appears in the OS Deployment/Migration Tasks wizard when you manually select a network adapter driver:

- DRIVER is the .DOS or .EXE network adapter driver.
- PROTOCOL often is the same as the driver name or the manufacturer name.

Editing the NIC.TXT file

NIC.TXT has information for detecting network adapters. You'll need to edit the NIC.TXT to add custom adapter information. Here's a sample entry:

```
ven=115D "Xircom"  
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"  
drv="CBENDIS.EXE"  
prot="XIRCOM"
```

These are the four possible keys and values:

- **ven** is four characters (for example, 1 must be 0001); description can be anything.
- **dev** is four characters; description can be anything.
- **drv** is the driver name; default extension is .DOS.
- **prot** is the protocol, often the same as the driver name or the manufacturer.

As you can tell by looking at NIC.TXT, not all drivers have all keys.

Injecting driver changes back into the virtual boot image

To inject driver changes back into the virtual boot image, use copyfile. The syntax is:

```
COPYFILE <imgfile> <srcfile> <destfile>
```

Example:

```
COPYFILE c:\Program  
Files\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG  
c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS
```

Note: The <destfile> variable can't contain the drive letter designation.

You need to copy the .DOS or .EXE network adapter driver to c:\Net\Drivers and the updated NIC.TXT to c:\Net

Adding network adapter drivers to the Windows PE boot environment

If you need to add custom network drivers to the Windows PE environment, follow the steps below.

To add Windows PE boot environment network drivers

1. Copy the network driver .INF and .SYS files to this folder on the core server:

```
C:\Program Files\LANDesk\ManagementSuite\LANDesk\Vboot\winpedrv
```

2. Add the network driver information to this file on the core server (see the sample entries inside for details):

```
C:\Program Files\LANDesk\ManagementSuite\altdriverspe.ini
```

Using the LANDesk imaging tool for DOS

Note: When you install the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

LANDesk's imaging tool for DOS (IMAGE.EXE) is a DOS-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most ATAPI CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

Limitations

IMAGE.EXE relies on the BIOS for processing disk functions. If a computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGE.EXE will also be limited.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- 16 MB RAM
- XMS

Getting started

IMAGE.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Environment variables

You can use several different environment variables with IMAGE.EXE:

- **IMSG** displays a message on the screen. To create a message with IMSG, use the set command (i.e., set msg=<include message of 80 characters or less here>).
- **IBXT** changes the method used to burn a set of CDs so that IMAGE.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1. (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGE.EXE to auto-respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.
- **IOBS=A** tests the network speed and uses the best buffer size for uploading/downloading an image.

Command-line options

You can use command-line options with IMAGE.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option to view a list of additional command-line options not explained here.

To create a compressed image to a file

Format 1: image /Ch# d:\filename.img (no validation)

Format 2: image /Ch#V d:\filename.img (validation)

Format 3: image /Ch#VB d:\filename.img (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGE.EXE without any command-line options and select Create Image. The screen that lists the partitions and volumes will display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

To create an uncompressed image to a file

Format 1: image /Ch# /U d:\filename.img (no validation)

Format 2: image /Ch#V /U d:\filename.img (validation)

Format 3: image /Ch#VB /U d:\filename.img (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Explanation: Same as above.

To restore an image from a file

Format 1: image /R d:\filename.img (no validation)

Format 2: image /RV d:\filename.img (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Explanation: The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

To limit the file size on creation

Format: d:\filename;s

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- When restoring an image, you shouldn't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system will reboot. This is required because the partitions and file system being used by the OS have changed. If a reboot didn't occur, the OS would still think the partition and file system was as it was before the restore. This could cause data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition goes to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, then a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGE.EXE via AUTOEXEC.BAT if desired.

Using the LANDesk imaging tool for Windows

LANDesk's imaging tool for Windows (IMAGEW.EXE) is a Windows 32-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most types of DVD+RW or CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

IMAGEW.EXE is compatible with LANDesk's imaging tool for DOS (IMAGE.EXE).

Limitations

For use with Windows 9x/Me, IMAGEW.EXE requires that the system support Int 13h extensions. If your computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGEW.EXE will also be limited on those OSes.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- Windows 32-based environment with 32 MB RAM minimum recommended
- Administrator privileges when running on Windows NT, Windows 2000, or Windows XP

IMAGEW.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Creating images

You can use various environment variables and command-line options to ensure that the images you create meet your requirements.

Environment variables

Environment variables for IMAGEW.EXE must be used with command-line options. The following environment variables are available:

- **IBXT** changes the method used to burn a set of CDs so that IMAGEW.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1 (i.e., set `ibxt=1`). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGEW.EXE to auto respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set `iar=Y`). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.

Command-line options

You can use command-line options with IMAGEW.EXE. Separate the options by spaces and enter them in the order shown below. Use the `/?` command-line option for additional command-line options not explained here.

To create a compressed image to a file

Format 1: `imagew /Ch# d:\filename.img` (no validation)

Format 2: `imagew /Ch#V d:\filename.img` (validation)

Format 3: `imagew /Ch#VB d:\filename.img` (byte-for-byte validation)

Explanation: Replace the `h` with the source hard drive number from 0 to 7 and the `#` with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as `0xPVV` where `P` is the extended partition and `VV` is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGEW.EXE without command-line options and select Create Image. The screen that lists the partitions and volumes will also display the ID in parentheses as a hexadecimal number. You should prefix that number with a `0x` on the command line.

To create an uncompressed image to a file

Format 1: `imagew /Ch# /U d:\filename.img` (no validation)

Format 2: `imagew /Ch#V /U d:\filename.img` (validation)

Format 3: `imagew /Ch#VB /U d:\filename.img` (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: `imagew /Ch# /CDx`

Explanation: The `h` and `#` information is the same as above. The `x` after `/CD` is the CD drive number to use. Omit the `x` (`/CD`) to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: `imagew /Ch# /U /CDx`

Explanation: Same as above.

To restore an image from a file

Format 1: `imagew /R d:\filename.img` (no validation)

Format 2: `imagew /RV d:\filename.img` (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: `imagew /R /CDx`

Explanation: The x after /CD is the CD drive number to use. Omit the x to get a list of the devices.

To limit the file size on creation

Format: `d:\filename;s`

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When running under Windows NT/2000/XP Pro, you must have administrator privileges. Under Windows 2000/XP, you can run as any user by right-clicking and selecting the Run As option.
- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- If you create a backup without a lock being obtained, that backup may not be in a consistent state if updates to the drive were occurring during the backup.
- When restoring an image, you can't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system may need to reboot. This is required under certain conditions and determined by the program. If you don't reboot when asked, the OS will think the partition and file system is as it was before the restore, potentially causing data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition will go to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGEW.EXE via AUTOEXEC.BAT if desired.

Understanding the Windows PE preboot environment

Windows PE is a mini-Windows system that provides limited services based on the Windows XP Professional and the Windows Server 2003 kernels. Windows PE is a hardware-independent Windows environment that contains the following:

- A subset of the Microsoft Win32 application programming interfaces (APIs).
- A command interpreter capable of running batch files.
- Support for adding Windows Script Host (WSH), HTML Applications (HTA), and Microsoft ActiveX Data Objects (ADO) to create custom tools or scripts.

Windows PE uses TCP/IP to provide network access and supports the same set of networking and mass-storage device drivers that Windows XP supports. Some limitations worth noting are that connectivity is limited to outgoing connections only (resource sharing is disabled), and to prevent client-usage of the OS, a hard-coded reboot will occur after 24 hours of use.

LANDesk has customized the Windows PE operating system to only include necessary libraries, utilities, and drivers. Additionally, the LANDesk agent files have been copied to the image to facilitate LANDesk functionality. Also, the command file initially loaded by the PE operating system has been modified to include the LANDesk staging commands. In Service Pack 2 for LANDesk 8.7, WMI support was added to the image.

This section will provide a list of the files that have been either added or modified in the PE image, an overview of the boot process and an explanation of each line in the startup command file.

Files modified or added to the WinPE image

In addition to drivers, the LANDesk Windows PE image includes the following modified or added files.

File	Purpose
winbom.ini	Turns off the Windows PE firewall
\i386\txtsetup.sif	LANDesk signature file
\i386\system32\winpeshl.ini	Defines the shell location
\i386\system32\peshell.exe	The actual shell used
\i386\system32\setupreg.hiv	Includes the LANDesk path
\i386\system32\startnet.cmd	Command file run at startup
\i386\system32\all.reg	LANDesk registry modifications
\i386\system32\winpe.bmp	LANDesk background wallpaper

File	Purpose
\CBA8	LANDesk agent
\LDCLIENT	LANDesk agent

LANDesk WinPE boot process

The WinPE boot process starts like this:

1. Once the boot sector is loaded, SETUPLDR uses NTDETECT.COM to scan the hardware so the correct HAL can be loaded.
2. The WINPEOEM.SIF is used to load boot drivers (administrators can customize this file to control which mass-storage drivers are loaded) and then NTOSKRNL.EXE finishes the environment setup and calls SMSS, which in turn loads the registry and calls Winlogon.
3. Winlogon starts the services, finishes driver loading and starts a user session.
4. CMD.EXE is executed and processes the STARTNET.CMD. This batch file is used to load the networking drivers and any other commands one adds to it. The original Windows PE STARTNET.CMD looks like this:

```
factory winpe
```

The LANDesk-modified WinPE image by default includes a custom STARTNET.CMD file. In version 8.7sp2, it looks like this:

```
@echo off
set path=%path%;x:\cba8;x:\ldclient
\ldclient\GetBootOptions set /a err = %errorlevel%
if %err% gtr 0 goto nofix
ldclient\Diskinfo fix
:nofix
factory winpe
reg import all.reg
 \ldclient\wait4ip /t 180
if %errorlevel% gtr 0 goto fail
CD \CBA8
RESIDENTAGENT.EXE /register
RESIDENTAGENT.EXE /start
CD \ldclient
 winpepds /install
 winpepds /start
If %err% gtr 0 goto pxe
miniscan /nodeviceid /usemacasname
Goto end
:pxe
if %err% lss 2 goto pxemenu
:pxeboot
miniscan /x /nodeviceid /usemacasname
goto end
:pxemenu
miniscan /nodeviceid /usemacasname
Replcore PxeMenuStart.cmd
call PxeMenuStart.cmd
goto end
:fail
```

```
@echo "Failed to get localhost IP address or resolve core server name.  
Please check your network and try again."  
@pause  
:end
```

STARTNET.CMD command definitions

The following section describes each line in STARTNET.CMD.

@echo off

Hides the output of this CMD file. REM this command out when troubleshooting the STARTNET.CMD.

set path=%path%;x:\cbsa8;x:\ldclient

Sets the path to include the added LANDesk agent files.

\ldclient\GetBootOptions

This executable sets the errorlevel to 0, 1, or 2. The values are 0 if the machine was virtual booted, 1 if the machine was PXE booted and the PXE menu was chosen, and 2 if the machine was PXE booted and managed boot was chosen.

set /a err = %errorlevel%

Sets the ERR variable to the value derived by GetBootOptions.

if %err% gtr 0 goto nofix

This line has the script skip to the next line if the machine was PXE-booted.

\ldclient\Diskinfo fix

This line is only processed if not PXE booting. Diskinfo.exe used with the fix switch resets the MBR to boot back into the original active partition. Vbooting had previously set this to boot to the WinPE RAM drive.

factory –winpe

The FACTORY.EXE command is used to load drivers and when called with the –winpe switch it will generate a unique name for the PE session (usually minint-<random suffix>) and then process the WINBOM.INI, which is where you can configure and add to the PE behavior. For example, since by default FACTORY.EXE is scanning all of the available drivers to find the one that matches the discovered hardware, you could limit the number of drivers scanned (thereby increasing bootup speed) by modifying the NetCards section of the WINBOM.INI file.

reg import all.reg

Imports the LANDesk environment settings into the WinPE registry. Specifically, the core server's name and the port used for inventory are defined in the ALL.REG file. Here is an example ALL.REG:

```
Windows registry Editor version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM]
"CoreServer"="<core_name>"
"InventoryServerPort"="5007"
```

ldclient\wait4ip /t 180

The wait4ip executable ensures we have an IP address before gathering inventory for this machine. The /t 180 defines a timeout limit of 3 minutes. A /s can be added to silence the output of this program. Additional information is available by executing with a /?.

if %errorlevel% gtr 0 goto fail

Skips the rest of the commands in this file if an IP address can't be obtained.

CD \CBA8

Changes the directory from X:\i386\system32 to X:\CBA8.

residentagent.exe /register

RESIDENTAGENT.EXE is the service that listens for and accepts connections for remote commands, and then starts the application needed to handle the request (which is how the LANDesk imaging operations are carried out). The /register switch will install and register the RESIDENTAGENT.EXE as a service. This is logged in the CBA8 directory in RESIDENTAGENT.LOG.

residentagent.exe /start

The /start switch will start the RESIDENTAGENT.EXE service, which proceeds to load necessary libraries. This too is logged in the RESIDENTAGENT.LOG.

CD \LDClient

Changes the directory from X:\CBA8 to X:\LDClient.

winpepds /install

WINPEPDS is the module pinged by the core server to discover this machine, verifying this is the correct managed node. The /install switch will install the service.

winpepds /start

The /start switch starts the WINPEPDS service.

if %err% gtr 0 goto pxe

This line means that PXE booted machines will continue the script at the PXE section further below.

miniscan /nodeviceid /usemacasname

This line is only executed by virtual booted machines, and is their last command. Miniscan is the utility used to grab minimal information about the system and store it in the LDMS inventory database. Running miniscan without switches will include a devicename and ID in its scan file, and thereby will show up in the console as "minint-<random suffix>". However, using the /nodeviceid /usemacasname switches removes this information from the scan file and limits the data sent to 3 things: MAC Address, IP Address, and Processor Count. In the console, these devices show up named after their MAC address.

if %err% lss 2 goto pxemenu

Tells PXE-booted machines that are supposed to get the menu to skip to the PXEmenu section.

miniscan /x /nodeviceid /usemacasname

This line is executed by those PXE booted machines that are a managed boot. If the /x is used when calling miniscan, an extra attribute is sent in the Network portion of the scan file, Pxeboot=Yes.

miniscan /nodeviceid /usemacasname

This line is only executed by PXE-booted machines that are to display a menu. Miniscan is the utility used to grab minimal information about the system and store it in the LDMS Inventory database. Running miniscan without switches will include a devicename and ID in its scan file, and thereby will show up in the console as "minint-<random suffix>". However, using the /nodeviceid /usemacasname switches removes this information from the scan file and limits the data sent to three things: MAC Address, IP Address, and Processor Count. In the console, these devices show up named after their MAC address.

replCore PxeMenuStart.cmd

REPLCORE.EXE is used to replace the %CoreServer% variable in the file it is pointed to with the value found in the registry String Value HKLM\Software\Intel\LANDesk\LDWM\CoreServer (this was populated with the ALL.REG earlier in the process). In this case, the PxeMenuStart.cmd is about to be called and it uses sdclient to contact the core server and therefore must have the correct core name in its command line.

call PxeMenuStart.cmd

If the menu option is chosen by the PXE booted machine, then the PXEMENUSTART.CMD will be executed. Two of the significant lines are:

```
sdclient /f /o /p="http://%CoreServer%/landesk/files/dosmenu.cfg"  
RunBatch 500 X:\LDClient PxeMenu dosmenu.cfg
```

First, sdclient is used to retrieve the DOSMENU.CFG from the core server. Then RunBatch (a simple utility that calls a process after a defined delay) is used to launch PXEMENU.EXE fed with the parameter of DOSMENU.CFG.

@echo "Failed to get localhost IP address or resolve core server name. Please check your network and try again."

If an IP address could not be obtained, this error message appears, indicating that the NIC or NIC drivers should be investigated.

Appendix C: Additional software distribution information

This chapter explains how to use LANDesk Management Suite's software distribution (SWD) to distribute software and files to devices throughout your network.

Read this chapter to learn about:

- [Scripting guide for .CFG files](#)
- [Troubleshooting .CFG files and their packages](#)
- [Scripting guide for deployment scripts \(.INI\) files](#)
- [Understanding Software Distribution error codes](#)
- [Files used in Software Distribution](#)

Scripting guide for .CFG files

This section describes what you can do with scripts and scripting commands as you build a software distribution package. At the end of this section, there's a sample script with remarks that explain the important parts of the script.

For detailed instructions about creating and modifying .CFG files, see the Package Builder online help. Click **Start | Programs | LANDesk Management | LANDesk Enhanced Package Builder**. Click **Help | Index** and select the following online help topics:

- Getting started with Package Builder
- Creating a simple installation
- Package Builder commands
- How does Package Builder do an installation?
- Using variables in commands and assigning values

Scripting basics

The Package Builder wizard steps you through the process of creating a software distribution package. The wizard saves the commands required to perform the same installation on other devices. It writes these commands to an ASCII file with a .CFG extension. You can edit this script file after creating it in Package Builder, or you can create one from scratch and build it into a package.

The Package Builder online help provides syntax information for each of the script commands. To access the help for a specific command, highlight a command in the left panel and press the **F1** key.

To access a specific script file, start Package Builder and click **File | Open**. Browse to the Configs folder in the Package Builder working folder and select a file.

Once a script has been modified, click **Build | Build** to build the script into a package.

Script commands

Each script includes two sections. Specific commands at the top of the script define the operating parameters, and the balance of the commands describes the installation of the application included in the software distribution package.

All of the commands included in a script can be grouped into one of these functional categories:

- Base Installation
- Appearance
- Messages & Input
- System Changes
- If Conditions
- Defaults & Calls

These categories contain related commands that describe the installation process for each package. Some commands describe the operating parameters of the installation and must be placed at the top of the script file. For details about each command, see the Package Builder online help.

Editing packages with the Package Builder

The Package Builder interface is divided into three areas:

- In the left pane, the functional categories are listed. Expand each functional category to display the individual commands within that category.
- The right pane is divided into two screens: The upper portion displays the script itself. The lower portion is a GUI template that contains entry boxes for the parameters of the highlighted command.

To see the details of a command in the script, highlight the command and view the parameter details in the lower portion of the screen.

To add a new command to the script, select the location in the script where the command should be located. Next, highlight the command in the left pane. Now complete the syntax template in the lower portion of the screen. When you've selected the command parameters, click **Add** to insert the new command.

Simple sample script

This script contains some of the commands used to install Package Builder on a package-building computer. Major sections or commands are described with remarks (REM).

```
REM This is the Package Builder installation
REM Set screen graphics environment
SCREENCOLOR: (0,0,255), (0,0,255)
```

```
ANIMATION: "W:\Software\Install\Intel\duck\DISK01.BMP",
"W:\Software\Install\Intel\duck\DISK02.BMP",
"W:\Software\Install\Intel\duck\DISK03.BMP",
"W:\Software\Install\Intel\duck\DISK04.BMP",
"W:\Software\Install\Intel\duck\DISK05.BMP",
"W:\Software\Install\Intel\duck\DISK06.BMP",
"W:\Software\Install\Intel\duck\DISK07.BMP",
"W:\Software\Install\Intel\duck\DISK08.BMP",
"W:\Software\Install\Intel\duck\DISK09.BMP",
"W:\Software\Install\Intel\duck\DISK10.BMP",
"W:\Software\Install\Intel\duck\DISK11.BMP",
"W:\Software\Install\Intel\duck\DISK12.BMP",
"W:\Software\Install\Intel\duck\DISK13.BMP"
SCREENGRAPHIC: "W:\software\INSTALL\Intel\OAKLAN~1.BMP", topleft
REM TITLE: "LANdesk Management Suite", fontsize=25, color=yellow
REM SUBTITLE: "Package Builder", fontsize=18, italic, color=yellow
REM Configure uninstallation options
UNINSTALL: yes, removegroup, packagename="Package Builder"
UninstallBeginPrompt: "Do you wish to remove the LANdesk Management Suite
Package Builder programs and directories from your system?"
UninstallEndPrompt: "LANdesk Management Suite Package Builder programs and
directories have been successfully removed from your system."
REM Check for sufficient disk space before installation
IF DISKSPACE() < 4000K
BEGINFIRSTSCREEN caption="Not Enough Disk Space", Package Builder requires
4 MB of disk space. Please arrange your hard disk so that a sufficient
amount of disk space is available.
ENDFIRSTSCREEN
REM This is only shown if there is less than 4 MB of disk space.
ENDIF
REM Define splash screen text
BEGINFIRSTSCREEN caption="LANdesk Management Suite Package Builder",
This installation program will set up LANdesk Management Package Builder
onto your hard disk. Contact your LANdesk Software Customer Support
representative if there are problems setting it up on your computer.
ENDFIRSTSCREEN
REM Define default directory from which to work. Notice the variable
$ProgFilesDir$ comes from a Windows system environment variable. The
DEFAULTDIR command must be used before any file commands are used.
DEFAULTDIR: "$ProgFilesDir$\Intel\Package Builder", prompt="Please enter
the drive and directory:", caption="Directory Name", text="The software
will install onto your system in a directory. Please accept the suggested
directory location or type in one of your own. Make certain to provide
both a drive letter and the directory name."
REM Add files common to all versions of Package Builder. Only one has been
included in this sample script.
FILE: "CTL3D.000", overwrite=yes,
From="W:\Software\Install\Intel\CTL3D.DLL"
REM Install registry information
BEGINREGISTRY
KEY: new, "HKEY_CLASSES_ROOT\CFG"
VALUE: reg_sz, replace, "Default", ".txtfile"
ENDREGISTRY
REM Setup Windows menu items
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\Builder.exe", "Package
Builder", replace, allusers
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\Replicator.exe",
"Package Builder wizard", replace, allusers
```

```
WINITEM: "LANdesk Management Suite", "$DEFAULTDIR$\ENUBLDRI.hlp", "Package
Builder wizard help", replace, allusers
REM Define and display final screen
BEGINLASTSCREEN caption="LANdesk Management Suite Package Builder",
The installation of the Management Suite Package Builder is now complete.
ENDLASTSCREEN
```

Registry commands

Commands that modify the registry begin and end with BeginRegistry and EndRegistry commands. In between these commands are the commands that identify the registry key and the value. The Package Builder wizard flags two keys as dangerous:

- \HARDWARE
- \SYSTEM\CURRENTCONTROLSET

These keys are considered dangerous because they are usually not compatible with any device other than the package-building computer. When these keys are modified, the Package Builder wizard places such commands within an IF \$DANGEROUS\$ = "TRUE" statement. If the changes to these keys are compatible with your target devices and you want them executed, you must define a \$DANGEROUS\$ variable at the top of the script and set its value to TRUE.

Launching a package from a package

You can specify INST32.EXE on the command line of a RunAtExit command in one package in order to launch another package. The syntax is:

```
RunAtExit "INST32.EXE PACKAGENAME.EXE"
```

If the package is found on the network, this is more efficient than just running "PACKAGENAME.EXE." It allows you to specify a package name via an HTTP path. For example:

```
http://myservername/packages/PACKAGENAME.EXE
```

Sample script with more complex commands

This next script is organized into sections with a brief explanation for each. Any applications launched by a RunAtStart or RunAtMiddle command must be closed for the script to continue processing.

The beginning section of this script enables you to include a window title, package name, animated or still graphics, and audio, as well as color and font selections. A RunAtStart command enables you to execute an external application at the beginning of the installation.

Next, the BeginFirstScreen command enables you to inform the user about the installation by displaying a text message. Finally, the Backup command indicates that any files that are to be replaced will be backed up, and the OverWriteFile command indicates that the user will be prompted before any existing files are overwritten.

```

ANIMATION: "C:\WINDOWS\CIRCLES.BMP", "C:\WINDOWS\CARVED~1.BMP",
"C:\WINDOWS\BUBBLES.BMP", "C:\WINDOWS\BLUERI~1.BMP",
"C:\WINDOWS\BLACKT~1.BMP"
RUNATSTART: "c:\program files\accessories\mspaint.exe"
TITLE: "Package Builder Functionality Script for Windows 98", bold
INTROSCREEN: "C:\WINDOWS\SETUP.bmp", waittime=5, full
INTROSOUND: "C:\WINDOWS\MEDIA\START.WAV"
SCREENCOLOR: magenta, yellow
SCREENGRAPHIC: "C:\WINDOWS\PINSTR~1.BMP", topleft
FONTNAME: "Tahoma"
BEGINFIRSTSCREEN title="First Screen", caption="Screen #1"
This is the text that appears on the first screen.
ENDFIRSTSCREEN
BACKUP: YES
OVERWRITEFILE: ask

```

The following examples show different prompt options. Text for each prompt can be modified.

```

CancelPrompt: "Cancel?"
CopyFilePrompt: "UPLOAD IN PROGRESS"
OkPrompt: "GOOD JOB"
QuitPrompt: "Do you really want to quit?"
CopyTitlePrompt: "Copying..."
NextPrompt: "Next"
BackPrompt: "Back"
NoPrompt: "No"
YesPrompt: "Yes"

```

This section runs an external application and waits for that application to be closed before continuing. When the script continues, the user is prompted for input. Based on the selected option, the application continues and copies a file on the local drive or exits.

```

RUNATMIDDLE: "c:\windows\calc.exe"
ASK1: Yesno, caption="Sample question.", text="This is an example using
Yes / No buttons. Choose `Yes' to continue, `No' to exit."
IF $ASK1$= "yes"
WINGROUP: "New Program Group", prompt="Select a group", caption="Program
Group selection", text="Please select a program group."
ELSE
IF $ASK1$= "No"
EXITMESSAGE
Sorry you had to leave so soon!
EXIT
ELSE
ENDIF
ENDIF
PROGRESSBAR: 302K
COPY: "C:\windows\setup.bmp", "C:\windows\temp\p1.bmp"
RENAME: "C:\windows\temp\p1.bmp", "C:\windows\temp\renamed p1.bmp"

```

This section launches an application as the last command before the script is completed. The RunAtExit command does not have to be the last line of the script.

This section also places a shortcut on the desktop and creates an uninstall package.

```

RUNATEXIT: "C:\WINDOWS\CDPLAYER.EXE"
BEGINLASTSCREEN title="Last screen", caption="The last screen"

```

This should be the last screen you see.

```
ENDLASTSCREEN
SHORTCUT: "c:\windows\notepad.exe", "NOTEPAD", dir="c:\windows\desktop\"
UNINSTALL: yes, makeicon, removegroup, packagename="Package Builder
Functionality"
```

Processing custom scripts

Custom scripts that control scheduled tasks (**Tools | Distribution | Scheduled tasks**) are processed in three sections:

- **Premachine:** The Premachine section of the custom script is processed first, and only once at the start of the task. Use this section for tasks that have no targeted device, and/or for Targeted Multicast. During the Premachine section of the script, only local commands, LOCxxx, should be used.
- **Machine:** The commands in this section of the script run second and only once per targeted device. These commands can use either the remote or local execution commands, and are primarily used for remotely executing SDCLIENT.EXE. Before the commands in this section of the script can be performed, the SWD agent must be installed on the targeted devices.
- **Postmachine:** This section is processed last, and again, only once after all devices have been processed. Software distribution does not add commands to this section, and it only supports the local commands, LOCxxx. The commands in this section won't be processed if devices in the task can't run them. The InventoryScanner.ini script that comes with Management Suite contains details about the script commands.

Custom Script Commands

Custom scripts support various local and remote commands:

- **LOCEXEC:** Local execute, this command is used to execute an application on the local device, which is always the core server.
- **LOCDEL:** Local deletion, deletes a file on the local device.
- **LOCMKDIR:** Local make folder, creates a folder on the local device.
- **LOCRD:** Local remove folder, this command is used to remove a folder on the local device.
- **REMCOPY:** Remote copy, copies a file from the local device to a remote device.
- **REMEXEC:** Remote execution, executes an application on the specified remote device
- **REMDL:** Remote deletion, deletes a file on the remote device
- **REMMKDIR:** Remote make folder, this command creates a folder on the remote device
- **REMRD:** Remote remove folder, this command deletes a folder on the remote device

Command-line parameters

Software distribution is facilitated by a deployment script. SDCLIENT.EXE manages the packages using command-line parameters from the script file that are passed to the application.

SDCLIENT.EXE supports the following command-line parameters:

```
sdclient.exe /p="<package path>" [/g=<pkg guid>] [/All] [/R] [/N] [/An]
[/Ac] [/Ab] [/fui] [/msi] [/exe] [/bw=xxx] [/E]
```

Parameter name	Description
/p=<package path>	Package Path. The package path must be specified, regardless of the package type. This parameter specifies the UNC or URL path to the package that is to be installed on the local device.
/g=<pkg guid>	Package GUID. For SWD or AutoInstall packages. This parameter specifies the GUID for the package. The package GUID is used to check the local .CFG file cache for a copy of the package's .CFG file.
/All	Uninstall Flag. This flag is set to indicate that the SWD or MSI package should be uninstalled rather than installed. This flag is case-sensitive (/all won't work).
/R	Always Reboot Flag. This flag indicates that the device should always be rebooted after the package installation. Not all MSI packages follow this guideline.
/N	Never Reboot Flag. This flag indicates that the device should never be rebooted after the package installation.
/An	Silent Installation Flag. This flag indicates that the installation should be silent. This means that no UI, or the smallest amount of UI possible, should be displayed during the installation.
/Ac	Disable Cancel Flag. This flag prohibits the user's ability to cancel the installation.
/Ab	No Background Flag. This flag only applies to SWD packages. When a package is being installed, the blue background won't be displayed.
/fui	Full UI Flag. This flag indicates that the full UI for legacy and MSI packages should be used.

Parameter name	Description
/msi	MSI Package Flag. This flag indicates that the package path points to an MSI package file.
/exe	Executable Package Flag. This flag indicates that the package path points to a legacy package or a generic executable file.
/bw=xxx	Bandwidth Requirements. Specifies a minimum bandwidth requirement for the package script to be run.
/F	Generic File Flag. This flag causes SDCLIENT.EXE to download the file to the LDCLIENT folder.
/msg=""	Sends a message to the core server while the task is executing. This message appears in the task status inside the Scheduled tasks window's Message column.

HTTP and UNC paths

These are examples of software distribution .INI files that reflect the differences between HTTP and UNC path script files.

HTTP path script file:

```
; This file was generated by Desktop Manager
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web
server>/packages/test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-
9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

UNC path script file:

```
; This file was generated by Desktop Manager
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -
p=\\sample_core\onefile\test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-
9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Notice that both .INI files have similar elements. In the MACHINES section, the -P option designates the path where the device will download the software package. In the HTTP example, the path is http://<web server>/packages/test package.exe.

The next option is the -G option, which is the GUID, a unique number identifier for each package. This number identifier is generated by the Package Builder, and it helps prevent confusion during installation between packages with similar names.

Troubleshooting .CFG files and their packages

Deciding what works and what doesn't work is the first step in script debugging. These are some basic troubleshooting tips that can help you resolve script errors:

- Create a new script that consists of only the portion of the script that produces an error. Check the functionality of this script and modify as required using the online command help.
- Compare the new script to an existing script to check for syntax.

Use the following guidelines when you create packages on your package-building computer. These tips will help you avoid unnecessary errors.

Using commands

Don't pass variables to the DLL Load command in Package Builder

If you create a package that depends on passing a variable into the DLL Load command, it won't work if the variable doesn't arrive at the correct time. If the .DLL doesn't receive the expected variable, the package won't complete the installation correctly. To avoid this problem, don't pass variables into the DLL Load command; the other DLL parameters work correctly.

Using the Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands

The Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands require the full path to the executable to run correctly. Also, the RunAtMiddle command must be positioned in the script after the DEFAULTDIR function to work correctly. RunAtStart and RunAtExit commands can be anywhere in the script and will run correctly.

Rebooting during package creation

When using the Package Builder wizard to create a package, you may be prompted to reboot the package-building computer. In many cases, rebooting before completing the package-building process causes the package to improperly install at the device. The application becomes configured for the package-building computer rather than the targeted device. However, in some cases, the reboot is required because the installation program accesses the installation CD after reboot.

You need to test the resulting package to determine whether you can stop the installation process and create the package before the reboot, or whether you need to reboot the package-building computer during the software installation and then continue to create the package.

Creating and naming software distribution packages

Package names can't be changed once they're created

You can't change a package name once you complete the package creation step. If you attempt to directly change the filename, your users can't access that package correctly.

Package names can't include hyphens or periods

If you use hyphens or periods in a package name, the package-creation process will truncate the name when it encounters them. You can still access the package in a script, and users can install it, but the truncated name might be confusing. Don't use hyphens or periods in a package name. You can use the underscore (`_`) character instead.

We recommend that you create a new working folder each time you begin creating a package. To create this folder, start the Package Builder wizard, and click Scan Options. In the Temporary Work Directory box, either type in the full path to a folder or browse to its location. Package Builder prompts you for permission to create a folder that does not already exist.

Store only software distribution packages in your distribution location

You should only keep packages in the Web server location or UNC folder that you set up for software distribution. If you store other types of executable files in this folder, they may be confused with packages when you're creating distribution package scripts. If you create a distribution script for an executable that's not a package, the distribution will fail. Store only software distribution packages in your distribution location.

For more information about creating and modifying packages, see the topic "Working with the Package Builder" in the Package Builder online help.

File collections can't contain more than 296 files

When you create a file collection package, you can add as many as 296 separate files or folders. If you attempt to add more than 296 items, the file collection stops. Files contained in an included folder count as one item, not as separate files.

Scripting guide for deployment scripts (.INI) files

You don't have to use the Create Software Distribution Script window to create the deployment script file. A deployment file is an .INI file containing the settings the device should use for installing a package. You can create your own deployment files in a text editor such as Notepad if you prefer.

A software distribution .INI script file has these components:

```
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

REMEXEC0 command parameters

The parameters for the REMEXEC0 command have been placed on separate lines to make the components more visible. When placed in an .INI file, the command needs to be on one line.

REMEXEC0 is the Remote Execute command. If you want to use more than one REMEXEC0 command in a single script file, increment the command each time it is used. For example, if you used three REMEXEC calls in a single .INI file, they should be REMEXEC0, REMEXEC1, and REMEXEC2. These commands don't need to increment if they're in separate files.

The C:\Program Files\LANDesk\LDClient parameter is the correct path to the SWD agent.

The /p parameter is the path statement where the device can download the package. For example:

```
/p="http://computer_name/95Packages/Acro32_95.exe"
```

The /g parameter points to a GUID identification number for the package. For example:

```
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
```

If you use this parameter, the device will only download the package with that exact ID number. Use the Create Distribution Script window to generate this ID number, because it's embedded in the software package.

The /Ac parameter hides the install from users. They can only cancel the installation if they're prompted for something. The /Ab parameter hides the background. The /An parameter hides all of the UI and prevents any interaction (prompts from reaching the users).

The /Ah+ parameter heals a package that was previously installed, without prompting the user. The /Ah- parameter reinstalls a package that was previously installed, without prompting the user.

The /N parameter doesn't force a reboot on the device after the package is installed. The /R parameter forces a reboot on the device after the package is installed. If you don't use either the /N or /R parameters, the device will reboot only if files in use were updated or a reboot is needed to complete the installation.

An optional /D parameter opens a debug window used to view operational parameters for SDCLIENT.EXE. The debug window displays the package path and name, the GUID, any error or message codes, as well as the exit code returned to the Scheduled Tasks window.

If the software distribution script is designed to uninstall an existing application, two uninstall option parameters can be used:

- The /Au parameter uninstalls the last instance of a package and rolls back one install instance.
- The /All parameter uninstalls all instances of a package and completely removes the package.

If you follow these guidelines, you can create your own software distribution scripts and schedule them to be sent to devices. These scripts are stored in the DTMScripts folder on the core server.

Understanding software distribution error codes

From the console, the right panel in the **Scheduled tasks** window displays the task status. If you click Failed under the task, you can see devices that failed the job and the resulting messages and logs. The status and errors are logged to the following files:

- If the error occurred while attempting to access the package, the error is logged in the AIClient.LOG file.
- If the error occurred while processing the package (for example, copying files), the error is logged in the INST32.LOG file.
- The SDCLIENT.LOG file contains general summary information about each installation request received from the core server.

These log files are stored on each device. The following table lists the error codes you may encounter in these files.

Error code	Definition
101	The user cancelled the install.
102	File access was denied.
103	The password used isn't valid.
104	No network found, or incorrect path provided.
105	A download error occurred.
106	A socket could not be created.

Error code	Definition
107	Unable to open an HTTP session.
108	A CFG download error occurred.
109	A save CFG error occurred.
110	No save CFG folder exists.
111	A file access error occurred.
112	A get CFG error occurred.
113	Unable to create a backup CFG.
114	A spawn error occurred because another package is already being installed.
117	The backup directory can't be created.
180	Networking error. Can't initialize.
188	Timed out while downloading over HTTP.
189	HTTP connection aborted.
191	Host not found.

Error code	Definition
197	HTTP file not found.
201	The UNC file cannot be found.
202	The file was not found on the installation disk.
203	Unable to create a file in the specified location.
204	Not enough disk space on the destination drive for installation.
205	An invalid drive was specified, or the drive required for this install was not available.
206	The file has a long filename and can't be installed by the 16-bit install program. You still have the option to continue to install other files.
207	The specified file is not an executable.
208	Multiple uninstall registry entries exist with the same source path.
209	Unable to locate the uninstall executable.
210	Encountered an invalid compressed file, or HTTP error(s).
211	A successful AFXSOCKETINIT command must occur before using this API.
212	The network subsystem failed.

Error code	Definition
213	No more file descriptors are available.
214	The socket can't be created. No buffer space was available.
215	The specified address was already in use.
216	The connection attempt was rejected.
217	The provided host address was invalid.
218	The network can't be reached from this host at this time.
219	The attempt to connect timed out without establishing a connection.
220	The virtual circuit was aborted due to a timeout or other failure.
221	The virtual circuit was reset at the remote site.
222	A non-stated HTTP error occurred.
223	An HTTP error occurred; the file wasn't open for reading.
224	An HTTP error occurred; no content-length setting provided.
225	An HTTP error occurred; not enough memory available.

Error code	Definition
226	A memory allocation error occurred.
227	Unable to read the file.
228	Insufficient memory available.
229	The .CFG file has an error at line XX.
240	The temporary path specified is invalid. It can't be accessed or created. The target computer has a configuration problem.
301	This application has never been installed on this computer; it can't be uninstalled.

Files used in script-based software distribution

This is a list of the files used in SWD, as well as descriptions of how they work together. You can use this information to customize how packages are created, stored, and deployed in your organization.

These files are installed at the core server:

- ManagementSuite\CUSTJOB.EXE
- ManagementSuite\SDMAKINI.DLL
- ManagementSuite\LANDesk.ManagementSuite.WinConsole.dll
- ManagementSuite\INSTALL\EN_PKG_BLDR\SETUP.EXE
- ManagementSuite\LDLOGON\SDCLNSTL.EXE

These files are installed at the device:

- C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE
- C:\Program Files\LANDesk\LDClient\AICLIENT.DLL
- C:\Program Files\LANDesk\LDClient\SDMCACHE (this is an empty folder)
- C:\LDCLIENT.LOG (this file is created by the SDCLIENT.EXE file)
- INST32.EXE
- EUNINST32.DLL (or other locale-specific resource file)

- \$WINDIR\$aiclient.log
- \$WINDIR\$inst32.log

File descriptions

SETUP.EXE: This standalone, binary installation file is used to create package-building computers, placing the Package Builder, Package Builder wizard tools, and accompanying online help files onto the computer. Each application that you package with Package Builder is made into a self-extracting .EXE.

If you're using the Web Console, you must copy the .EXE to the packages folder on your Web server for users to access.

SETUP.EXE installs the following types of files on the package-building computer in the Program Files\Intel\Package Builder folder:

- BUILDER.EXE: Enhanced Package Builder executable
- ENUBLDR.DLL: Enhance Package Builder resource file
- REPLICATOR.EXE: Package Builder wizard executable
- ENUREPLC.DLL: Package Builder wizard resource file
- BASIC.CFG: A simple installation script for building a software distribution package
- TYPICAL.CFG: A more complex installation script for building a software distribution package
- ENUBLDR.HLP: Help file for the Package Builder
- ENUBLDRI.HLP: Help file for the Package Builder wizard

CUSTJOB.EXE: This file is launched directly by the Scheduler when a job is to begin.

SDC_INSTALL.INI: This job script is processed by CUSTJOB.EXE. It copies SDCINSTL.EXE to a remote device and then executes it on that device via the standard LANDesk agent (CBA). This file is placed in the DTM\Scripts folder.

SDCLNSTL.EXE: This file installs the SWD client files SDCLIENT.EXE and AICLIENT.DLL on Windows 95/98 and Windows NT/2000/2003/XP devices. This file is placed in the DTM\LDLogon folder on the core server.

SDCLIENT.EXE: This file is ultimately placed on the device in the C:\Program Files\LANDesk\LDClient folder. It's invoked with command-line parameters that include the URL or UNC path of the distribution package to be installed. This invocation is normally a result of the core server Scheduler calling CUSTJOB.EXE.

AICLIENT.DLL: This file is called by SDCLIENT.EXE; it's copied to the same folder as SDCLIENT.EXE.

INST32.EXE: This is the actual installer program. It's embedded within every self-extracting package. It's also installed into the LDClient folder and launched by SDCLIENT.EXE whenever a request to install a software package is received.

ENUINST32.DLL: This is a locale-specific resource file, and its name varies with the locale.

AICLIENT.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to AICLIENT.LOG1. When the new AICLIENT.LOG file exceeds the 50 KB limit, AICLIENT.LOG1 is renamed to AICLIENT.LOG2. It's incremented one more time to AICLIENT.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current AICLIENT.LOG file.

INST32.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to INST32.LOG1. When the new INST32.LOG file exceeds the 50 KB limit, INST32.LOG1 is renamed to INST32.LOG2. It's incremented one more time to INST32.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current INST32.LOG file.

Appendix D: Additional security scanner information

LANDesk Security Suite includes the Security and Patch Manager tool as the main component of its comprehensive security management solution. Use the Security and Patch Manager tool to: download updates for various security content type's definitions and patches; create, configure, and run security assessment scans and remediation scans; enable security alerts; generate security reports, and more. Security and Patch Manager basics are covered in "Security and Patch Manager" on page 315 and "Security and Patch Manager help" on page 722.

This chapter provides supplemental information about using the security (vulnerability) scanner.

Read this chapter to learn about:

- "Vulnerability scanner command-line parameters" on page 643

Vulnerability scanner command-line parameters

The security (vulnerability) scanner is called VULSCAN.EXE and it supports the following command-line parameters:

Parameter name	Description
General parameters	
/AgentBehavior=ScanRepairSettings ID	Overwrites the default behavior of the security scanner (scan and repair settings) for only the current security assessment or remediation scan job. The ScanRepairSettings ID is a number value.
/ChangeBehaviors /AgentBehavior=ScanRepairSettings ID	Changes the default scan and repair settings for any subsequent security assessment or remediation scan job by writing the scan and repair setting to the device's local registry. Use the exact syntax to the left, with both switches in the command line. The ScanRepairSettings ID is a number value. Note: You can use this option to change the default scan and repair settings for a device without having to do a full agent configuration deployment to the device.
/ShowUI	Shows the scanner UI on an end user device.

Parameter name	Description
/AllowUserCancelScan	Shows a Cancel button on the scanner UI that lets the end user cancel the scan.
/AutoCloseTimeout=Number	Timeout value in seconds. Note: If the value is set to -1, then the scanner UI waits for the end user to manually close it.
/Scan=Number Code (0-8)	Identifies which security content type is being scanned for. The number codes for the different security content types are: 0 - vulnerability 1 - spyware 2 - security threat 3 - LANDesk updates 4 - custom definition 5 - blocked application 6 - software updates 7 - driver updates 8 - antivirus 100 - all types
/Group=GroupID	Identifies the security content group being scanned for. This option overrides specific content type parameters, if present.
/AutoFix=True or False	Enables or disables the autofix feature.
Repair parameters	
/Repair (Group=GroupID, or	Tells the scanner which group or vulnerability to repair

Parameter name	Description
Vulnerability=VulnerabilityID, or Vulnerability=All)	(remediate). You can specify All for vulnerabilities in order to repair all detected vulnerabilities instead of a single vulnerability by its ID.
/RemovePatch=PatchName	Removes the specified patch from the patch repository.
/RepairPrompt=MessageText	Lets you display a text message that prompts the end user.
/AllowUserCancelRepair	A string that allows the end user to cancel repair if using a repair prompt.
/AutoRepairTimeout=Number	A timeout value of repair prompt in seconds. If it's set to -1, then the UI waits for user to close manually.
/DefaultRepairTimeoutAction	A string for the default action for vulscan to take if timeout expires for repair prompt, acceptable values. Values include: start and close.
/StageOnly	A string to retrieve patch or patches needed for repair but don't install.
/Local (get files from peer)	Forces peer only download.
/PeerDownload	Same as /local.
/SadBandwidth=Number	Maximum percentage of bandwidth to use when downloading.
Reboot parameters	
/RebootIfNeeded	Use this parameter to reboot a machine if needed

Parameter name	Description
/RebootAction	A string that determines vulscan's reboot behavior when repairing, acceptable values: always, never, or empty (anything else), If anything else, then vulscan will reboot if needed.
/RebootMessage	A string that displays text message to user in a reboot prompt.
/AllowUserCancelReboot	A string that allows user to cancel reboot if using a reboot prompt.
/AutoRebootTimeout=Number	Timeout value of reboot prompt in seconds, if set to -1, then UI waits for user to close manually.
/DefaultRebootTimeoutAction	A string that determines the action for vulscan to take if timeout value expires for reboot prompt, acceptable values: reboot, close, snooze.
/SnoozeCount=Number	Number of snoozes, vulscan decrements each time the user clicks snooze on the reboot prompt.
/SnoozeInterval=Number	Number of seconds for vulscan to sleep between snoozes.
MSI parameters	
/OriginalMSILocation=path	Path to original MSI location.
/Username=username	Username for MSI directory.
/Password=password	Password for MSI directory.

Parameter name	Description
Disable parameters	
/NoElevate	Don't launch vulscan via core tech.
/NoSleep	Prevents sleeping during definition scan (1/18th).
/NoSync	Doesn't get mutex, scans multiple instances.
/NoUpdate	Don't get a new version of vulscan.
/NoXML	Don't look for msxml.
/NoRepair	Same as autofix=false. Overrides autofix setting if present.
Data files parameters	
/Dump	Dumps vulnerability data directly from Web service.
/Data	Sucks in vulnerability data (from /dump).
/O=Path\Filename	Output scan results.
/I=Path\Filename	Input scan results.
/Log=Path\Filename	Overrides log file name.
/CoreServer=Server name	Identifies core server name.

Parameter name	Description
/Reset	Removes delta file base information (wipes out application data directory).
/Clear or /ClearScanStatus	Clears all vulnerability scan information.

Appendix E: Context-sensitive help

LANDesk Antivirus help

LANDesk Antivirus features are accessed from the Security and Patch Manager tool window (**Tools | Security | Security and Patch Manager**). LANDesk Antivirus lets you download and manage antivirus content (virus definition files); configure antivirus scans; and customize antivirus scanner display/interaction settings that determine how the scanner appears and operates on target devices, and which interactive options are available to end users. You can also view antivirus-related information for scanned devices, enable antivirus alerts, and generate antivirus reports.

The "LANDesk Antivirus" on page chapter introduces this complementary security management tool, which is a component of both LANDesk Management Suite and LANDesk Security Suite. In that chapter you'll find an overview, antivirus content subscription information, as well as step-by-step instructions on how to use LANDesk Antivirus features.

This chapter contains the following online help sections that describe the LANDesk Antivirus tool's dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog:

- "About the LANDesk Antivirus tab on the Download updates dialog" on page 649
- "About the Configure LANDesk Antivirus settings dialog" on page 652
- "About the Antivirus settings dialog" on page 653
- "About the Add excluded path dialog" on page 660
- "About the Schedule periodic antivirus scans dialog" on page 660
- "About the Schedule periodic antivirus updates dialog" on page 661
- "About the Create LANDesk Antivirus scan task dialog" on page 662
- "About the Antivirus activity and status information dialog" on page 662
- "About the Threshold settings dialog (for LANDesk Antivirus)" on page 663
- "About the Install or update LANDesk Antivirus task dialog" on page 663
- "About the Remove LANDesk Antivirus dialog" on page 664

About the LANDesk Antivirus tab on the Download updates dialog

Use the **LANDesk Antivirus** tab of the **Download Updates** dialog to configure settings for downloading virus definition file updates from LANDesk Security services. You can select to download LANDesk Antivirus content (virus definition/pattern files), specify when virus definition files are available to distribute to managed devices (immediately or after a pilot test period), and whether definition files are backed up.

You should be aware that the **Updates** tab of the **Download updates** dialog includes several Antivirus updates in the definition type list, including one named LANDesk Antivirus Updates. When you select LANDesk Antivirus Updates, both the scanner detection content AND the LANDesk Antivirus virus definition file updates are downloaded.

Antivirus updates are scanner definitions that detect:

- Installation of common antivirus scanner engines (including the LANDesk Antivirus tool)
- Real-time scanning status (enabled or disabled)
- Scanner-specific pattern file versions (up to date or old)
- Last scan date (whether the last scan is within the maximum allowable time period specified by the administrator)

Antivirus scanner detection content versus virus definition content

Antivirus updates does not imply actual virus definition (or pattern) files. When you download third-party antivirus updates, only scanner detection content is downloaded to the default repository, but scanner-specific virus definition files are not downloaded. However, when you download LANDesk Antivirus updates, both the scanner detection content AND the LANDesk Antivirus-specific virus definition files are downloaded. LANDesk Antivirus virus definition files are downloaded to a separate location on the core server. The default virus definition file repository is the \LDLogon\Antivirus\Bases folder.

You must have the proper LANDesk Security Suite content subscription in order to download each type of security content.

A basic LANDesk Management Suite installation allows you to download and scan for LANDesk software updates, and to create and use your own custom definitions. For all other security and patch content types, such as platform-specific vulnerabilities, spyware, and including virus definition (pattern) files, you **MUST** have a LANDesk Security Suite content subscription in order to download the corresponding definitions. For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

After you specify the types of content you want to download and the other options on the Download updates dialog:

- To perform an immediate download, click **Update Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog. If you click **Close**, you'll be prompted whether you want to save the settings.
- To schedule a download security content task, click **Schedule update** to open the **Scheduled update information** dialog, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks.

Task-specific settings and global settingsNote that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific. However, all of the settings on the other tabs of the **Download updates** dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global setting it is effective for all security content download tasks from that point on.

To save your changes on any tab of this dialog at anytime, click **Apply**.

The **LANDesk Antivirus** tab contains the following options:

- **Virus definitions approved for distribution:** Displays the date and version number of the most recently approved virus definition files that are now available to distribute to your managed devices. Approved virus definition files are located in the default folder (\LDLogon\Antivirus\Bases) from which they are deployed to target devices as part of on-demand and scheduled antivirus scans. The exact time of the virus definition file update (downloaded from the LANDesk Security content site, which has the very latest known pattern files) is noted in parentheses below this field.
- **Virus definitions currently in pilot testing:** Displays the date and version number of the virus definition files currently residing in your pilot folder, if you've downloaded virus definitions to that location. Pilot testing helps you verify the validity and usefulness of a virus definition file before using it to scan your managed devices for viruses. Virus definitions that have been downloaded to the pilot test folder can be deployed to designated "test" target devices.
- **Virus definition updates**
 - **Immediately approve (make available to all computers):** Downloads virus definitions directly to the default folder (\LDLogon\Antivirus\Bases). Virus definitions downloaded to the default folder are approved and can be deployed to target devices for antivirus scanning.
 - **Restrict them to a pilot test first:** Download virus definition files to the pilot folder for testing purposes. Virus definitions in the pilot folder can be deployed to designated test machines before being deployed to your managed devices.
 - **Automatically approve pilot definitions after test period expires (during next update):** Automatically moves downloaded virus definition files from the pilot folder to the default virus definition folder when the next virus definition update after the time period specified below occurs. This option is available only if you're restricting virus definition file updates to a pilot test, and lets you automate the approval of definition files. If you don't enable this option, virus definition files in the pilot folder must be approved manually with the **Approve now** button.
 - **Minimum test period:** If you've enabled automatic approval of virus definitions in the pilot folder, this value specifies the duration of the test period. Be aware that during this period scheduled virus definition file update tasks are not processed.
 - **Get latest definitions:** Starts an immediate virus definition file download process. The **Updating Definitions** dialog shows download progress.
 - **Approve now:** Lets you move virus definition files from the pilot folder to the default virus definition folder so that they can be deployed to target devices for antivirus scanning.
- **Definition backups**
 - **Make backups of previous definitions:** Saves downloads of earlier virus definition files. This can be helpful if you need to go back to an older definition file to scan and clean infected files, or to restore a virus definition file that resolved a particular problem. (Virus definition file backups are saved in separate folders named by the date and time they were created, under: \LDLogon\Antivirus\Backups\)
 - **Number of backups to keep:** Specifies the number of virus definition file downloads to save.
 - **History:** Lists all of the available virus definition file backups.
 - **Restore:** Moves the selected virus definition file backup to the antivirus default folder so that they can be distributed to target devices.
 - **Delete:** Removes the selected virus definition file backup permanently from the core server.
- **Update now:** Immediately downloads the selected security content types. The **Updating Definitions** dialog shows progress and status of the download.

- **Schedule update:** Opens the **Scheduled update information** dialog, where you can type a unique name for this download task, verify the download settings, and click OK to save the task in the Scheduled task tool. (Note that only the definition types, languages, and definition and patch download settings are saved and associated when you create a particular task. Download settings on the other tabs of this dialog, such as patch download location, proxy settings, and alerting settings, are global, meaning they apply to all the security content download tasks. However, you can change those settings at any time and they will be effective for all security content download tasks from that point on.)
- **Apply:** Saves your selected download settings so that they are applied to the **Download updates** dialog and appear the next time you open the dialog.
- **Close:** Closes the dialog without saving your latest settings changes.

For a description of the options on the other tabs of the **Download updates** dialog, see "About the Download updates dialog" on page 723 in the Security and Patch Manager help section.

About the Configure LANDesk Antivirus settings dialog

Use this dialog to manage your LANDesk Antivirus settings. Once configured, you can apply antivirus settings to antivirus scan tasks. You can also assign antivirus settings to a change settings task in order to modify the default antivirus settings on managed devices with the LANDesk Antivirus agent.

Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.

This dialog contains the following options:

- **New:** Opens the LANDesk Antivirus settings dialog where you can configure the antivirus scan options.
- **Edit:** Opens the LANDesk Antivirus settings dialog where you can modify the selected scan and repair setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename. This is useful if you want to make minor adjustments to antivirus settings and save them for a specific purpose.
- **Delete:** Removes the selected setting from the database.

Note the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.

- **Close:** Closes the dialog, without applying a setting to the task.

About the Antivirus settings dialog

Use this dialog to create and edit an antivirus setting. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates.

You can create as many antivirus settings as you like and edit them at any time.

If you want to modify a device's default antivirus settings without redeploying an antivirus scan task, make your desired change to any of the settings on the various tabs of the Antivirus settings dialog, assign the new setting to a change settings task, and then deploy the change settings task to target devices.

Once configured, you can apply antivirus settings to antivirus scan tasks and to change settings tasks.

Antivirus settings

- **Name:** Identifies the antivirus setting with a unique name. This name appears in the LANDesk Antivirus settings drop-down list on an antivirus scan task dialog.

The **Antivirus settings** dialog contains the following tabs:

- "About the General tab" on page 653
- "About the Scheduled scan tab" on page 654
- "About the Virus scan tab" on page 655
- "About the Quarantine / Backup tab" on page 657
- "About the Real-time protection tab" on page 658
- "About the Virus definition file updates tab" on page 659

About the General tab

Use this tab to configure the basic antivirus scanner settings on target devices.

This tab contains the following options:

- **Show LANDesk Antivirus icon in system tray:** Makes the LANDesk Antivirus icon appear in the device system tray. The icon's appearance depends on the status of antivirus protection, indicating whether real-time protection is enabled. If the arrow icon is yellow, real-time protection is enabled meaning the device is continuously being monitored for viruses. If the icon is gray, real-time protection is not enabled.

End users can double-click the icon to open the LANDesk Antivirus client and perform tasks. They can also right-click the icon to access the shortcut menu and select to run a scan and update antivirus files.

- **Enable email scanning:** Enables real-time email scanning on target devices. Real-time email scanning continuously monitors incoming and outgoing messages (supported applications include: Microsoft Outlook), checking for viruses in both the body of the message and any attached files and messages. Any detected viruses are removed.
- **Enable right-click scanning:** Provides an option on the LANDesk Antivirus client that allows end users to select a file, group of files, folder, or group of folders, and right click the selection to perform an antivirus scan.
- **Scan for risky software in addition to viruses (extended database):** Provides an option on the LANDesk Antivirus client that allows end users to scan for riskware (i.e., FTP, IRC, remote control utilities, etc.) using an extended database that is loaded on the managed device.
- **Allow user to add files and folders to Trusted Items list:** Provides an option on the LANDesk Antivirus client that lets users identify files and folders they don't want scanned for viruses. Files and folders in this list are ignored by an antivirus scan. Users should be made aware that they should move only safe files to their trusted items list.
- **CPU utilization when scanning:** Lets you control CPU usage on target machines when LANDesk Antivirus runs an antivirus scan.
- **Owner:** Lets you specify an owner for the antivirus setting in order to prevent unauthorized modification. Only the owner and users with the LANDesk Administrator right can access and modify the setting. Other users can only view the setting. The public user option allows universal access to the setting.
- **Set as default:** Establishes this antivirus setting (including the option settings on all of the Antivirus setting dialog's tabs) as the default on target devices. Unless an antivirus scan task has a specific antivirus setting associated with it, the default settings are used during scan and definition file update tasks.
- **Restore defaults:** Restores the predefined default settings for all of the antivirus options on the dialog's tabs.

About the Scheduled scan tab

Use this tab to enable and configure a recurring scheduled antivirus scan on target devices.

LANDesk Antivirus scan types

You can scan your managed devices for viruses with scheduled scans, on-demand scans, as well as real-time file and email protection. End users can also perform on-demand scans of their own computer.

This tab contains the following options:

- **Have LANDesk Antivirus scan devices for viruses at a scheduled time:** Enables a recurring scheduled antivirus scan that runs on target devices according to the start time, frequency, time restriction, and bandwidth requirement you specify.
- **Change settings:** Opens the Schedule dialog where you can set the scheduling options. See "About the Schedule periodic antivirus scans dialog" on page 660.
- **Allow user to schedule scans:** Lets the end user create a local scheduled antivirus scan on their own machine.

About the Virus scan tab

Use this tab to specify which files to scan for viruses, what to exclude from the scan, and whether to use heuristics to scan for suspicious files.

This tab contains the following options:

- **Scan all file types:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Scan infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean. See below for a list of infectable file types.
- **Use heuristics to scan for suspicious files:** Utilizes the scanner's heuristic analysis capability when scanning target devices. Heuristic scanning attempts to detect files suspected of being infected by a virus by looking for suspicious behavior, such as: a program that is self-modifying, immediately tries to find other executables, or appears changed upon termination. Using heuristic scanning may negatively affect performance on managed devices.
- **Exclude the following files and folders**
 - **Add:** Opens the **Add excluded path** dialog where you can create new exclusions to specify the files, folders, or file types (by extension) you want to exclude from an antivirus scan associated with this setting.
 - **Edit:** Opens the selected exclusion so you can modify a file path, file name, file extension, and variables.
 - **Delete:** Removes the selected exclusion from the antivirus setting.

System restore point scanning

LANDesk Antivirus will scan the files in any system restore point folders that may exist on the managed device.

Infectable file types

Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned.

Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files. See below for a list of infectable file types by the file format's standard or original file extension.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN

- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

About the Quarantine / Backup tab

Use this tab to configure the size of the quarantine/backup folder, and the object restore options you want to make available to end users.

This tab contains the following options:

- **Limit size of quarantine/backup folder:** Allows you to specify the maximum size of the shared quarantine\backup folder on target devices. This folder is a safe, isolated storage area on devices that have LANDesk Antivirus. By default, the quarantine storage size is 50 MB and quarantined objects are stored for 90 days. Objects in the quarantine\backup folder can be rescanned, deleted, or restored.

Quarantined files are automatically rescanned with the latest virus definitions whenever an on-demand scan is run or whenever the antivirus pattern files are updated on the device, in order to find out if any infected objects can be cleaned. If a quarantined file can be cleaned, it is automatically restored and the user is notified.

When a virus infection is discovered, the infected file is first backed up (with a *.bak extension in the \LDClient\Antivirus\ folder) and then cleaned. If it can't be disinfected the original file it is moved to the quarantine folder (with a *.qar extension in \LDClient\Antivirus folder). Then the virus string is removed and the file is encrypted so it can't be accessed or executed.

- **Maximum size:** Specifies the maximum size of the shared quarantine/backup folder on devices with the LANDesk Antivirus agent.
- **Allow user to restore suspicious objects:** Provides end users the option of restoring suspicious objects detected by an antivirus scan or by real-time protection. Suspicious objects are those which contain code that is either modified or reminiscent to that of a known virus. Suspicious objects are automatically quarantined. If this option is checked, end users can move the original file from the quarantine folder to a specified destination folder or to its original location, where it was stored before quarantining, disinfection, or deleting. Note that If real-time protection is running, the restored file is scanned and if it's still infected it's put back in the quarantine.
- **Allow user to restore infected objects and risky software:** Provides end users the option of restoring infected objects detected by an antivirus scan or by real-time protection. Infected objects are those containing harmful code which is detected by a known viruses definition (pattern or signature) file. Infected objects can further damage managed devices. Risky software is essentially client software that has the possibility of being risky for the end user. For example: FTP, IRC, Mlrc, RAdmin, or remote control utility software. (In the case of a false-positive scan result, the end user may feel confident and comfortable enough to restore the file. This option lets users restore files to network shares. If they restore an infected file to the original location, the next antivirus scan will detect the same virus, even if it's false-positive, and simply put the file back in quarantine.)
- **User must enter password to restore objects:** Requires users to enter the specified password before they can restore suspicious or infected objects, or risky software. The user is prompted to enter the password when they attempt to restore the object from the quarantine/backup folder. If you enable this option to password protect quarantined objects, you must share this password with the users you want to be able to restore those objects.
- **Password:** Enter the password needed for users to restore quarantined objects.

About the Real-time protection tab

Use this tab to enable and configure real-time file protection, which files to protect and what to exclude, and end user notification.

Real-time protection is an ongoing (background) scan of specified files, folders, and file types by extension. When real-time protection is running, files are scanned for viruses every time they are opened, closed, accessed, copied, or saved.

When real-time protection is enabled, the LANDesk Antivirus system tray icon is yellow. The icon is gray when real-time protection is turned off.

This tab contains the following options:

- **Enable real-time file protection: Turns on real-time file protection on target devices. Real-time file protection runs in the background and scans for known viruses according to the downloaded virus definition files.**
- **Also show real-time messages on client:** Displays messages on target devices to notify users of certain LANDesk Antivirus activities. End users are notified when an infected file is detected, quarantined, deleted, skipped, or cleaned. Message dialogs show the path, file name, virus name, and a note telling the end user to contact their network administrator.
- **Allow user to disable real-time scanning for up to:** Provides an option on the LANDesk Antivirus client that allows the end user to turn off real-time file protection for a specified period of time. You should keep the amount of time to a minimum so that users can't disable real-time protection long term.
- **Scan all file types:** Specifies that files of all types on the target device are scanned by an antivirus scan. This may take a long time so it is a good idea to scan all file types with an on-demand scan rather than real-time protection.
- **Scan infectable files only:** Specifies that infectable files only are scanned. Infectable files are those types of files known to be vulnerable to virus infections. Scanning only infectable files is more efficient than scanning all files because some viruses affect only certain file types. However, you should make a habit of regularly scanning all the files with an on-demand scan in order to ensure devices are clean.

Infectable file types are identified by their format identifier in the file header rather than by their file extension, ensuring that renamed files are scanned. Infectable files include: document files such as Word and Excel files; template files that are associated with document files; and program files such as Dynamic Link Libraries (.DLLs), communication files (.COM), Executable files (.EXEs), and other program files.

- **Use heuristics to scan for suspicious files:** Utilizes the scanner's heuristic analysis capability when scanning target devices.

Heuristic scanning attempts to detect files suspected of being infected by a virus by looking for suspicious behavior such as a program that: modifies itself, immediately tries to find other executables, or is modified after terminating. Using heuristic scanning may negatively affect speed/performance on managed devices.

- **Exclude the following files and folders**

- **Add:** Opens the **Add excluded path** dialog where you can create new exclusions to specify the files, folders, or file types (by extension) you want to exclude from an antivirus scan associated with this setting.
- **Edit:** Opens the selected exclusion so you can modify a file path, file name, file extension, and variables.
- **Delete:** Removes the selected exclusion from the antivirus setting.

About the Virus definition file updates tab

Use this tab to configure virus definition (pattern) file updates scheduling, user download options, and access options, for target devices with this antivirus setting.

This tab contains the following options:

- **Download pilot version of virus definition files:** Download virus definition files from the pilot test folder instead of from the default repository (\LDLogon\Antivirus\Bases) on the core server. Virus definitions in the pilot folder can be downloaded by a restricted set of users for the purpose of testing the virus definitions before deploying them to the entire network. When you create an antivirus scan task, you can also select to download the latest virus definitions updates, including those residing in the pilot test folder, then associate an antivirus setting with this option enabled to ensure that the test machines receive the latest known virus definition files. If this option is selected, virus definition files in the default folder (\LDLogon\Antivirus\Bases) are not downloaded.
- **Users may download virus definition updates:** Provides end users on target devices the option of downloading virus definition files by themselves. This option displays on the LANDesk Antivirus client and can be accessed from that dialog as well as by right-clicking the LANDesk Antivirus system tray icon.

When an end user downloads virus definition file updates, the device attempts to connect to servers in the following order: preferred server (if one is configured); core server; LANDesk Security content server website.

- **Schedule virus definition updates:** Enables a recurring scheduled virus definition file update that runs on target devices according to the start time, frequency, time restriction, and bandwidth requirement you specify.
- **Change settings:** Opens the Schedule dialog where you can set the scheduling options. See "About the Schedule periodic antivirus updates dialog" on page 661.
- **Internet Updates:**
 - **Download directly from LANDesk if the core is not available:** Allows target devices to download virus definition file updates directly from the LANDesk Security site in the event that they can't access their core server. Downloads would occur via this Internet connection whether initiated as a scheduled task or by the end user. This is useful if you have mobile users who want to keep their virus definitions files up to date.
 - **Select update source site:** Specifies the LANDesk Security content server that is accessed to download the latest definitions your database. Select the server nearest your location.
 - **Fall back to alternate source site on failure:** Automatically attempts to download updates from another LANDesk Security content server, with the antivirus signatures, if the specified source site is unable to transmit files.

About the Add excluded path dialog

Use this dialog to add exclusions that specify objects that aren't scanned for viruses by either an antivirus scan or real-time protection. Antivirus scan tasks (and change settings tasks) associated with this antivirus setting will use these exclusions.

You can exclude specific files, entire folders, and file types by their extensions.

This dialog contains the following options:

- **Type:** Indicates the type of object you want excluded from antivirus scanning. Select a type and then enter its precise attributes in the Object field.
- **Object:** Type the full file path and name of (or browse to and select) the file or folder you want to exclude. If you selected the file extension type, type the extension's characters in the Object field.
- **Insert variable:** Allows you to use system environment variables to identify the path to a folder or an object that you would like to exclude from the antivirus scan or protection scope.

About the Schedule periodic antivirus scans dialog

If you want this antivirus setting to include a recurring antivirus scan, use this dialog to specify start time, frequency, time restriction, and bandwidth requirement settings. Antivirus scan tasks (and change settings tasks) associated with this setting will use the rules defined here.

All criteria in this dialog that you configure must be met before the task will execute. For example, if you configure a schedule that repeats every day between 8 and 9 o'clock with a **Machine state of Desktop must be locked**, the task will only execute if it's between 8 and 9 o'clock AND the machine is locked.

This dialog contains the following options:

- **Schedule:**
- **Start:** Click this option to display a calendar where you can select the day you want the task to start. Once you pick a day, you can also enter a time of day. These options default to the current date and time.
- **Run periodically:** Schedules the scan to recur periodically.
 - **Run every:** Check this option to select the number of minutes, hours, and days to control how often the task repeats. If the time period is longer than one day, the scan runs at the start time above.
 - **Run when user logs in:** Check this option to run the task whenever a user logs in. When a user logs in, the local scheduler will run the task directly.
 - **Run whenever the machine's IP address changes:** Check this option if you want the task to run if the device's IP address changes or is renewed through DHCP.
- **Run only once:** Schedules the scan to occur one time only.
- **Run filters:**
- **Time of day:** If you want the task to run between certain hours, select the start and end hours. The hours are in 24-hour (military) time format.
- **Day of week:** If you want the task to run between certain days of the week, select the start and end days.

- **Day of month:** If you want the task to run between certain dates of the month, set the start and end dates.
- **Device bandwidth required:** Enforces a minimum bandwidth requirement for target devices in order for the antivirus scan to run successfully.
 - **Minimum bandwidth:** When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute. (You can select these minimum bandwidth options:
 - RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
 - WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
 - LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools | Configuration | Agent Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.
 - **Computer name:** Identifies the computer that is used to test the device bandwidth. The test transmission is between a target device and this computer.
- **User logged in state:** If you want the task execution criteria to include a logged in state, select one of these states: **User must be logged in**, or **User must be logged out**.
- **Machine locked state:** If you want the task execution criteria to include a machine state, select one of these states: **Screen saver or desktop locked**, **Desktop must be locked**, **Machine must be idle**. The criteria for the idle state are: the OS is locked, the screen saver is active, or the user is logged out.
- **Additional random delay once all other filters pass:** If you want an additional random delay, use this option. If you select a random delay that extends beyond the time limits you configured for the task, the task may not run if the random value puts the task outside the configured time limits.
- **Delay up to:** Select additional random delay you want.
- **And at least:** If you want the task to wait at least a certain number of minutes before executing, select this option. For example, if you're scheduling an inventory scan, you could enter a five here so a computer has time to finish booting before the scan starts, improving the computer's responsiveness for the user.

About the Schedule periodic antivirus updates dialog

If you want this antivirus setting to include a recurring virus definition update, use this dialog to specify start time, frequency, time restriction, and bandwidth requirement settings. Antivirus scan tasks (and change settings tasks) associated with this setting will use the rules defined here.

For information about the options, see "About the Schedule periodic antivirus scans dialog" on page 660 above since it is a common dialog.

About the Create LANDesk Antivirus scan task dialog

Use this dialog to create and configure a task that runs an antivirus scan on target devices. Scanner behavior, scanned objects, and end user options are determined by its associated antivirus settings.

On-demand antivirus scan

You can also run an immediate antivirus scan on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), click **LANDesk Antivirus scan now**, select an antivirus setting, choose whether to update virus definition files before scanning, and then click **OK**.

This dialog contains the following options:

- **Task name:** Identifies the antivirus scan task with a unique name.
- **Create a scheduled task:** Adds the scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
 - **Automatically target all LANDesk Antivirus machines:** Adds managed devices that have been configured with the LANDesk Antivirus agent to the task's target devices list.
 - **Start now:** Runs the antivirus scan on devices with the LANDesk Antivirus agent, adding it to the Scheduled tasks tool, as soon as you and click **OK**.
- **Create a policy:** Adds the antivirus scan task as a policy to the Scheduled tasks window, where you can configure the policy's options.
- **LANDesk Antivirus settings:** Specifies antivirus settings used for the scan task.

Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select a setting from the drop-down list. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Antivirus settings dialog" on page 653.

- **Update virus definitions (including pilot) before scan:** Automatically updates virus pattern files on target devices before the scan is launched, including virus definition files that currently reside in the pilot folder.

About the Antivirus activity and status information dialog

Use this dialog to view detailed antivirus activity and status information for all of your managed devices with the LANDesk Antivirus agent. This scan result data is used to generate the LANDesk Antivirus reports available in the **Reports** tool.

To customize the scope and focus of data that is displayed, click **Thresholds** and change the time period thresholds for scanned device's recent antivirus activity and devices that haven't recently been scanned.

You can also right-click a device in this view to access its shortcut menu and directly perform available tasks.

This dialog contains the following options:

- **Refresh:** Updates the fields in the dialog with the latest antivirus scan information from the database.
- **Thresholds:** Opens the **Threshold settings** dialog, where you can define the duration (in days) for both recent antivirus activity and "not recent" antivirus scanning. Thresholds determine the time period for which antivirus scan results are gathered and displayed for the two computer-specific display categories.
- **Infections by computer:** Lists devices in the right pane on which virus infections were discovered during the last system scan. Select a device to see the specific viruses infecting the device.
- **Infections by virus:** Lists viruses in the right pane that were discovered on managed devices during the last system scan. Select a virus definition to see the devices it has infected.
- **Computers not recently scanned for antivirus vulnerabilities:** Lists all of the devices with the LANDesk Antivirus agent that have not been scanned for viruses within the time period specified on the **Threshold settings** dialog. If you want to run an immediate antivirus scan, right-click the device, click LANDesk Antivirus scan now, select an antivirus setting, and then click OK.
- **Computers with recent antivirus activity:** Lists all of the devices with the LANDesk Antivirus agent that have been scanned and have returned antivirus activity within the time period specified on the **Threshold settings** dialog. Select a device to see its specific antivirus activities, including: virus detection, removal, infected object quarantine, backup, and restoration.

About the Threshold settings dialog (for LANDesk Antivirus)

Use this dialog to define time periods for antivirus scan results that appear in the **Antivirus activity and status information** dialog.

- **Threshold for recent antivirus activity:** Indicates the maximum number of days for which antivirus activity is reported from scanned devices to the core server.
- **Threshold for not recently scanned:** Indicates the maximum number of days to check for devices that haven't been scanned for viruses.

About the Install or update LANDesk Antivirus task dialog

Use this dialog to create and configure a task that installs the LANDesk Antivirus agent on target devices that don't yet have it installed, or updates the existing version of the LANDesk Antivirus agent on target devices that already have it installed. (The LANDesk Antivirus installation is executed by the Security and Patch Manager tool's security scanner.)

You can also select to have existing antivirus software automatically removed from the device before installing LANDesk Antivirus. See below for a list of antivirus products that can be removed.

This task lets you conveniently deploy and update a managed device's LANDesk Antivirus agent (and associated antivirus settings) without having to redeploy a full agent configuration.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Show UI:** Indicates whether the security scanner dialog displays the progress of the LANDesk Antivirus agent installation/update on target devices.
- **Remove existing antivirus agent:** Automatically removes other antivirus software that might already be installed on devices before installing LANDesk Antivirus. (**Note:** You can also select to remove existing antivirus software from managed devices when doing an initial agent configuration.)
- **LANDesk Antivirus settings:** Specifies antivirus settings associated with this particular LANDesk Antivirus agent installation.

Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select a setting from the drop-down list. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Antivirus settings dialog" on page 653.

- **Scan and repair settings (reboot only):** Specifies the scan and repair settings associated with this particular LANDesk Antivirus agent installation. The task will use the selected scan and repair settings' reboot options **ONLY**, which determine reboot requirements and actions on target devices during LANDesk Antivirus agent installation.

Antivirus products that can be automatically removed during configuration

Antivirus products that can be automatically removed when deploying LANDesk Antivirus include:

- Symantec* Antivirus (versions 7, 8, 9, and 10)
- McAfee* Enterprise (versions 7.0, 8.0i, and 8.5)
- Trend Micro* PC-cillin 2004, 2005, and 2006
- Trend Micro OfficeScan
- Trend Micro ServerProtect
- eTrust* Antivirus (versions 6, 7, 7.1, and 8)

About the Remove LANDesk Antivirus dialog

Use this dialog to create and configure a task that removes the LANDesk Antivirus agent from target devices.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the task.

- **Create a scheduled task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Show UI:** Indicates whether the security scanner dialog displays the progress of the LANDesk Antivirus agent removal from target devices.
- **Scan and repair settings:** Specifies the scan and repair settings associated with this particular LANDesk Antivirus agent removal task. The task will use the selected scan and repair settings' reboot options ONLY, which determine reboot requirements and actions on target devices during agent removal.

Handheld Manager help

Handheld Manager's file exchange feature lets you place files on Pocket PC handhelds or transfer files from Pocket PC handhelds to the core server.

About the Windows CE CAB wizard dialog

The **Windows CE CAB wizard** dialog has these options:

- **CAB file name:** The filename for the cab you're creating. Don't include a path. CABs are saved in the core server's \Program Files\LANDesk\ManagementSuite\PocketPCCABS folder.
- **Select file to include in CAB:** The path and name of the file you're including in the .CAB.
- **File destination on the handheld:** Where to place the file on the handheld.
- **Add/Remove:** Once you've specified a .CAB name, file to include, and a file destination, click **Add** to add the file to the .CAB. You can add as many files as you want by entering the file information and clicking the **Add** button after each one.
- **Create:** Creates the .CAB based on the information you provided.

About the Handheld files to back up dialog

The **Handheld files to back up** dialog has these options:

- **Handheld path and file name to back up:** The full path and filename on the handheld that you want to back up. You don't need to include a drive letter. For example: \Program Files\landesk\test.doc.
- **Add/Remove:** Use these buttons to add or remove files you want to back up.
- **Delay between buffer writes:** How long the handheld waits after sending one buffer's worth of data. Use this to influence the amount of network bandwidth the backup consumes.
- **Write buffer size:** How much data to send before the buffer write delay occurs. Use this to influence the amount of network bandwidth the backup consumes.

Inventory help

About the Inventory window

Use the **Inventory** window to view a device's complete inventory, including the following components:

- **BIOS:** Type, date, ID bytes, manufacturer, ROM version, SMBIOS version, and system model for the BIOS. The BIOS permanently resides in the computer's ROM (read-only memory) and enables the computer's memory, disk drives, and monitor to communicate.

Additional BIOS information appears in the Inventory window as BIOS text strings. To view and search BIOS text strings, expand the **BIOS** object, select **BIOS Strings**, right-click the **Data** attribute and select **Properties**, and then click **Extended Values**. During an inventory scan, the available text strings are exported to the BIOS to a text file, LDBIOS.TXT. You can set up a query in the LDAPPL3.INI file that outputs one or more of the BIOS text strings to the console. For more information, see "Appendix A: Additional inventory operations and troubleshooting" on page 595 .

- **Bus:** Bus type. The bus connects the microprocessor, disk drives, memory, and input/output ports. Bus types can be ISA, EISA, VESA Local Bus, PCI, and USB.
- **Coprocessor:** Type of coprocessor, if present. The coprocessor is distinct from the main microprocessor, though it can reside on the same motherboard or even the same chip. The math coprocessor evaluates floating point operations for the main microprocessor.
- **Environment:** File locations, command path, system prompt, and other variables for the Windows environment.
- **Keyboard:** Keyboard type attached to the device. Currently, the most common type of keyboard is the IBM-enhanced keyboard. Code page is the language the keyboard uses.
- **LANDesk Management:** Information about the agents, client manager, and Alert Management System (AMS). Also contains information about the inventory scanner and initialization files.
- **Mass Storage:** Storage devices on the computer, including floppy drives, hard disks, logical and tape drives, and CD-ROM. The hard disk and floppy drive objects include head, number, sector, and total storage attributes.
- **Memory:** Page file, physical, and virtual memory attributes. Each of these memory objects includes byte attributes. The first byte is the amount of memory available. The second byte is the total memory.
- **Mouse:** Type of mouse attached to the device. Mouse type values include PS/2, serial, and infrared.
- **Network:** Network adapter, NIC address, and the adapter's node address information. The Network object includes information for each protocol loaded on the computer. Typical values include IPX*, NetBEUI, NetBIOS, and TCP/IP objects.
 - **IPX** is a protocol that NetWare* servers can use to communicate with their devices and other servers. The IPX object contains the address, network number, and node address attributes.
 - **NetBEUI** allows a computer to communicate with Windows NT/2000, Windows for Workgroups, or LAN Manager servers. Microsoft now recommends using TCP/IP for these connections.
 - **NetBIOS** is an interface (API) for applications to send and receive packets to each other over TCP/IP, NetBEUI, or IPX.

- **TCP/IP** is a protocol that enables a computer to communicate over the Internet and with WANs. This object contains the address (contains the computer's TCP/IP address), host name (contains the computer's DNS context), IP routing enabled, and NetBIOS resolution (uses DNS and WINS proxy enabled attributes).
- **Network Adapters:** Attributes for every installed network adapter on the device.
- **OS:** Operating system, drivers, services, and ports. These objects and their attributes vary according to the configurations of the loaded drivers and services.
- **Ports:** Objects for each of the computers output ports (serial and parallel). Each output port contains address and name attributes. The address attribute contains the hardware address for the port.
- **Printers:** Objects for each printer connected to the computer, either directly or through a network. The printer objects contain driver, name, number, and port attributes. The port attribute contains either the network queue or the port the printer is connected to.
- **Processor:** Attributes of the device's CPU. Detects Intel, Motorola 680x0, and PowerPC processors.
- **Resources:** Objects for every hardware resource of the computer. Each hardware resource object contains attributes that describe the type of resource and any ports and interrupts it is using.
- **Software:** Objects for every software application installed on the device's hard drive. Each software program object lists attributes that typically contain the software name, location, and version number.
- **Video:** Objects for each video adapter on the device. The video adapter object typically contains attributes that describe the resolution and the number of supported colors.

About the Inventory attribute properties dialog

Use this dialog to view an attribute's properties. The **Characteristics** tab can display the following information. Depending on the attribute and whether you are adding, editing, or viewing an attribute, not all fields may appear.

- **Name:** The name of the core database attribute whose properties you're viewing.
- **Value:** The value assigned to this inventory attribute.
- **User defined:** Indicates whether the selected attribute was defined by the user or not. This option can't be changed.
- **Format specifier (Integer values only):** Notation used to display the value in appropriate form. For example, %d MB displays the attribute value without decimal values; %.1f MB displays the attribute value to the first floating decimal point in MB units. If no factor value is entered, this format specifier must describe integer values (%d). If a factor value is entered, this format specifier must describe floating point values (%f).
- **Factor (Integer values only):** Integer value used to divide the attribute into units. If you change the factor value, you must enter the appropriate code in the format specifier field. For example, to view the number of Megabytes if the attribute is recorded in Kilobytes, enter the value 1000.
- **Formatted value:** Sample text demonstrating the specified format and factor.

About the Inventory change settings dialog

Use this dialog to select which inventory attributes are logged when changes occur at individual devices, and to determine where those changes are logged.

- **Current inventory:** Lists all objects stored in the core database. Click an object to display its attributes in the Log event in list. Expand an object group to see the data objects contained within it.
- **Log event in:** Lists the attributes of the inventory object selected in the Current inventory list.

To set where inventory changes are logged, select an attribute and check one or more options. Check the **Inventory** option to log inventory changes in the device's **Inventory changes history** dialog. Check the **NT Log** option to log inventory changes in the Windows NT event log. Check the **AMS** option to send inventory changes as an alert via AMS (configure AMS alerts with the Alert Settings tool).

- **Log/Alert severity:** Lists the alert priority options. This feature is dimmed until an attribute is actually selected. You can select a severity level of None, Information, Warning, or Critical.

About the Inventory changes history dialog

Use this dialog to view a device's inventory changes. You can also print and export the inventory changes history from this dialog.

- **Device Name:** Displays the name of the device(s) selected in the console's network view for which inventory change data is requested.
- **Component:** Identifies the system component that has changed. (Only components selected in the **Inventory Change Settings** dialog can appear here.)
- **Attribute:** Identifies the specific component attribute being logged.
- **Time:** Indicates when the change occurred.
- **New Value:** Shows the new (changed value for the listed attribute).
- **Old Value:** Shows the old (previous value for the listed attribute).
- **Print:** Opens a standard print dialog where you can print the contents of the inventory changes history.
- **Export:** Opens a Save As dialog where you choose a name and location for the exported .CSV file containing the inventory changes history.

You can click a column heading to sort the listing by that attribute. Click the heading again to reverse the sort order.

About the Create/Edit a Custom Data Form dialog

Custom data forms are not supported in LANDesk Security Suite

Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite license in order to use the custom data forms feature.

Use this dialog to create or edit a custom data form.

- **Form name:** Identifies the form and appears on the form viewer when a user fills out the form.
- **Description:** Provides additional information to users about the form.
- **Add:** Opens the **Add question** dialog where you can create a new question for the form.
- **Edit:** Opens the **Edit question** dialog where you can edit any of the question's options.

- **Delete:** Removes the question from the form.
- **Page break:** Controls the layout of the form by adding page breaks to group questions on pages. When there's a page break, users click the Next button to proceed to questions on the next page.

Note: The maximum number of questions per page is nine.

- **Preview:** Opens the form so that you can preview how it will look for users. In preview mode, you don't have to fill in any data and nothing you type is saved.

About the Add/Edit question dialog

Use this dialog to create or edit questions that appear on the custom data form. Forms consist of questions and a place for users to put their answers. First, identify the question:

- **Question text:** One-line description of what's being asked for. This text appears beside the data field.
- **Inventory Name:** Name of the database field in the core database. If you wanted to query the core database for this item, the label ID is what you would query on.
- **Description:** Additional information that appears when users click Help (or press F1 while in this question's data field).

You also need to specify what type of data field (control to show beside each question, and if it is required). The available data fields are:

- **Edit box: Users** type their answer in an editable text box.
- **Combo box (edit list):** Users select one of the predefined list items, or type in a new one of their own.
- **Combo box (fixed list):** Users select one of the predefined list items.
- **Make the control a required field to fill out:** Forces the user to answer the question. The user can't finish a form or move to the next form page before responding to required fields.

About the Add items dialog

Use this dialog to add items to a drop-down list that the user can choose from when answering that question on a form.

- **Item name:** Identifies the item. This name appears in the question's drop-down list.
- **Items list:** Lists all the items that appear in the question's drop-down list.
- **Insert:** Places the item in the Items list.
- **Delete:** Removes the item from the Items list.

About the Select Multiple Forms to Distribute dialog

Use this dialog to create a group of forms that shows the group name and lists available forms that can be part of a group.

- **Name of group:** Identifies the group in the **Custom data forms** window.
- **Available forms:** Lists all of the available forms you can add to the group.

- **OK:** Saves the group and closes the dialog.
- **Cancel:** Closes the dialog without saving the group.

Local accounts management help

About the New user dialog

Use this dialog to create a new user. For more information, see "Managing local users" on page 285.

- **User name:** Specifies the user name for the new user
- **Full name:** Specifies the full name of the user.
- **Description:** Provides a description of the user
- **Password:** Specifies a password for the user to authenticate to the console.
- **Confirm password:** Confirms the password.
- **User must change password at next logon:** Causes the user to have to change their password upon initial logon into the console.
- **User cannot change password:** Disallows the users from changing the password.
- **Password never expires:** Causes the password to never expire, so the user won't have to change the password.
- **Account is disabled:** Disables the account.

About the Edit user dialog

Use this dialog to edit the user properties. The dialog consists of three configuration tabs, **General**, **Member of**, and **Profile**.

For more information, see "Managing local users" on page 285.

General

Use this configuration page to specify the user name, full name, and description of the user. You can also change some of the account properties.

- **User name:** Specifies the user name of the user (if available).
- **Full name:** Specifies the full name of the user.
- **Description:** Specifies the description of the user
- **User must change password at next logon:** Specifies if the user to has to change their password upon logging in to the console.
- **User cannot change password:** Specifies if the user can change their password.
- **Password never expires:** Specifies if the password will expire.
- **Account is disabled:** Specifies if the account is disabled.
- **Account is locked:** Unlocks the account so the user can authenticate to the console. This option is available when the user has unsuccessfully tried to log in to their account over three times in one session.

Member of

Use this configuration page to assign the user to groups.

- **Selected groups:** Lists the groups the user is a member of.
- **Add:** Launches the **Select groups** dialog, which enables you to add the groups you want the user to be a member of.
- **Remove:** Removes the user as a member of the selected groups and removes the groups from the list.

Profile

Use this configuration page to specify the account information for the user.

- **User profile path:** Specifies the network path to the user's account and profile.
- **Logon script:** Specifies the logon scripts.
- **Local path:** Specifies a local path as the home directory.
- **Connect:** Specifies a network directory as the home directory. Select a drive and then insert the network path.

About the Group properties dialog

Use this dialog to configure the group. For more information, see "Managing local groups" on page 286.

- **Group name:** Specifies the name of the group.
- **Description:** Provides a description of the group.
- **Members:** Lists the users that belong to the group.
- **Add:** Launches the **Select users** dialog, which enables you to add users to the group.
- **Remove:** Removes the selected users from the group.

Configuring the LANDesk Management Gateway

The LANDesk Management Gateway is an Internet appliance that provides secure communication and functionality over the Internet. It acts as a meeting place where console and managed devices are connected through their Internet connections—even if they are behind firewalls or use a proxy to access the Internet.

Read this topic to learn about:

- "Setting up the Management Gateway connection" on page 672
- "Posting the core certificate to the Management Gateway" on page 672
- "Managing client certificates" on page 672
- "Creating an on-demand remote control agent package" on page 673

Setting up the Management Gateway connection

The **Gateway information** tab lets you specify and test the connection and proxy settings used by the core to connect to the Management Gateway.

To specify the connection information

1. On the **Gateway information** tab, specify the Management Gateway information.
2. If the Management Gateway uses an internal address that is different from its public address (for example, if it's located in a DMZ-type environment, check **Use separate internal address** and specify the internal name and address).
3. If the core will connect to the Management Gateway through a proxy, check **Use proxy** and specify the proxy settings.
4. Click **Test settings** to test the core server connection to the Management Gateway.
5. If the test fails, check the information you entered and correct any mistakes, then click **Test settings** to make sure the connection works.

Posting the core certificate to the Management Gateway

Before the core can connect through the Management Gateway, you must post the core certificate to it.

To post the core certificate

1. On the **Certificates** tab, click **Post to Management Gateway**.
2. Click **OK** to post the certificate.

Managing client certificates

Each managed device is required to have a valid digital certificate in order to connect through the Management Gateway. You can manage the list of devices that have been granted certificates by blocking or deleting the ability of any formerly trusted device to connect through the Management Gateway.

To block or delete connection ability

1. Select the device(s) you want to block or delete. You can use **Shift-click** or **Ctrl-click** to select multiple devices.
2. Click **Block selection** or **Delete selection**.
3. When finished, click **OK**.

To unblock connection ability

1. Uncheck the **Block** checkbox for each device you want to unblock.
2. When finished, click **OK**.

Creating an on-demand remote control agent package

You can create an on-demand remote control agent package that can be downloaded by devices that have not been configured to connect through the Management Gateway. This allows them to be remote controlled through the Management Gateway.

To create an on-demand remote control agent

1. Click the **Certificates** tab.
2. Click **Create**.
3. Specify the organization name. The device will only be viewable to administrators that belong to the same organization.
4. Click **Save**.
5. Specify the location to which you want the remote control agent to be saved.
6. Click **Save**.

After creating the remote control agent, you can distribute it on CD or post it to an accessible location for download by managed devices.

Managed device help

The **Agent configuration** window (**Tools | Configuration | Agent configuration**) is where you customize device agent configurations. Use the **Agent configuration** dialog to specify the agents you want to install and the options for those agents. You can create as many agent configurations as you want. Only one configuration can be the default. You can use this window to create Windows, Macintosh, Linux, and server agent configurations.

To create a configuration

1. Click **Tools | Configuration | Agent configuration**.
2. Click the **New** button to create a new Windows configuration. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the **Agent configuration** dialog as described in the following sections. Click **Help** on a page for more information.

Note: If you use the **Agent configuration** dialog to create a new default agent configuration, be aware that all devices who are configured by WSCFG32 using login scripts will be automatically reconfigured with the new default configuration settings the next time they log in, even if their current settings match the new default settings.

The following sections describe the **Agent configuration** dialog pages.

About the Agent configuration dialog's Start page

The **Agent configuration** dialog's **Start** page contains the following options:

- **Configuration name:** This option appears above all dialog pages. Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Default configuration:** Shows whether this configuration is the default configuration that gets installed. The only way to change this option is by clicking **Set as default** from the configuration's shortcut menu.

Agent components to install (standard):

- **Standard LANDesk agent:** Installs the standard LANDesk agent that forms the basis of communication between devices and the core server. This option is required. You can't disable it, but you can customize the components associated with it. (Note the security and patch scanner is automatically installed with the standard LANDesk agent, but you configure it with the options on the security and patch scan page below.)
- **Custom data forms:** Presents a form to users for them to complete. You can query the core database for the data users enter. Use this to retrieve customized information from users directly.
- **Remote control:** Lets you take control of a device or server from across the network. Minimizes the time it takes to resolve customer issues from a centralized help desk. Use this to provide remote management of devices across the LAN/WAN.

Agent components to install (distribution):

- **Software distribution:** Automates the process of installing software applications or distributing files to devices. Use this to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.
- **Profile migration:** Doesn't install a separate agent on devices; but ensures that the necessary LANDesk agents are present on managed devices in order for them to be capable of capturing and migrating user profiles.

Agent components to install (security):

- **LANDesk Trust Agent:** Installs the LANDesk Trust Agent (LTA) on managed devices, which allows the device to communicate with the LANDesk DHCP server and posture validation server. An agent is required in order to use the following LANDesk network access control solutions that enables compliance security (i.e., end-point security) scanning and remediation: LANDesk DHCP-based network access control, integrated Cisco NAC, and LANDesk IP Security authentication. (**Note:** If you've implemented the LANDesk DHCP solution or the LANDesk IP Security solution, you can use an agent configuration to install the LTA on managed devices. If you've implemented the Cisco NAC solution, you must manually install the Cisco Trust Agent (CTA) on managed devices. Keep in mind that you can also install the LTA on managed devices even if you're using the Cisco NAC solution in order to provide additional device management capabilities such as inventory scanner and local scheduler. In other words, with Cisco NAC, you can have both agents installed on the device. However, if you're using the LANDesk DHCP or LANDesk IP Security solutions, you should install only the LTA on managed devices.)

- **LANDesk Antivirus:** Installs the LANDesk Antivirus agent on managed devices. LANDesk Antivirus uses the security and patch scanner (installed with the standard LANDesk agent) to scan for and identify viruses on managed devices, and to provide options for handling infected files and folders. The LANDesk administrator downloads virus definition updates and configures virus scans at the Management Suite console, including how the LANDesk Antivirus client displays on managed devices and which options are available to the end user. You must first select the **LANDesk Antivirus** agent checkbox on the Agent configuration's **Start** page in order to configure the **LANDesk Antivirus** page.
- **LANDesk Host Intrusion Prevention:** Installs the LANDesk HIPS agent on managed devices. LANDesk HIPS proactively defends managed devices from zero-day attacks by monitoring applications and processes and blocking unauthorized actions based on customized rules and file certifications.

Other options:

- **Select all:** Selects all available agents in the **Agents to install** list.
- **Clear all:** Clears all available agents in the **Agents to install** list, except for **Standard LANDesk agent**, which is mandatory.
- **Defaults:** Selects all agents in the **Agents to install** list, except for the security agents: **LANDesk Trust Agent**, **LANDesk Antivirus**, and **Host intrusion prevention**.
- **Perform full inventory scan during installation:** When this configuration is installed on clients, whether to do a full inventory scan during the agent installation. The default is checked.
- **Show start menu on end user device:** When checked, creates Windows Start menu entries for installed agents that have a user interface. Clearing this option installs the agents but doesn't create any Start menu entries.
- **Temporary install directory:** Specifies the temporary folder used on managed devices during agent installation. This folder must be writeable for agent installation to succeed.

Deploying the standard LANDesk agent (includes the inventory scanner, local scheduler, and security scanner)

All Management Suite components require the standard LANDesk agent (formerly known as CBA), which is installed by default on all device installations. Among other things, the standard LANDesk agent provides device discovery and manages core server/device communication.

Use the Standard LANDesk agent pages to configure the Standard LANDesk agent, which includes these components and settings:

- Inventory scanner
- Local scheduler
- Bandwidth detection
- Device reboot options

About the Agent configuration dialog's Standard LANDesk agent page

Use this page to configure certificate-based security and what scope devices using this configuration will have.

Trusted certificates

Select the core server certificates you want devices to accept. Devices will only communicate with cores and consoles they have certificates for. For more information on certificates and copying them from other core servers so you can select them here, see "Agent security and trusted certificates" on page 90.

Below the trusted certificates box you can modify the core server that devices using this agent configuration will communicate with. By default, this box contains the current core server. The core name can either be a Windows computer name, an IP address, or fully-qualified domain name. A fully-qualified domain name for a core may be necessary if you'll be pushing agent configurations to devices in multiple domains or anytime a device can't resolve the core name unless it is fully-qualified. Managed devices will use the information you enter here to communicate with the core server, so make sure the name you enter is resolvable from all devices that will receive this configuration.

The core name you enter here as part of an agent configuration are added to a device's registry under:

- HKLM\Software\Intel\LANDesk\LDWM\CoreServer

Once you've selected trusted certificates, and changed the core name if necessary, you can test them. When you click **Test**, a message box appears indicating whether the device name or IP address you entered was resolvable. Note that the **Test** button doesn't ping the device you entered or verify that the name or IP address belongs to a core server.

Scope

If you want devices to be included in scopes that are based on custom directories, enter a directory path in the **Path** field. The path you enter here defines the device's computer location inventory attribute. Scopes are used by Management Suite's role-based administration to control user access to devices, and can be based on this custom directory path.

Custom directory paths use a format that's similar to a file path, but with forward slashes as separators. If you want to use custom directory-based scopes, first decide how you want to categorize your devices for role-based administration. You might do categorize devices by geographic locale, department or group name, or any other organizational detail you prefer.

Directory paths you enter here as part of an agent configuration are added to a device's registry under:

- HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation

You don't have to fill in this field. If you leave it blank, the device's computer location attribute is defined by its Active Directory or eDirectory path.

When the inventory scanner is run on a device, it records the device's computer location inventory attribute. If you entered a custom directory path in the **Path** field, that path is the directory the scanner records. If you left the custom directory path blank, the scanner tries to populate the computer location inventory attribute with the device's Active Directory or NetWare eDirectory path. If neither a custom directory path or an LDAP-compliant directory is found, the computer location attribute isn't defined. However, the device can still be accounted for in both query scopes or device group scopes.

For more information on how scopes are used in Management Suite's role-based administration, and how you can define a scope using custom directory paths, see "Role-based administration" on page 59.

About the Agent configuration dialog's Inventory scanner page (under standard LANDesk agent)

The **Agent configuration** dialog's **Inventory scanner** page contains the following features:

- **Manual update:** The software list used to exclude titles during software scans is loaded down to each remote device. Each time the software list is changed from the console, you must manually resend it to remote devices.
- **Automatic update:** Remote devices read the software list from the core server during software scans. If this option is set, each device must have a drive mapped to the LDLOGON directory on the core server so they can access the software list. Changes to the software list are immediately available to devices.
 - **Update using HTTP:** Beginning with Management Suite 8, the inventory scanner can use HTTP for LDAPPL3.INI file transfers. This allows the scanner to support Targeted Multicast features like polite bandwidth and peer download. Peer download allows devices needing LDAPPL3.INI updates to check with the core server for the latest version's date, then broadcast to peers on their subnet to see if a peer has the update in its multicast cache. If a peer has the update, the file transfer happens on the local subnet without generating network traffic across routers or WAN links.
- **At startup using the run key registry setting:** Check this option if you want inventory scans to run at startup. You can also click **Change settings** and configure a custom schedule based on time, day of week or month, whether a user is logged in, on IP address changes, and available network bandwidth. If you clear **At startup using the run key registry setting** and don't configure additional settings by clicking **Change settings**, inventory scans won't run automatically.

About the Agent configuration dialog's Local scheduler page (under standard LANDesk agent)

The local scheduler agent enables Management Suite to launch device tasks based on a time of day or bandwidth availability. The local scheduler agent is most useful for mobile computers that may not always be on the network or may connect to the network via a dialup connection. For example, you can use the local scheduler to allow mobile computer package distribution only when those devices are on the WAN.

When you schedule software packages for distribution, or when you create application policies, you can specify which bandwidth the packages or policies require before they are applied.

The local scheduler runs as a service on Windows NT/2000/XP, or as a pseudo-service on Windows 95/98.

The **Local scheduler** page contains the following features:

- **Enter the frequency that the agent polls for tasks:** How often the local scheduler checks for tasks. The default is 10 seconds. The polling interval you select is stored on the local computer.
- **Bandwidth detection frequency:** How often the local scheduler should check bandwidth. The default is 120 seconds. Bandwidth checks happen only when there's a pending scheduled task.

About the Agent configuration dialog's Bandwidth detection page (under standard LANDesk agent)

Bandwidth detection enables bandwidth detection between devices and the core server. You can limit Management Suite actions such as software distribution based on available bandwidth. Use this option if you have remote devices or devices that connect to the network via a slow link.

The **Agent configuration** dialog's **Bandwidth detection** page contains the following features:

- **Choose bandwidth detection method:** Select whether to use ICMP or PDS for bandwidth detection. ICMP sends ICMP echo requests of varying sizes to the remote device and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup connections). However, not all routers or devices support ICMP echo requests.
If your network isn't configured to allow ICMP echo requests, you can select PDS. The PDS bandwidth tests aren't as detailed, but they detect either a LAN or a low-bandwidth RAS (typically dialup connection). The PDS method only works if the PDS service is running on the package server. You can install this service by deploying the standard LANDesk agent to the package server.
- **LAN threshold, in bits per second:** The threshold that classifies a connection as WAN rather than LAN. The default is 262144 bps.
- **Enable dynamic throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. This option also forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted.
This option is also available from the **Delivery methods** dialog. If you enable this option in agent configuration but not in the **Delivery methods** dialog, it will still be enabled on the device. If you don't enable this option in agent configuration but do enable it in the **Delivery methods** dialog, dynamic bandwidth throttling will be enabled on the device for that package script.

About the Agent configuration dialog's Device reboot options page (under standard LANDesk agent)

Once you install Management Suite agents on devices, they may need a reboot to complete the agent configuration. The **Agent configuration** dialog's **Device reboot options** page contains the following features:

- **Do not reboot devices after configuration:** Devices won't reboot, even if the selected components require a reboot. If a reboot is necessary, components won't work correctly until the device reboots.
- **Reboot devices if necessary:** Reboots devices only if a selected component requires a reboot.
- **Reboot with user option to cancel:** If a selected agent requires a reboot, users will have the option to cancel the reboot. If a reboot is necessary, components won't work correctly until the device reboots. You can select how long the reboot prompt stays on the user's screen before the computer reboots. This timeout is useful for users that are away from their computers when the device deployment happens.
- **Allow user to cancel reboot within this time period:** If you want to give users a chance to cancel the reboot before it happens automatically, enter how long you want the reboot prompt to appear.

Deploying alerting rulesets

Alert rulesets define which events require immediate action or need to be logged for your attention. A ruleset contains a collection of alert rules, each of which has a corresponding alert action. When you define an alert ruleset you can deploy it to one or more devices to monitor the items that are important for that kind of device.

You can deploy one of the predefined rulesets or you can deploy rulesets you've created inside the alerting tool.

The Alerting page contains the following features:

- **Add:** Click **Add** to add an existing ruleset to the **Selected alert ruleset** list. Rulesets in this list will be deployed to devices receiving this agent configuration.
- **Remove:** Click a ruleset and click **Remove** to remove it from the **Selected alert ruleset** list.

Deploying custom data forms

You can create and distribute custom data forms to collect device information that will supplement the standard information available in the core database. The forms you create using the Form Designer can be distributed by a device deployment service or by using the **Agent configuration** dialog.

Customize the forms that are distributed to devices in your management domain using the form designer. For more information, see "Using custom data forms" on page 118.

About the Agent configuration dialog's Forms sent with agent page

The custom data forms section consists of two pages. The **Custom data forms** page contains the following features:

- **Manual update forms:** Selected forms are sent to each device. If the forms change or new forms are added, you must manually resend the forms to remote devices.
- **Automatic update:** Remote devices check the core server for updated forms each time the inventory scanner is run, such as at startup. Each device must have a drive mapped to the LDLOGON directory on the core server to access the updated forms.
- **Display forms to end user:** Choose how remote devices access custom forms:
 - **On startup:** The selected forms run automatically at startup on each device.
 - **When inventory scanner runs:** The selected forms run only when the inventory scanner is run on each device. The inventory scanner runs automatically on startup, and can be run manually by devices at any time.
 - **When launched from the LANDesk program folder:** The selected forms appear as items in the device's LANDesk Management folder. They aren't automatically run.

The **Forms sent with agent** page lists all defined custom data forms. Mark which forms are made available to devices receiving this configuration task. You'll have to create forms (**Tools | Configuration | Custom Data Forms**) before they can appear in this list.

Deploying software distribution

Software distribution automates the process of installing software applications and distributing files to devices. Use this agent to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.

Software distribution uses a Web or file server to store packages. Devices access this package server when downloading a package. You'll need to configure a package server as described in the software distribution chapter in the *User's Guide*. You can deploy the software distribution agent to devices before you set up a package server. For more information, see "Software distribution" on page 162.

About the Agent configuration dialog's Software distribution page

The **Agent configuration** dialog's **Software distribution** page contains the following features:

- **Client destination:** The location where deployed virtualized applications are stored on managed devices. This option has no effect if you aren't distributing virtualized applications created with the LANDesk Application Virtualization add-on.

About the Agent configuration dialog's Policy options page (under software distribution)

The policy-based distribution agent enables you to automatically install sets of applications on groups of devices. Use this agent to manage groups of devices that have common software needs.

The LANDesk software deployment portal runs on managed devices and shows available software for that managed device. To display available software, the software deployment portal needs to get policy information periodically from the core server. Policy updates happen when:

- A user launches the LANDesk software deployment portal from the Windows Start menu.
- At logon if the run at logon **LANDesk software deployment portal** option is checked.
- At logon if the run at logon **Update policy information from core** option is checked.
- At the local scheduler interval you specify when you click the **Change settings** button. By default, managed devices use the local scheduler to get policy updates once a day .

The **Policy options** page contains the following features:

- **LANDesk software deployment portal:** If checked, the managed device shows the LANDesk software deployment portal after a user logs on. Users can then see what software is available for them.
- **Update policy information from the core:** If checked, the managed device updates policy information after a user logs on.
- **Change settings:** Use this to change how often and when the local scheduler will look for policy updates. This schedule is in addition to any of the run at logon options you check.

Deploying remote control

When deploying remote control, you need to consider which security model you want to use. You have these choices:

- **Local template:** This is the most basic security that uses whatever remote control settings are specified on the device. This model doesn't require any other authentication or group membership.
- **Windows NT security/local template:** This security model uses a Windows NT Remote Control Operators group. Members of this group are allowed to remote control devices. Permitted users still use the device's remote control settings, such as permission required.
- **Certificate-based/local template:** This is the most secure option and is new to Management Suite 8. It's also known as on-demand secure remote control and is described in the next section.
- **Integrated security:** This is the new default security model that was added in Management Suite 8.7.

About certificate-based on-demand secure remote control

LANDesk Management Suite 8 introduces a new on-demand secure remote control (certificate-based/local template) that you can use. This new remote control improves on the prior version in these ways:

- Remote consoles authenticate with the core server.
- The remote control agent on a device loads on-demand once a remote control session is authorized by the core.
- All remote control authentication and traffic is encrypted over an SSL connection.
- Once remote control finishes with a device, the remote control agent unloads.

Here's an outline of the remote control communication flow:

1. The Management Suite console asks the core server for permission to remote control the specified device.
2. If the console/user is authorized to remote control the specified device, the core server tells the device to load the remote control agent with a randomly generated set of authentication credentials.
3. The core server passes the authentication credentials to the console.
4. The console authenticates to the device with the authentication credentials and remote control begins.

Warning: On-demand remote control requires the core server

With on-demand remote control, if the core server isn't available, consoles won't be able to remote control devices. On-demand remote control requires the core server to work.

About Integrated security

Integrated security is the new default security model. It is similar to certificate-based remote control, except the remote control agent is always loaded and remote control begins more quickly. Here's an outline of the integrated security remote control communication flow:

1. The remote control viewer connects to the managed device's remote control agent, but the agent replies that integrated security authentication is required.
2. The viewer requests remote control rights from the core server.
3. The core server calculates remote control rights based on the viewer's scope, role-based administration rights, and Active Directory rights. The core server then creates a secure signed document and passes it back to the viewer.
4. The viewer sends this document to the remote control agent on the managed device, which verifies the signed document. If everything is correct, the agent allows remote control to begin.

Warning: Integrated security requires the core server

With integrated security remote control, if the core server isn't available, consoles won't be able to remote control devices. Integrated security remote control requires the core server to work.

Using Windows NT security/local template with Windows XP devices

For Windows NT security/local template authentication to work with Windows XP devices, you must configure devices so that the Windows XP sharing and security model for local accounts is classic (local users authenticate as themselves). If you don't do this, the default guest-only authentication won't work with remote control's Windows NT security.

To set the Windows XP security model to classic

1. On the Windows XP device, click **Start | Control Panel**.
2. In the **Administrative Tools, Local Security Policy** applet, click **Security Options | Network access: Sharing and security model for local accounts**, and set it to **Classic - local users authenticate as themselves**.

About the Agent configuration dialog's Remote control page

The **Agent configuration** dialog's **Remote control** page contains the following features:

- **Local template:** Uses only the local device simple permissions set from the remote control **Permissions** page.
- **Windows NT security/local template:** Only allows members of the Remote Control Operators group to initiate remote control connections from the console to remote devices. Permitted users are still required to use the permissions set from the Remote Control Settings page of this wizard.
Since the Remote Control Operators group is a local group, each device has its own copy of the group. To avoid managing each device's Remote Control Operators group individually, include global (domain level) groups with each local group. Permitted users still use the device's remote control settings, such as permission required.
- **Certificate-based/local template:** Communication between the console and remote devices is authenticated using the core server; only consoles authenticated from the same core server can use remote control functions for these devices. Select the certificates you want to allow in the Trusted Certificates list. Permitted users are still required to use the permissions set from the **Permissions** page. This option is also known as on-demand secure remote control, as described earlier in this chapter.
- **Integrated security:** This is the default security model and is described earlier in this chapter. Permitted users are still required to use the permissions set from the **Permissions** page.

Adding users to the Remote control operators group and the View only group

If you select **Windows NT security/local template** as your security model, the **Remote control operators group** and **View only group** boxes list the users for the console or for the selected Windows NT domain. The users you select here will have remote control access to the devices that receive the settings defined in this configuration settings file. **View only group** users can only view remote devices. They can't take over the mouse or keyboard.

When adding users to one of the remote control groups, the console uses the logged-on user's Windows credentials, not the LANDesk console user's credentials, to list the users in a domain. If the **List users from** box isn't showing the domain you want, log in to Windows as a user with rights on that domain.

To choose from an existing server or domain

1. In the **Remote control** page, click **Windows NT security/local template** and click the **Add** button.
2. In the **List names from** box, select either the core server name or a Windows NT domain name containing user accounts.
3. In the user list, select one or more users and click **Insert** to add them to the **Inserted names** list.
4. Click **OK** to add the selected names to the Remote Control Operators group on each device that receives these configuration settings.
5. If you want any of these users to be in the **View only group**, select them and move them over. Users can only be in one group.

To manually enter names

You can enter names manually by clicking in the **Inserted names** list and using any of the following formats to enter names. Use semicolons to separate names.

- **DOMAINusername** where DOMAIN is the name of any domain accessible to the target device.
- **MACHINEusername** where MACHINE is the name of any device in the same domain as the target device.
- **DOMAINgroupname** where DOMAIN is the name of any domain accessible to the target device, and groupname is the name of a management group in that domain.
- **MACHINEgroupname** where MACHINE is the name of any device in the same domain as the managed node, and groupname is the name of a management group on that device.

If you don't specify a domain or device name, it is assumed that the user or group specified belongs to the local device.

Click **OK** to add the names to the Remote Control Operators user group on the target device.

About the client setup dialog's Permissions page (under remote control)

The **Remote control** section's **Permissions** page contains the following features:

- **Remote control:** Grants permission to control the device.
- **Reboot:** Grants permission to reboot the device.
- **Chat:** Grants permission to chat with the device.
- **File transfer:** Grants permission to transfer files to and from the device's local drives.
- **Run programs on remote device:** Grants permission to run programs on the device.
- **Draw:** Grants permission to use the viewer window's drawing tools on the device.

You can also specify these remote control settings:

- **Permission required:** Requires the console user to receive permission from the device before any kind of remote access is granted.

- **Only when the user is logged on:** Prompts the user currently logged on for permission. If nobody is logged on, remote control doesn't require permission.
- **Ask for all permissions at once:** Prompts user once for session permissions. Normally with permission required, the user has to permit remote control, chat, file transfer, and so on individually. This option gives permission for all remote control-related options for the duration of a session.
- **View only:** Remote control operators can only view the device, they can't interact with it remotely.

About the Indicators page (under remote control)

The **Remote control** section's **Indicators** page contains the following features:

- **Floating desktop icon:** Displays the remote control agent icon on the device screen at all times or only when being remotely controlled. When being controlled by the console, the icon changes to show a magnifying glass and the icon's title bar turns red.
- **System tray icon:** Places the remote control agent icon in the system tray. Again, the icon can be visible all the time or only while being remotely controlled.
- **Use mirror driver:** Checked by default, this option uses the remote control mirror driver on devices for faster remote control performance.
- **Use screen blanking driver:** Checked by default, this option uses a special driver that can tell the target device's display driver to turn off the monitor. When active, this driver filters commands going to the real display driver to prevent them from turning the monitor back on. Remote control operators can turn screen blanking on or off from the remote control viewer application. If you're having compatibility problems with this driver, you can clear the checkbox to use a more compatible but possibly less effective mode of screen blanking. If you don't use the screen blanking driver, the alternative mode of screen blanking may cause some screen flicker on the target device during remote control. This option requires the mirror driver.

When using certificate-based remote control security, the indicator is only visible during remote control. This security model unloads the remote control agent and the indicator icon when remote control isn't being used.

Deploying and configuring the LANDesk security and patch scanner

The security and patch scanner agent is installed by default with the standard LANDesk agent. However, you need to use the options on the specific Security and patch scan page when creating device agent configurations in order to configure certain aspects of how and when the security scanner runs on managed devices. You can also enable and configure custom variable override settings, frequent security scans, real-time spyware, and application blocking

The security scanner allows you to scan managed devices for known OS and application vulnerabilities and other security risks, such as: spyware, viruses, unauthorized applications, software and driver updates, system configuration security threats, custom security definitions, and more. The content of your security scan depends on your Security Suite content subscription and which security type definitions you've downloaded with the Security and Patch Manager tool. You can also remediate detected problems via autofix, repair tasks, and repair policies. For details on these procedures, see *Using Security and Patch Manager in the Users Guide*.

Information about the following security-related pages can be found below. Click a link to go to that section.

- "About the Agent configuration dialog's LANDesk Antivirus page" on page 689
- "About the Agent configuration dialog's Windows Firewall page" on page 690
- "About the Agent configuration dialog's LANDesk Host Intrusion Prevention (HIPS) page" on page 691
- "About the Agent configuration dialog's Agent Watcher page" on page 691
- "About the Agent configuration dialog's Extended Device Discovery page" on page 692
- "About the Agent configuration dialog's LANDesk 802.1x Support page" on page 693

About the Agent configuration dialog's Security and patch scan page

Use this page to configure how the security scanner is launched and how it behaves on managed devices with this agent configuration. (You can also run security scans as scheduled tasks and policies from the console, or manually at a managed device.)

The **Security and patch scan** page contains the following options:

- **During login using the Run key registry setting:** Places the security scanner in the Windows registry's run key which causes the scanner to launch whenever a login occurs on managed devices with this agent configuration.
- **Change settings:** Opens the **Schedule security and patch scan** dialog, where you can configure scheduling settings for security scans that are launched by the local scheduler. The local scheduler automatically launches a security scan on a recurring basis, at the earliest opportunity within the time period and restrictions you specify. You can also configure options for running the security scanner when a device meets certain conditions, such as: only when a user is logged in, only if a specified minimum bandwidth is available, and any time a device's IP address changes. Once you've configured these scheduling settings for the security scanner, simply click **Save** to return to the main page where the scheduling criteria now appears.

- **Global settings:** Applies to all devices with this agent configuration, overriding task-specific settings.
 - **Never reboot:** Ensures devices with this agent configuration won't reboot when the security and patch scanner is running. This is a global setting for all devices with this agent configuration, which means it overrides any end user reboot settings that are applied to either a security scan or repair task. In other words, regardless of the end user reboot settings used by a security task, this global setting will take precedence. Check this option if you know you don't want devices to reboot during any security and patch scanner operation, and leave it clear if you want to be able to configure the reboot options with the Security and patch manager tool.
 - **Never autofix:** Ensures devices with this agent configuration won't allow a security and patch scan to perform an auto fix when remediating detected vulnerabilities, even if the vulnerability has auto-fix enabled. As a global setting for all devices with this agent configuration, this setting overrides any end user auto-fix setting you've applied to a security scan task. Use this setting if you want to guarantee devices can't have detected vulnerabilities automatically remediated by a security scan.
- **Scan and repair settings:** Determines the information displayed by the security scanner on managed devices, end user interaction, reboot operation, and content settings when the scanner is launched on managed devices with this agent configuration by the method selected above (run key during login, local scheduler, or both). Select a scan and repair setting from the drop-down list to apply it to the configuration you're creating. You can also click **Configure** to create and apply a new scan and repair setting or to edit an existing one.

About the Custom Variables page (under security and patch scan)

Use this page to assign a custom variable override setting to devices with this agent configuration.

The security and patch scanner can utilize custom variables (editable values included in certain security types' definitions) to scan for and modify specific settings, and to implement standard system configuration settings to managed devices. You can change the value of a setting and select whether to override the current value with the new value, and then use this agent configuration to apply the configuration to target devices. In some situations you may want to ignore a custom variable setting, or in other words create an exception to the rule. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules.

A custom variable override setting is not required with an agent configuration.

You can select an existing setting from the drop-down list, click **Configure** to create a new setting, or leave the field blank.

This **Custom Variables** page contains the following options:

- **Custom Variable settings:** Specifies custom variable override settings used on target devices when they're scanned for security definitions that include custom variables (such as security threats and viruses). Custom variable override settings let you specify setting values you want to ignore or bypass during a security scan. This is very useful in situations where you don't want a scanned device to be identified as vulnerable according to a definition's default custom variable settings. Select a setting from the drop-down list. From the drop-down list, you can also select to remove the custom variable override settings from target devices. The **Remove custom variable settings** option lets you clear a device so that custom variable settings are in full affect. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Custom variable override settings dialog" on page 751.

About the Frequent security scan page (under security and patch scan)

Use this page to enable and configure a recurring security scan for a specific collection of high-risk vulnerabilities or other security definitions on devices with this agent configuration. A frequent security scan is useful if you need to regularly scan devices for particularly aggressive and harmful security attacks.

Group scans only

Frequent security scans are based on the security definitions contained in a group you've selected from predefined security content groups in Security and Patch Manager.

This page contains the following options:

- **Use the frequent security scanner:** Enables a frequent security scan on devices with this agent configuration.
- **Scan only when a user is logged in:** Restricts the frequent security scan so that it runs only if a user is logged into the target device.
- **Every:** Specifies the time interval for a the frequent security scan.
- **Choose a scan and repair setting (that scans for a group):** Specifies the scan and repair settings that control the security scanner for frequent security scans. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, and user interaction. The setting you select must be configured to scan a group, not a type. You can also click **Configure** to create a new scan and repair setting that is associated with a group.

About the Spyware page (under security and patch scan)

Use this page to enable real-time spyware detection and notification on devices with this agent configuration.

Real-time spyware detection checks only for spyware definitions that reside in the **Scan** group in Security and Patch Manager, and that have autofix turned on. You can either manually enable the autofix option for downloaded spyware definitions, or configure spyware definition updates so that the autofix option is automatically enabled when they are downloaded.

Real-time spyware detection monitors devices for new launched processes that attempt to modify the local registry. If spyware is detected, the security scanner on the device prompts the end user to remove the spyware.

This page contains the following options:

- **Enable real-time spyware blocking:** Turns on real-time spyware monitoring and blocking on devices with this agent configuration.
- **Notify user when spyware has been blocked:** Displays a message that informs the end user a spyware program has been detected and remediated.
- **If an application is not recognized as spyware, require user's approval before it can be installed: Even if the detected process is not recognized as spyware according to the device's current list of spyware definitions, the end user will be prompted before the software is installed on their machine.**

About the Application blocker page (under security and patch scan)

Use this page to enable real-time unauthorized application blocking and notification. Real-time application blocker checks only for applications that reside in the **Scan** group in Security and Patch Manager.

With real-time application blocking, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to those unauthorized applications. Security and Patch Manager uses the LANDesk Software license monitoring tool's softmon.exe feature to deny access to specified application executables even if the executable file name has been modified because softmon.exe reads the file header information.

This page contains the following options:

- **Enable blocking of unauthorized applications:** Turns on real-time application blocking on devices with this agent configuration.
- **Notify user when an application has been blocked:** Displays a message that informs the end user they have attempted to launch an unauthorized application and access has been denied

About the Agent configuration dialog's LANDesk Antivirus page

Use this page to select an antivirus setting that applies to devices with this agent configuration, and to select whether to remove any existing antivirus products from those devices when they are configured.

In order to select an antivirus setting, you must first check the **LANDesk Antivirus** agent's checkbox on the **Start** page.

Antivirus settings let you control how the antivirus scanner operates on target devices. You can define antivirus scan parameters such as: files and folders to be scanned or excluded, manual scans, real-time scans, scheduled scans, quarantine and backup options, virus pattern file update options, and the information and interactive options that display on end user devices during the antivirus scan.

Deploying LANDesk Antivirus to devices that already have an antivirus product installed

If another antivirus product is installed on target devices, you can select to have it removed automatically during LANDesk agent configuration by selecting the **Remove existing antivirus product** option. If you choose not to remove the other antivirus product during agent configuration, LANDesk Antivirus is disabled until you manually remove the other product. However, you can still deploy the LANDesk Antivirus agent to target devices.

For a current list of antivirus products that can be removed from devices when deploying LANDesk Antivirus, see "Antivirus products that can be automatically removed during configuration" on page 478.

This page contains the following options:

- **Remove existing antivirus product:** Automatically removes other antivirus software that might already be installed on devices before installing LANDesk Antivirus. (**Note:** You can also select to remove existing antivirus software from managed devices when creating an **Install or update LANDesk Antivirus** task with Security and Patch Manager.)
- **LANDesk Antivirus settings:** Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select a setting from the drop-down list. Click **Configure** to create a new setting. For more information, see "About the Antivirus settings dialog" on page 653.

About the Agent configuration dialog's Windows Firewall page

Use this page to enable and configure the Windows firewall on managed devices with this agent configuration. You can enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs).

You can use this feature to deploy a configuration for the firewall on the following Windows versions:

- Windows 2003/XP
- Windows Vista

This page contains the following options:

- **Configure Windows firewall:** Enables automatic Windows firewall configuration on devices with this agent configuration.

- **Choose a Windows firewall setting:** Specifies the Windows firewall settings deployed on target devices with this agent configuration. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click **Configure** to create and apply a new scan and repair setting or to edit an existing one.

About the Agent configuration dialog's LANDesk Host Intrusion Prevention (HIPS) page

Use this page to select a HIPS setting for managed devices with this agent configuration. HIPS settings determine whether the LANDesk HIPS client is password protected, availability of interactive options to end users, signed code handling, operating mode, and file certifications.

In order to select a HIPS setting, you must first check the **LANDesk HIPS** agent's checkbox on the **Start** page.

LANDesk HIPS is compatible with LANDesk Antivirus and Symantec Antivirus

LANDesk HIPS is supported on managed devices with either LANDesk Antivirus or Symantec Antivirus installed. Do NOT deploy LANDesk HIPS to devices with any other antivirus solution installed.

This page contains the following options:

- **Host Intrusion Prevention settings:** HIPS settings determines how LANDesk HIPS appears and operates on protected devices. Select a setting from the drop-down list. Click **Configure** to create a new setting. For more information, see "About the Host Intrusion Prevention settings dialog" on page 502.

About the Agent configuration dialog's Agent Watcher page

Use this page to enable and configure the LANDesk Agent Watcher utility on devices with this agent configuration.

Agent watcher allows you to actively monitor devices for selected LANDesk agent services and files. Agent watcher restarts agent services that have been stopped and resets the startup types for services that have been set to automatic. The utility also removes monitored agent files from lists of files to be deleted on reboot, in order to prevent deletion. Additionally, Agent watcher alerts you when agent services cannot be restarted, when agent files have been deleted, and when agent files are scheduled to be deleted on reboot.

This page contains the following options:

- **Use the Agent Watcher:** Enables the LANDesk Agent Watcher utility on devices with this agent configuration.
- **Check for changes in selected configuration:** Automatically checks for settings changes in the selected (deployed) agent watcher setting. If a change is detected, the updated agent watcher setting is automatically deployed to the devices with this agent configuration.
- **Interval to check:** Specifies the time interval to check for changes in the selected agent watcher setting.

- **Choose an Agent Watcher setting:** Specifies agent watcher settings deployed on target devices with this agent configuration. Agent watcher settings determine which services and files are monitored and how often, as well as whether the utility remains resident on the device. Select a setting from the drop-down list. Click **Configure** to create a new setting. For more information, see About the Agent watcher settings dialog.

About the Agent configuration dialog's Extended Device Discovery page

Use this page to enable and configure Extended device discovery on managed devices with this agent configuration.

Extended device discovery is an extension of Unmanaged device discovery tool, and finds devices on your network that haven't submitted an inventory scan to the core database. With extended device discovery, you can use one or both of the following discovery methods: ARP (address resolution protocol) discovery, and WAP (wireless access point) discovery.

With ARP discovery, the extended device discovery agent listens for network ARP broadcasts. The agent then checks any ARP-discovered devices to see whether they have the standard LANDesk agent installed. If the LANDesk agent doesn't respond, the ARP-discovered device displays in the Computers list. Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

Keep in mind that you don't have to deploy the extended device discovery agent to every managed device on your network, though you can if you want to. Deploying this agent to several devices one each subnet should give enough coverage.

This page contains the following options:

- **Use Address Resolution Protocol (ARP):** Enables extended device discovery using the address resolution protocol (ARP) discovery method on devices with this agent configuration.
- **Choose an ARP discovery setting:** Specifies the ARP setting that controls the extended device discovery agent when performing ARP discovery on your network. ARP settings determine the discovery scan frequency and logging level. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click Configure to create and apply a new setting or to edit an existing one
- **Use Wireless Access Point discovery (WAP):** Enables extended device discovery using the wireless application protocol (WAP) discovery method on devices with this agent configuration.
- **Choose a WAP discovery setting:** Specifies the WAP setting that controls the extended device discovery agent when performing WAP discovery on your network. WAP settings determine the discovery scan frequency and logging level. Select a setting from the drop-down list to apply it to the configuration you're creating. You can also click Configure to create and apply a new setting or to edit an existing one.

- **Configuration download frequency (in minutes):** Specifies how often managed devices with the extended device discovery agent installed check with the core server for an updated extended device discovery configuration. The agent always updates its configuration from the core when it first loads. The default value is 720 minutes (12 hours). If you set this value too high, it will take a long time for configuration changes to propagate to devices. If you set this value too low, there will be more load on the core server and the network.

About the Agent configuration dialog's LANDesk 802.1x Support page

Use this page to enable the 802.1X implementation of LANDesk Network Access Control (NAC). You can use LANDesk 802.1X to enforce your compliance security policy on managed devices that support 802.1X, by running compliance security scans, granting or blocking access depending on device health status (compliance), quarantining unhealthy (non-compliant) devices, and performing remediation.

This page contains the following options:

- **Enable LANDesk 802.1x support:** Turns on 802.1X network access control on devices with this agent configuration. (**Note:** This option is unavailable if you haven't already enabled the 802.1X Radius Server in the console's LANDesk NAC tool.). LANDesk 802.1X uses the EAP type specified in LANDesk NAC in the Security and Patch Manager tool. The EAP type setting is core-wide. In other words, all devices configured with this agent configuration will be configured with the EAP type specified in the console.
- **Use IP in self-assigned range:** Specifies that devices determined to be unhealthy (non-compliant), based on the compliance security policy, will be sent to a quarantine network area using the TCP/IP protocol's built-in self-assigned IP address range functionality.
- **Use DHCP in quarantine network:** Specifies that devices determined to be unhealthy (non-compliant), based on the compliance security policy, will be sent to a quarantine network area using a DHCP server and remediate server you've configured on your LANDesk network.
 - **Select remediation server:** Specifies the remediation server you want to use for repairing unhealthy devices so that they can be scanned again and allowed access to the corporate network.
- **Quarantine client if no health scan has been performed within:** Use this option to automate device quarantine by specifying a maximum period of time a device can be considered healthy without having a compliance security scan run on it. If this time expires without a scan, the device is automatically placed in the quarantine network area.

Client Setup Utility

About the Client Setup Utility dialog

The **Agent configuration utility** dialog displays the status of a scheduled device configuration task as the task is processed. This dialog is for information only; the devices to be configured were selected when the task was scheduled.

The **Agent configuration utility** dialog contains the following features:

- **Clients to configure:** Lists the devices scheduled to receive these configuration settings.
- **Clients being configured:** Lists the devices that have been contacted by the console and are in the process of being configured with this settings file.
- **Clients completed:** Lists the devices that the console has configured during this scheduled session. If the configuration attempt was successful, the status is Complete. If the configuration attempt failed for any reason, the status is Failed. These statuses are mirrored in the Scheduled Tasks window when this task is selected.
- **Creating configuration files:** Displays a status bar indicating the completion status of the entire configuration task.

Deploying to NetWare servers

You can install the inventory scanner to NetWare servers. The NetWare agent configuration utility will modify the AUTOEXEC.NCF to load the scanner on startup. You must have the NetWare client loaded on the console you're installing the agent from and you must have write access to the NetWare server you want to install the agents on.

To install remote control and inventory on a NetWare server

1. In the Management Suite console, click **Configure | Deploy LDMS client to NetWare server**.
2. Enter the NetWare server name. Click **Install**, and then click **OK**. This installs the agents to the NetWare server.

About the Add a bare metal server dialog

Use the **Add a bare metal server** dialog to add devices to the queue so they can have provisioning tasks run on them. This is particularly helpful for the initial provisioning of new devices. Devices are added to the holding queue by using an identifier. A server identifier is a piece of information that can be used to uniquely identify a server. A server identifier may be a MAC address (most common), a vendor serial number, an IPMI GUID, or an Intel AMT GUID. In all cases, the identifier must be able to be queried by an agent running in the preboot environment on the target server. You can add devices one at a time or many at a time.

To add a single device

1. In the **Network view**, expand the **Configuration** group. From the **Bare metal server** item's shortcut menu, click **Add devices**.
2. Type a descriptive name in the **Display name** box. While the display name is optional, it is highly recommended. On a bare-metal device, the **Display name** is the only differentiator in the Provisioning view.
3. Select an identifier type from the upper drop-down list (any of Mac address, serial number, IPMI GUID, or Intel AMT GUID), and enter the **Identifier**.
4. Click **OK**.

To add multiple devices

1. In the **Network view**, expand the **Configuration** group. From the **Bare metal server** item's shortcut menu, click **Add devices**.
2. In the lower drop-down list, select an identifier type, and type the location of a text file (CSV) which contains the identifier information in the text box (or click Browse to find the file), and click **Import**.

Each identifier should be separated by comma in the CSV file. Import file format: identifier; display name.

Deploying to Linux servers

You can use the console's agent configuration tool to deploy agents to these Linux versions:

- Red Hat Linux 7.3, 8.0, and 9
- Red Hat Linux Enterprise 3 and 4
- SuSE Linux 9.3

For more information on Linux agent deployment, see "You can use LANDesk Management Suite to manage supported Linux/UNIX distributions. " on page 93.

About the Start page (under Linux Agent configuration)

The Linux **Agent configuration's Start** page has these options:

- **Configuration name:** Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Standard LANDesk agent, Remote control, and Software distribution:** These options install by default and you can't disable them.
- **LANDesk vulnerability scanner:** Installs the Linux version of the vulnerability scanner. The scanner only reports on problems, it doesn't remediate them.
- **Defaults:** Resets the options to default (disables the **LANDesk vulnerability scanner** option).

About the Standard LANDesk agent page (Under Linux Agent configuration)

The Linux **Agent configuration**'s **Standard LANDesk agent** page has these options:

- **Trusted certificates for agent authentication:** certificates control which core servers can manage devices. Check the core server certificates that you want installed with this configuration. For more information, see "Agent security and trusted certificates" on page 90.
- The other options on this page are dimmed and don't apply to Linux agent configurations.

About the Inventory scanner page (Under Linux Agent configuration)

The **Linux Agent configuration**'s **Inventory scanner** page has these options:

- **Start inventory scan:** You can select **Daily, Weekly, or Monthly**. The option you select adds a command to the server's cron.daily, cron.weekly, or cron.monthly file that runs the inventory scanner.

About the Remote control page (Under Linux Agent configuration)

The **Linux Agent configuration**'s **Remote control** page has these options:

- **Run as a service using Windows NT security:** The agent runs as a service, and runs in the background. It uses NT-based security. If you want to add users or groups to use NT-based remote control, you must add them to the Remote Control Operators group.
- **Run on-demand using certificate-based security:** The agent only runs when needed. It uses certificate-based security.

About the Rulesets page (Under Linux and Default server agent configuration)

Both the **Linux Agent configuration** and the **Default Server Agent Rulesets** pages have these options:

- In the **Rulesets** tab, select any monitoring and/or alerting rulesets you want included with the configuration. These rulesets are stored in the Idlogon/alertrules folder. New rulesets can be created in the System Manager **Monitoring** or **Alerting** tools. In order for newly-created rulesets to display in the drop-down lists, you must generate the XML for the custom ruleset in the Server Manager console.

About the Server reboot options page (Under Linux and Default server agent configuration)

The **Linux agent configuration** reboot options page is disabled. The **Default server agent configuration** page has these options:

- Do not reboot servers after configuration: Doesn't reboot the server, even if it's necessary to finish agent configuration. You will need to reboot the server manually before all agents will work correctly.
- Reboot servers if necessary: Automatically reboots the server if necessary.
- Reboot servers always: Always reboots the server.

About the System Manager page (Under Default windows configuration)

The System Manager page is available if you have installed System Manager on your core server. It has these options:

- **Install monitoring:** Installs the System Manager monitoring agent on devices. This agent reports device health to the core server. You can configure alerts in the System Manager console based on the monitoring agent data.
- **Monitoring and Alerting:** Select any monitoring and/or alerting rulesets you want included with the configuration. These rulesets are stored in the Idlogon/alertrules folder. New rulesets can be created in the System Manager **Monitoring** or **Alerting** tools. In order for newly-created rulesets to display in the drop-down lists, you must generate the XML for the custom ruleset in the System Manager console.

OS deployment and Profile migration wizard help

This chapter contains the following context-sensitive help topics for the OS deployment/Migration tasks wizard.

Help for the OS deployment/Migration tasks wizard

This chapter provides descriptions of the options and settings found on each page (and dialog) of the OS deployment/Migration tasks wizard. This wizard is used to create scripts that capture or deploy OS images, and capture or restore user profiles. Scripts can then be scheduled as tasks on target devices on your network. The wizard is accessed from either the Toolbar button or shortcut menus in the Manage Scripts window (**Tools | Distribution | Manage Scripts**).

You can also access this information by clicking the Help button on the corresponding wizard page itself.

For detailed step-by-step instructions on how to use the OS deployment/Migration tasks wizard, and what you need to know in order to plan and implement image deployment and migration jobs, see "OS deployment" on page 226 and "Profile migration" on page 272.

Note: All pages of the OS deployment/Migration tasks wizard are described here. However, the pages you actually see when running the wizard depends on the type of imaging or migration task you selected on the first page of the wizard.

About the OS deployment/Migration tasks wizard: Choose a task page

Use this page to specify which type of OSD/profile migration script you want to create, based on the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost*, PowerQuest*, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a User-initiated profile migration package that can be run locally at individual devices.
 - **Continue with file capture errors:** Allows the profile capture process to continue even if files designated to be captured report file errors (such as invalid file names, locked files, or files that change size during the capture). The profile capture completes, and file errors are recorded in the log file.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Deploy image (with profile capture and restore):** Creates a script that performs a comprehensive deployment and migration job (capturing profile data, deploying an OS image, and then restoring the profile).
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files to target devices).
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches on devices).

About the General page

Use this page to configure the following characteristics of an OS imaging task:

Note: Some of the options listed below may be disabled, depending on what type of task (capture or deploy) you selected.

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** Additional text you can add to describe the script.
- **Choose network adapter to use if the driver autodetection fails:** (capture image only) Ensures that the image deployment job is successful to all target devices. We recommend that you enable this option, and then select a network adapter that is common to your systems. This is especially important if you're deploying to laptops. You should **carefully choose a listed network adapter to ensure your job succeeds.**

OS deployment uses a phased approach to network adapter detection:

- OS deployment first tries to detect the network adapter from the target device's operating system prior to imaging over it.
- If that fails, OSD will reboot the target device and try to detect the network adapter from DOS.
- If that fails, OSD uses the network adapter you specified in the Undetectable network adapters option on this page of the wizard.
- If the adapter you specify fails, you must go to the target device and manually reboot it. The device will reboot normally into its original OS.

About the Capture profile dialog: General page

Use this page to identify the OS deployment or profile migration script. The text you enter here is used when the script displays in the Manage Scripts and Scheduled Tasks windows:

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** (Optional) Helps you remember the script with the text you type in here.
- **Continue with File capture errors:** Allows capture to continue, even if there are errors during the capture.

Note: If you add this script to the LANDesk PXE DOS Menu, the description you enter here will appear in the menu.

About the capture image dialog: Credentials page

Use this page to provide authentication credentials for the network share, or shares, where the OS image and the imaging tool used to create the image are stored:

Note: You can enter only one set of credentials that will be used to access both shares, so the shares must have matching credentials. The credentials must belong to a local user account on the device hosting the share.

- **Domain and user name:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password/Confirm password:** Enter and confirm the user's password.

About the capture image dialog: Image type and path page

Use this page to specify the image type you want to capture with this script, where the image will be stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the image file captured by this script, selected from the list of imaging tools.

- **Enter the UNC path to the desired image, including the name of the image:** Locates the server and share where the image file will be stored. The image must be stored on a share accessible by devices. Note that the share name cannot include any spaces. You can enter just the device name in UNC format, then browse for the remainder of the path by clicking the browse button. In some cases, browsing for a path will insert a local path. You must convert this to UNC format.

Note: During the imaging process, devices will map this UNC path to drive I:.

- **Enter the UNC path to the imaging application, including the name of the application:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename. Note that the share name cannot include any spaces. In some cases, browsing for a path will insert a local path. You must convert this to UNC format.

Note: During the imaging process, devices will map this UNC path to drive H:.

About the capture image dialog: Additional commands page

Use this page to customize the script by adding custom commands.

- **Enter additional commands to after the end user device is rebooted and imaged:**
You can add commands in this text box, one per line, as if you were typing at a command prompt. Commands are sent to devices one at a time. These commands are run after the device is rebooted and imaged.

About the deploy image dialog: Methods and credentials page

Use this page to provide authentication credentials for the network share, or shares, where the OS image and the imaging tool used to create the image are stored:

- **Use Multicast:** Uses existing multicast domain representatives on subnets of your network to deploy the OS image via the LANDesk Targeted Multicast technology. Multicasting enables you to transmit software packages to multiple devices at once, significantly reducing time and bandwidth requirements. Instead of sending a package across the wire for each device, only one transfer is made for each subnet.

Note: Before using multicasting, make sure the multicasting components are in place on the subnet you're distributing to. Multicasting requires LANDesk Management Suite 6.62 or later agents and a LANDesk Management Suite 6.62 or later multicast domain representative.

- **Image uses SysPrep:** Indicates that you used Microsoft Sysprep to configure the OS image to be deployed. Selecting this option allows you to specify Sysprep file information and deployment options later in the wizard.

- **Include profile migration:** Integrates both profile capture and restore processes as part of the image deployment job. Selecting this option allows you to specify profile migration options later in the wizard.
- **Continue with file capture errors:** Allows capture to continue, even if there are errors during the capture.

Note: You can enter only one set of credentials that will be used to access both shares, so the shares must have matching credentials. The credentials must belong to a local user account on the device hosting the share.

- **Domain and user name:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password/Confirm password:** Enter and confirm the user's password.

About the deploy image dialog: Multicast discovery page

Use this page to configure the following basic LANDesk Targeted Multicast options for an image deployment script:

- **Use Multicast domain discovery:** Searches for multicast domain representatives on subnets of your network prior to using Targeted Multicasting to deploy the image to devices across the network.
- **Use Multicast domain discovery and save results:** Searches for multicast domain representatives on subnets of your network prior to deploying the image, and saves the resulting data to help facilitate future Targeted Multicasting deployments.

Only one discovery's results are saved at a time, so selecting this option for an image deployment script will replace the results of the previous discovery.

- **Use results of last Multicast domain discovery:** Uses the most recent list of discovered multicast domain representatives when deploying the image to devices.

Note: Select this option ONLY if you've already saved the resulting data of a multicast domain representative discovery at least once.

- **Configure advanced Multicast options:** Allows you to further customize Targeted Multicasting behavior for a deployment script by configuring advanced Multicast options on the next page of the wizard.
- **Domain representatives can wake up managed devices:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the Multicast Options dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Number of seconds to wait for Wake on LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About the deploy image dialog: Advanced options page

Use this page to configure the following advanced LANDesk Targeted Multicast options for an image deployment script:

- **Maximum number of Multicast Domain Representatives working simultaneously:** Controls the maximum number of multicast domain representatives that can actively deploy an image via Targeted Multicasting at the same time.
- **Number of days files stay in the managed device cache:** Controls the amount of time the image file being multicast can reside in the local cache on each target device. After this period of time, the file will be automatically purged.
- **Number of days files stay in the multicast domain representative cache:** Controls the amount of time the image file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions:** Controls the minimum amount of time to wait between sending out multicast packets. This value is only used when the multicast domain representative is not multicasting a file from its own cache. You can use this parameter to limit bandwidth usage across the WAN.

Note: If this parameter is not specified, then the default minimum sleep time stored on the subnet's multicast domain representative will be used.

- **Maximum number of milliseconds between packet transmissions:** Controls the maximum amount of time to wait between sending out multicast packets.

About the deploy image dialog: Image information page

This page also appears in the capture image dialog. Use this page to specify the type of image you want to restore with this script, where the image is stored, and where the imaging tool is located:

- **Select the image type:** Identifies the file type (format) of the existing image file you want to deploy with this script, selected from the list of imaging tools.
- **Enter the UNC path to the desired image...:** Locates the server and share where the image file is stored, including the image filename. The image must be stored on a share accessible to devices.
- **Enter the UNC path to the imaging application...:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename.
- **Deploy image to this partition:** (Windows PE images only.) Lets you choose the partition on the managed device that you want the image deployed to. The partition you select becomes the C: drive.

Related topics

- Creating imaging scripts with the OS deployment/Migration tasks wizard
- OS deployment overview

- Profile migration overview

About the deploy image dialog: Tool additional commands page

If you're using Powerquest as your imaging tool, you can add additional Powerquest commands on this page. The page is dimmed if you didn't select Powerquest as your imaging tool.

About the deploy image dialog: Pre-boot commands page

Use this page to customize the script by adding custom commands.

- **Enter commands to run before the device is rebooted and imaged:** You can add commands in this text box, one per line, as if you were typing at a command prompt. Commands are sent to devices one at a time. These commands are run before the device is rebooted and imaged.

About the deploy image dialog: SYSPREP.INF page

Use this page to provide the following information about the Sysprep file (SYSPREP.INF) used by this script to modify the image being deployed:

- **Use existing SYSPREP.INF file as a template:** Uses an existing SYSPREP.INF file as a template for a new file and indicates where the existing file is stored. The new SYSPREP.INF file, containing the settings you specify in this wizard, overwrites the existing default Sysprep file. If you want OSD to base its SYSPREP.INF file on one you've already created, you can browse for that file. If you don't select an existing SYSPREP.INF, OSD creates a new one.

Note: After you finish the wizard, you can edit the SYSPREP.INF associated with a script by right-clicking that script and clicking **Advanced Edit**.

- **Location of SYSPREP.INF in the image being deployed:** Locates where the SYSPREP.INF file was stored on the hard drive of the device where Sysprep was originally run. In other words, the device whose image is being deployed by this script.
- **SYSPREP.INF multiprocessor image support - Configure advanced multiprocessor options:** Allows you to configure an image to support multiprocessors (on Windows 2000 or Windows XP devices).

Note: Only select this option if the processor count within your image is different than the processor count on any of your target devices.

About the deploy image dialog: Multiprocessors page

Use this page to configure the following multiprocessor settings for the image being deployed by this script:

- **Choose the operating system type for the image being deployed:** Specifies the OS that is part of the image being deployed, either Windows 2000 or Windows XP.
- **Specify the device type the image was created on:** Indicates whether the image being deployed was created on a uniprocessor or multiprocessor device, with either the APIC or MPS architecture.
- **Enter the location of the HAL-related .INF files inside your image:** Specifies the path to the HAL-related .INF file for the image being deployed by this script. By default, the wizard uses Microsoft's default .INF file paths for each OS. If you used the default paths when setting up your device for imaging, leave the information in this text box as is. Otherwise, type in the different path you used to the HAL-related .INF file.

Additional multiprocessor information

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP kernels. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's Sysprep documentation for more details.

WARNING: As a general rule when considering sharing uniprocessor and multiprocessor images, remember that both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.

Related topics

- OS image guidelines
- OS deployment overview

About the deploy image dialog: Image settings page

Use this page to specify the following generic settings for the SYSPREP.INF file used by this script to modify the image being deployed:

- **Time zone:** Indicates the time zone where the target devices are located.
- **Volume license key:** Specifies the license number for the OS that is being deployed.

- **Local administrator password for this image:** Provides the administrator's password for the device that was imaged.
- **Name:** Identifies the target devices with a name, such as a department name or geographic location.
- **Organization:** Identifies your organization with a name, such as a division or company name.

About the deploy image dialog: Network credentials page

Use this page to specify the following network settings you want to include in the SYSPREP.INF file for this image:

- **Workgroup:** Indicates that your target devices reside in a workgroup. If you select this option, enter the name of the workgroup in the text box.
- **Domain:** Indicates that your target devices reside in a domain. If you select this option, enter the name of the domain in the text box and provide the following domain account information:
 - **Domain username:** Identifies the name of a user in the domain that has privileges to add a machine account to the domain.
 - **Domain password:** Provides the user's password.
 - **Add device to an Active Directory OU:** Allows you to specify the path (using LDAP path syntax) to a specific Microsoft Active Directory OU where you want to add the target devices being imaged.

About the deploy image dialog: Naming convention page

Use this page to assign the naming convention for target devices that will be imaged by the image deployment script:

- **First attempt to get and use existing computer names from the Inventory database:** Preserves existing Windows computer names if the targeted devices have already had the inventory scanner run on them. The image will attempt to use any computer names that already exist in the core database.
- **When necessary, use the following template to name target computers:** Provides a template that defines a naming convention to create unique names for target devices that do not currently have a device name assigned to them in the core database. This template is useful for LANDesk agent-discovered and PXE-booted devices. You can review the examples on the wizard page.

About the deploy image dialog: LANDesk agent page

Use this page to provide the following information needed by the image to install LANDesk device software onto target devices:

- **UNC path to directory containing WSCFG32.EXE:** Specifies the UNC path (usually \\<corename>\LDLogon) to the core server or service center where WSCFG32.EXE (the LANDesk device setup file) resides.
- **LANDesk credentials to access core servers:** Provides a domain\username, password, and confirmed password to authenticate to the core server or service center, so that the image can install WSCFG32.EXE onto target devices.

About the deploy image dialog: Collections page

This page also appears in the capture profile dialog. Use this page to select a collection of rules for the profile migration script and to access the Collection Manager dialog. A collection determines the profile content to be migrated (captured or restored) by the migration script:

- **Available collections:** Lists all of the available collections on your core server. A collection is a user-defined set of rules, each rule identifying a specific application, desktop setting, or file that can be migrated. When you highlight a collection in the list, a description of that collection appears in the message box below.

Note: You can select only one collection for each migration script. However, you can create and modify as many collections as you like, using different combinations of application, desktop, and file rules.

- **Manage:** Accesses the Collection Manager dialog, where you can create and edit collections and file rules and create user-initiated migration packages.

About the Collection Manager dialog

Use this dialog to create, edit, or delete collections of rules, as well as specific file rules. You can also use this dialog to create or delete user-initiated profile migration packages:

(You can access the Collection Manager dialog from either the OS deployment/Migration tasks script wizard, or directly from the Manage Scripts toolbar in the console).

- **File rules:** Displays all available file rules in the list box. You can create a new file rule or edit an existing one.

Note: When you delete a file rule, the rule is removed from the core server. Any collection that contained that rule provides a notice about this change the next time you open or edit the collection.

- **Collections:** Displays all available collections in the list box. You can create a new collection or edit an existing one.

Note: When you delete a collection, the collection is removed from the core server. Any migration script referencing that collection will not run properly. You should also delete the script.

- **User-Initiated packages:** Displays all available packages in the list box. You can create a new migration package, which is a self-extracting executable file that can be run on individual devices. You can't edit an existing user-initiated package.

Note: When you delete a user-initiated package, the package is removed from the core server. Other copies of the package may still exist depending on how and where you distributed the package to users.

About the File Rule dialog

Use this dialog to create new file rules or edit existing ones (in the Collection Manager dialog, click **File rules** and then click **New**).

A file rule determines which files are migrated, based on the following criteria: drive and directory location, subdirectories, file naming (including wildcard support), and destination location.

- **Rule name:** Identifies the file rule with a unique name. If you enter the name of an existing file rule, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the file rule.
- **Rule description:** (Optional) Helps you remember the file rule.
- **Source directory:** Specifies the drive and directory path to the location of the files you want to migrate.

Note on disk partitions: You can migrate files from a device's fixed drives, including disk partitions. Removable media, such as CD-ROM drives, and network shares are not supported. If the target device does not have a matching disk partition drive letter, a new directory named "Migrated_[drive letter]_Drive" is created at the root of the target device's C drive, and the files (along with their associated directory structure) are migrated to that new directory on the target device.

- **Include subdirectories:** Searches for files in all subdirectories of the specified source directory.
- **Remap destination directory:** Moves files to a path on the target device that is different than the source directory path. A file's associated directory structure will still be preserved under the remapped path.
- **Destination directory:** Specifies the drive and directory path on the target device where you want to migrate files that match the location and naming criteria.
- **Files to include:** Captures files in the specified source directory that match the filename syntax you enter here. You can use exact filenames to limit the inclusion to an individual file. You can also use wildcard naming syntax (* and ?) to include files by file type/extension (i.e., *.txt), prefix (i.e., myname*.*), or any other valid wildcard usage.

Note: Separate multiple filenames with a semi-colon character (;) .

- **Files to exclude:** Does not capture files in the specified source directory that match the filename syntax you enter here. You can use exact filenames to limit the exclusion to an individual file. You can also use wildcard naming syntax (* and ?) to exclude files by file type/extension (i.e., *.txt), prefixes (i.e., myname*.*), or any other valid wildcard usage.

Note: If the include control and the exclude control contradict each other, the exclude control takes precedence and the file(s) will not be captured by the file rule.

About the Collection of Rules dialog

Use this dialog to create new collections and edit existing ones (in the Collection Manager dialog, click **Collections** and then click **New**).

A collection is a user-defined set of application, desktop and file rules, that determines the profile content to be migrated.

- **Collection name:** Identifies the collection with a unique name. If you enter the name of an existing collection, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the collection.
- **Description:** (Optional) Helps you remember the collection. The description you enter here will display in both the Collection Manager dialog and the Selecting a collection page of the wizard to help you identify the collection.
- **Rules:** Indicates the profile content you want migrated by this collection. Use the plus-sign and minus-sign boxes to expand and collapse the tree structure to view all of the Applications, Desktop Settings, and File Rules. You can select any combination of the rules available in the Rules tree listing when defining a collection.

About the Capture profile dialog: Storage UNC page

The options on this page also appear in the deploy image and restore profile dialogs' **Profile storage** page. Use this page to specify where to store the profile data and to provide authentication credentials:

- **UNC path to profile storage directory:** Specifies the UNC path to where the profile data will be stored. You can enter just the computer name in UNC format, then browse for the remainder of the path by clicking the Browse button.
- **Domain and user name:** Identifies a user with valid authentication credentials to the specified UNC path.
- **Password/Confirm password:** Specifies the user's password.
- **Force authentication using these credentials:** Forces an authentication (log out and log in using the credentials specified above) on devices that are scheduled for a profile migration IF the currently logged in user's credentials fail. If such a failure occurs, checking this option ensures that the device has sufficient rights to access and save data on the network share where the profile data will be stored.
- **Default local user account(s) password:** (Only available in the deploy image dialog) Provides a password that will become the common default password for all of the *new* migrated local user accounts created on the target device. If a user account already exists, settings are migrated, but the current password is preserved and should be used to log in.
Note: If you leave this text box empty, the password is automatically set to the default: password.

About the User-Initiated Package dialog

Use this dialog to create a self-extracting executable file that can be run on devices as a user-initiated profile migration (in the Collection Manager dialog, click **User-initiated packages** and then click **New**).

Note: User-initiated migration packages can be run on LANDesk-managed devices, as well as computers that are not managed by the LANDesk agents.

- **Package name:** Identifies the user-initiated profile migration package with a unique name. If you enter the name of an existing profile migration package, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the user-initiated package.

Note: Do not type the filename extension here; the .EXE extension will be appended automatically to the name you enter.

- **Rule collection:** Lists all of the of available rule collections. The collection you select determines the content of the user-initiated profile migration. You can select only one collection per migration package.

Note: The user-initiated migration package (*.EXE) is saved by default to the following directory on your core server:
c:\Program Files\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables

Related topics

- [Creating user-initiated profile migration packages](#)
- [Running user-initiated profile migration packages](#)
- [Creating a collection](#)
- [Profile migration overview](#)
- [Profile content](#)

About the DOS task script editor: General page

Use this page to create a script that runs DOS commands (including application executable names) on target devices. The commands are sent to devices one at a time.

- **Name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Description:** Additional text you can add to describe the script.
- **Enter the DOS commands to execute on this device:** DOS commands can be added to this box, one per line, as if you were typing at a DOS command prompt. You can enter as many commands as you like.
- **Abort this job if any command fails:** Causes the imaging job to abort if any of the DOS commands entered on this page fail. Applications (launched from the DOS command line) that generate a DOS errorlevel code when failing will also cause the imaging job to abort. If no errorlevel code is created when a command or application fails, the imaging job will continue.

Validating the OS deployment boot environments

The Linux PE boot environment is the only environment OS deployment supports that doesn't require additional validation. Before you can use the DOS or Windows PE* boot environments, OS deployment has to verify you have a license to use the files that the boot environment requires.

- DOS: License verification requires a Windows NT 4 server CD and a Windows 98 CD. This 7 MB image is the smallest one, reducing the network bandwidth used. It potentially is the slowest at creating and restoring images, and has lower hardware compatibility than the other imaging solutions.
- Windows PE: License verification requires a Windows PE 2005 CD and a Windows 2003 SP1 CD. This 120 MB image is the largest one. It has the best hardware compatibility and is potentially the fastest at creating and restoring images. The imaging speed benefits from 32-bit drivers and applications. This imaging environment also supports Microsoft's imaging tools.

*This product contains Windows software licensed from Microsoft Corporation and/or Microsoft Affiliate(s).

Adding additional drivers to the Windows PE image

If you have hardware on your devices that isn't supported by the standard Windows PE image, you can add drivers to the image. This dialog supports two main types of drivers:

- OEM storage drivers that include a txtsetup.oem file.
- Non-OEM drivers that include a .inf file.

To add drivers to the Windows PE image

1. In the **Operating System Deployment** pane, click the **Add additional drivers into the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Click the type of driver you're installing and click **Next**.
4. Browse for the drivers .inf or txtsetup.oem file and associated files. Click **Next**.
5. Enter the amount of space you want to leave in the Windows PE image after resizing it.
6. Click **Next** when done.

Resizing the Windows PE image

If necessary, you can add space to a Windows PE image.

To add space to a Windows PE image

1. In the **Operating System Deployment** pane, click the **Resize the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Enter the amount of space you want to leave in the Windows PE image after resizing it. You can enter a negative number to reduce the image size.

4. Click **OK** when done.

Changing the Windows PE image wallpaper

If necessary, you can change the Windows PE image wallpaper.

To add space to a Windows PE image

1. In the **Operating System Deployment** pane, click the **Change the wallpaper of the Windows PE image** toolbar button.
2. Browse for the Windows PE image file you want to update.
3. Browse for the wallpaper file you want to use. For best results, use a 24-bit 800x600 bitmap file.
4. Click **OK** when done.

Reports help

About the Report Properties dialog

Use this dialog to configure your report. For more information, see "Creating custom reports" on page 129.

- **Title:** Specifies the title of the report.
- **Description:** Provides a description of the report.
- **Query filter:** Specifies the query applied to the report.
- **Select:** Enables you to select an existing query, which provides the parameters for generating the report.
- **Edit:** Enables you to edit the query of the report.
- **New:** Enables you to create a custom query.
- **Chart type:** Specifies whether the report will include charting diagrams and information, as well as what type of chart to use.
- **Query field:** Specifies the parameter or query data that the chart will be based on.
- **Preview:** Generates and launches a preview of the report.
- **Design:** Launches the report designer, which enables you to customize your report and create report templates.
- **OK:** Saves the report and closes the dialog.
- **Cancel:** Closes the dialog without saving any changes.
- **Help:** Launches the help file.

About the Report published dialog

Use this dialog to perform the following tasks:

- **Report successfully published to:** Identifies the full path and file name of the published report. This is the network path of the file share that can be sent to viewers along with the LANDesk Report users name and password, in order to provide access to the published report. This field can't be edited.

- **Preview:** Opens the report in the appropriate application. An .HTML report opens in the default browser. If you don't have the appropriate application installed to access the file format, you can't preview the report from this dialog. For example, if the report is saved as a PDF file, you won't be able to preview the report without a PDF viewer like Adobe* Acrobat installed.
- **Copy path to clipboard:** Copies the full path and file name to the system clipboard for later pasting.
- **Close:** Closes the dialog.
- **Help:** Launches the help file.

About the Scheduled task - properties dialog

Use this dialog to select an owner for the task, schedule the publishing of the report, designate the destination of the report, and configure the SMTP server. For more information, see "Scheduling to publish a report" on page 127.

Overview

Use this page to specify the owner of the task and to change the scheduled time of the task. This page summarizes the choices you've made in the dialog. If you want to modify any of your choices, click **Change** beside that choice.

- **Owner:** Specifies the owner of the task.
- **Show in common tasks:** Check this option if you want the task should show in the owner's common tasks folder.
- **Scheduled time:** Provides the schedule information of the task.
- **Change:** Takes you to the **Schedule task** page to reschedule the task.

Schedule task

Use this page to schedule the task. You can configure when the task runs and how retries should work.

- **Start time:** Specifies when to perform the task.
- **Leave unscheduled:** Leaves the task unscheduled, but retains the task.
- **Start now:** Initiates the task once the dialog is closed.
- **Start later:** Specifies the task to occur at a designated date and time.
 - **Date:** Specifies the date the task will occur.
 - **Time:** Specifies the time the task will occur.
- **Repeat every:** Check this option to specify the reoccurrence of the task based on the start time.

Recipients

Use this page to select the recipients of the report.

- **Name:** Check these options to specify where the report will be delivered.
- **Destination:** Provides the file path or e-mail address for where the report is delivered.
- **Reply e-mail:** Specifies a sender for e-mailed reports, which is the account that will receive reply e-mails.

- **Check all:** Selects all destinations.
- **Clear all:** Clears the selection of all destinations.

SMTP configuration

Use this page to configure the SMTP server.

- **Outgoing mail server (SMTP):** Specifies the SMTP server. Leaving <localhost> as your selection uses the default SMTP service on your core server.
- **Port number:** Specifies the port number for sending e-mail. The default port is 25.
- **This server requires a secure connection (SSL):** Check this option to specify if your SMTP server requires SSL.
- **My outgoing server (SMTP requires authentication):** Check this option to specify if your SMTP server requires authentication.
- **Log on using NTLM authentication:** Specifies if your server uses NTLM for authentication.
- **Log on using:** Specifies whether your server uses a user name and password for authentication.
 - **User name:** Provides the user name for authenticating to the SMTP server.
 - **Password:** Provides the password for authenticating to the SMTP server.
- **Test e-mail:** Specifies an e-mail address that will receive a message verifying the SMTP server is set up correctly.
- **Test:** Sends the test e-mail to verify proper setup.

About the Report template properties dialog

Use this dialog to create a new report template. For more information, see "Creating a report template" on page 133.

- **Title:** Enter a unique title for the report template.
- **Description:** Enter a description for the report template.

About the Report template dialog

Use this dialog to apply a report template. For more information, see "Applying a report template" on page 133.

- **Report templates:** Lists the report templates that have been created.
- **Load:** Loads the selected report template and closes the dialog.
- **Delete:** Deletes the selected report template.
- **Rename:** Renames the selected report template.
- **Close:** Closes the dialog without applying any template.
- **Help:** Launches the help file.

About the New CSV report dialog

Use this dialog to create a .CSV report. For more information, see "Creating .CSV files" on page 134.

- **File Name:** Enter a unique file name at the end of the existing path. If the directory path does not exist, you're prompted whether you want to create it.
- **Browse:** Enables you to browse to a file location.
- **Report on all devices:** Specifies the report to run on all devices, or only on currently selected devices in the network view.
- **Report on selected nodes:** Specifies the report to run on selected devices in the network view.
- **Current codepage encoding:** Causes the current codepage encoding to be used.
- **Unicode encoding:** Causes unicode encoding to be used
- **OK:** Saves the report and closes the dialog.
- **Cancel:** Closes the dialog without saving the report.
- **Help:** Launches the help file.

About the Select Items dialog

This dialog enables you to specify your reporting criteria, which determines what information will be included in the report. By configuring these reporting parameters and narrowing your focus, you are able to produce more precise reports. In order to apply your reporting criteria, make your desired selections and click **OK**. For more information, see "Reports" on page 123.

Role-based administration help

About the user properties dialog

Use this dialog to specify the selected user's rights, e-mail address, and scope. You can also see what groups or organizational units (OUs) the user is a member of. For more information, see "Role-based administration" on page 59.

Rights

Use this page to specify the user's rights. For more information, see "Understanding rights" on page 66.

- **Assigned rights:** Specifies the rights of the user.

Member of

Use this page to see what groups or OUs the user is a member of. **Member of:** Specifies the groups the selected user belongs to.

Scopes

Use this page to specify the user's scope. For more information, see "Creating scopes" on page 404.

- **Assigned scopes:** Specifies the scopes the user is assigned to.

- **Add:** Enables you to add the user to additional scopes.
- **Remove:** Removes the selected scope from the user, so the user is no longer assigned to that scope.
- **New:** Enables you to create a scope.
- **Edit:** Enables you to edit the selected scope.

User

Use this page to specify the user's email address. For more information, see "E-mailing reports" on page 128.

- **E-mail:** Specifies the user's e-mail address.

Asset access

Use this page to assign an asset access filter to the user. (**Note:** This page is visible only if the logged in user has administrator rights and if LANDesk Asset Manager add-on has been installed.)

Filters are based on the global list types defined in Asset Manager. You can restrict access to asset information by first creating a global list filter in Asset Manager and then assigning a detail from that global list type to the user so that they will see only those assets that match.

About the Remote control settings dialog

Use the Remote control settings dialog to provide more specific rights to the remote control right, such as actions a remote control user can execute and the days and/or times the user can execute these rights. These settings are only enforced when managed devices use the integrated security model or the certificate-based security model. You can set the remote control security model in the remote control agent configuration pages.

To use the remote control settings dialog

1. In the **User rights/Scopes** dialog, click **Remote control settings**. If this button is dimmed, you must click the Remote control tools right
2. In the **Remote control rights** tab, click the rights you want the remote control right to allow.
3. In the **Time** tab, click **User time settings**, click the days of the week you want the right to be active, and select a time range you want the right to be active. If you select the same time for both the **From** and **To** time range, the right will be active for the entire 24 hours of the selected days (as defined by the database server's clock).
4. Click **OK**.
 - **Remote control:** Lets the user view a remote device's desktop and control the keyboard and mouse.
 - **View:** Lets the user view a remote device's desktop without the ability to execute any actions on it.
 - **Execute program:** Lets the user start any program on a remote device to diagnose issues.

- **File transfer:** Lets the user transfer files to and from the source device and the remote device.
- **Chat:** Lets the user remotely chat with a remote device.
- **Reboot machine:** Lets the user remotely reboot a device.

All remote control time ranges are based on the database server's clock. If a remote control operator is in a different time zone than the database server, you need to adjust the time settings for that operator's account so they are based on the database server's clock, not the operator's local clock.

About the group and OU Properties dialog

Use this dialog to specify the rights of the selected group or organizational unit (OU). You can also see what other groups or OUs it is a member of. For more information, see "Role-based administration" on page 59.

Rights

Use this page to specify the rights of the group or OU. For more information, see "Understanding rights" on page 66.

- **Assigned rights:** Specifies the rights of the group or OU.

Member of

Use this page to see what groups or OUs the selected group or OU is a member of.

- **Member of:** Specifies the groups or OUs the selected group belongs to.

About the Scope Properties dialog

Use this dialog to configure the scope's properties. For more information, see "Creating scopes" on page 404.

- **Scope name:** Specifies the name of the scope.
- **Select a scope type:** Specifies what the scope applies to. The scope type determines what definitions can be applied to the scope.
- **New:** Enables you to create a scope definition based on the selected scope type.
- **Definition:** Displays the parameters that determine what the scope applies to.
- **Device group filters:** Lists any filters that affect the scope.
- **Edit:** Enables you to edit the scope's definition.

About the Login to Active Directory dialog

Use this dialog to access your active directory, so you can add groups and organization units (OUs) to the application. Then you'll be able to assign them rights and add them to other groups.

- **LDAP:** Specifies the path to the LDAP directory in order to access the groups and OUs (see "Using active directories" on page 64).
- **User name:** Specifies the user name to authenticate to the server.
- **Password:** Specifies the password to authenticate to the server.

About the Available Active Directory Groups and OUs dialog

Use this dialog to add groups and organizational units (OUs) to your **Active Directory** folder. These groups can be assigned rights and added to other groups. When users become a member of a group or OU, they inherit the rights of the parent node in addition to their own. A user's individual rights may allow access to functionality beyond the rights granted by the group or OU. Otherwise, they'll assume the same rights as the group or OU they belong to.

Scheduled tasks help

About the Schedule task dialog

Access this dialog from the **Scheduled tasks** window (**Tools | Distribution | Scheduled tasks**). In the **Scheduled tasks** window, click the **Create software distribution task** toolbar button, or from the shortcut menu of the task you want to configure, click **Properties**.

Use this dialog to set the start time for the task and whether to make it a recurring task and how often. This dialog also shows the task targets. Depending on the task type you're scheduling, you may also see options for delivery methods and distribution packages.

About task copying

You can also create groups for your common tasks to categorize them. Other users will see groups only if their RBA scope allows them to see a task in that group. If you try deleting a group that contains tasks, you won't be able to delete the group if there are tasks in the group that your scope doesn't allow you to see.

About the Overview page

This page lets you pick an owner for the task and summarizes the choices you've made in the Scheduled tasks dialog. If you want to modify any of your choices, click **Change** beside that choice. If you want the task to appear in the **Scheduled tasks** window's **Common tasks** group, rather than the **My tasks** group, click **Show in common tasks**.

About the Distribution package page

Use this page to select the distribution package you want to deliver. Once you select a **Package type**, the **Distribution package** list shows the packages of that type that you can distribute. The packages in the list correspond to the packages you can see under that type in the **Distribution packages** window for the current user and the public user. Click the **Distribution package** you want.

Push-based software distribution tasks can include a preliminary package and a final package. When using multiple packages, the packages are installed in order one at a time. The previous package must return a successful task status before the next package begins installing. For more information, see "Using multiple distribution packages in a task" on page 172.

About the Delivery method page

Use this page to select the delivery method to use for the package you're delivering. Once you select a **Delivery type**, the **Delivery methods** list shows the delivery methods of that type that you can use. The delivery methods in the list correspond to the delivery methods you can see in the **Delivery methods** window for the current user and the public user. Click the **Delivery method** you want.

About the Target devices page

Use this page to view target devices for the task you're configuring. You can't add targets on this page. You can add targets later by dragging and dropping them into the task in the **Scheduled tasks** window. Targeted devices can be in these categories:

- Targeted devices
- Targeted LDAP objects
- Targeted queries
- Targeted LDAP queries
- Targeted device groups

You can also check the **Wake up devices** option on this page. This option wakes up a powered-down computer for the selected task by using Wake On LAN. When the task is complete, the computer shuts itself down again. This feature only works on computers with BIOS versions that support Wake on LAN technology. Selecting this option will make tasks take longer, since the task waits for devices that just woke up to boot. Don't mark this option for pull distribution packages.

About the Schedule task page

Use this page to configure when the task runs and how retries should work:

- **Leave unscheduled:** Adds the task to the Scheduled tasks window but doesn't schedule the task. Use this option if you want to preserve a task configuration but you don't want it to run.
- **Start now:** Starts the task as soon as the dialog is closed. There can be a delay of up to a minute before the task actually starts.

- **Start later:** Starts the task at the specified time and date.
- **Time:** Starts a task at the selected time. By default, this field displays the current time.
- **Date and time:** Runs a task on selected date. Type the date using MM/DD/YY format, or click the drop-down list to pick the date off a calendar.
- **Repeat every:** Schedules the task to recur periodically. Select Day, Week, or Month from the drop-down list to choose how often the task repeats. It repeats at the time set above.
- **Schedule these devices:** For the first time a task runs, you should leave the default of **Schedule these devices**. For subsequent runs, choose from **All**, **Devices that did not succeed**, or **Devices that did not try to run the task**. These options are explained in more detail below.

When rescheduling a task, you can limit the devices the task runs on. You may want to do this if the task failed on a large number of devices and you don't expect the failed device state to change, for example. Limiting the task this way would help the task complete more quickly because the scheduler wouldn't keep trying devices that won't process the task. You can choose to run tasks on devices in these states:

- **Waiting or currently working:** This is the default and should be used the first time a task runs. If you're rerunning the task, this option targets devices that succeeded the previous time you ran the task.
- **All:** Select this if you want the task to run on all devices, regardless of state. Consider using this option if you have a task, especially a repeating one, that needs to run on as many devices as possible.
- **Devices that didn't succeed:** Select this if you only want the task to run on all devices that didn't complete the task the first time. This excludes devices that have a **Successful** state. The task will run on devices in all other states, including **Waiting** or **Active**. Consider using this option if you need the task to run on as many unsuccessful devices as possible, but you only need the task to complete successfully once per device.
- **Devices that didn't try to run the task:** Select this if you only want the task to run on devices that didn't complete the task and didn't fail the task. This excludes devices that were in an **Off**, **Busy**, **Failed**, or **Canceled** state. Consider using this option if there were a lot of target devices that failed the task that aren't important as targets.

About the Schedule dialog

Several Management Suite agents have features that you can schedule using the local scheduler agent that is installed on managed devices. Use this dialog to configure that schedule.

You can also use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script or customize the schedule for a device agent, you can deploy it to devices by using the **Scheduled tasks** window.

To configure a local scheduler task, in the **Managed scripts** window (**Tools | Distribution | Managed scripts**), from the **My scripts** shortcut menu, click **New local scheduler script**.

All criteria in this dialog that you configure must be met before the task will execute. For example, if you configure a schedule that repeats every day between 8 and 9 o'clock with a **Machine state** of **Desktop must be locked**, the task will only execute if it's between 8 and 9 o'clock AND the machine is locked.

These options are available in the **Schedule** dialog:

The Schedule dialog's "Events" section

The events section is dimmed unless you're configuring a local scheduler script from the **Manage scripts** tool.

- **Run when user logs in:** Check this option to run the task whenever a user logs in. When a user logs in, the local scheduler will run the task directly.
- **Run whenever the machine's IP address changes:** Check this option if you want the task to run if the device's IP address changes or is renewed through DHCP. For example, you can use this option to trigger an inventory scan when the IP address changes, keeping the IP address in the Management Suite database synchronized.

The Schedule dialog's "Time" section

Use this section to configure times for the task to run. If you launched this dialog from the agent configuration tool, you can specify a random delay on the agent configuration page you came from. The random delay interval you specify is a time range during which the task may run. For example, if you have a large number of users who log in at the same time, this delay allows tasks that run on login to not all run at the same time, assuming your delay interval is long enough. The default delay is one hour.

- **Start:** Click this option to display a calendar where you can select the day you want the task to start. Once you pick a day, you can also enter a time of day. These options default to the current date and time.
- **Repeat after:** If you want the task to recur, click the list box and select **minutes**, **hours**, or **days**. Then in the first box enter the length you want for the interval you selected. For example, 10 days.
- **Time range:** If you want the task to run between certain hours, select the start and end hours. The hours are in 24-hour (military) time format.
- **Weekly between:** If you want the task to run between certain days of the week, select the start and end days.
- **Monthly between:** If you want the task to run between certain dates of the month, set the start and end dates .

The Schedule dialog's "Run filters" section

When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute.

When specifying bandwidth criteria for devices that may be connecting to the core through a LANDesk Management Gateway, you should put the Management Gateway's IP address in the **to** field. This allows the bandwidth test to complete and the task can then execute.

You can select these **Minimum bandwidth** options:

- **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
- **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
- **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools | Configuration | Agent Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.

The run filters section has these options:

- **Minimum bandwidth:** If you want task execution criteria to include available bandwidth, select the minimum bandwidth you want and enter the device name or IP address that will be the target for the bandwidth test between the target and device.
- **Machine state:** If you want the task execution criteria to include a machine state, select one of these states: **Screen saver or desktop locked**, **Desktop must be locked**, **Machine must be idle**, **User must be logged in**, or **User must be logged out**. The criteria for the **Machine must be idle** state are: the OS is locked, the screen saver is active, or the user is logged out.

The Schedule dialog's other options

- **Additional random delay once all other filters pass:** If you want an additional random delay, use this option. If you select a random delay that extends beyond the time limits you configured for the task, the task may not run if the random value puts the task outside the configured time limits.
- **Delay up to:** Select additional random delay you want.
- **And at least:** If you want the task to wait at least a certain number of minutes before executing, select this option. For example, if you're scheduling an inventory scan, you could enter a five here so a computer has time to finish booting before the scan starts, improving the computer's responsiveness for the user.
- **Command:** Enter the program you want to run locally. Include the full path to the program or make sure the program is in a folder that's in the device's path. This path must be the same on all devices you deploy this script to.
- **Parameters:** Enter any command-line parameters you want passed to the program.

Security and Patch Manager help

The Security and Patch Manager window (**Tools | Security | Security and Patch Manager**) is where you download and manage security and patch content, configure security tasks such as assessment scanning and remediation, customize and apply security scanner display/interaction settings, and view comprehensive security-related information for scanned devices, among other important security management tasks; all designed to help you protect your LANDesk managed devices from the many prevalent types of security risks and exposures that could harm your network.

The "Security and Patch Manager" on page 315 chapter introduces this security management tool, which is an integral component of both the LANDesk Management Suite and LANDesk Security Suite products. In that chapter you'll find overview and security content subscription information, as well as step-by-step instructions on how to use all of the tool's features. Also included in that chapter is a section describing the interface and functionality of the tool, see "Understanding and using the Security and Patch Manager tool window" on page 321.

As for this chapter, it contains the following online help sections that describe the Security and Patch Manager tool's dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog:

- "About the Manage filters dialog" on page 723
- "About the Filter properties dialog" on page 723
- "About the Download updates dialog" on page 723
- "About the Definition properties dialog" on page 726
- "About the Download associated patches dialog" on page 729
- "About the Detection rule properties dialog" on page 729
- "About the Purge security and patch definitions dialog" on page 737
- "About the Create security scan task dialog" on page 738
- "About the Configure scan and repair (and compliance, and firewall) settings dialog" on page 739
- "About the Scan and repair settings dialog" on page 739
- "About the Security and patch information dialog" on page 745
- "About the Create compliance scan task dialog" on page 746
- "About the Create reboot task dialog" on page 746
- "About the Create repair task dialog" on page 747
- "About the Multicast options dialog" on page 748
- "About the Uninstall patch dialog" on page 749
- "About the Change settings task dialog" on page 749
- "About the Configure custom variable override settings dialog" on page 751
- "About the Custom variable override settings dialog" on page 751
- "About the Alert settings dialog" on page 752
- "About the Rollup core settings dialog" on page 752
- "About the Select columns dialog" on page 753
- "About the Configure firewall settings dialogs" on page 753

About the Manage filters dialog

Use this dialog to manage filters you can use to customize the security and patch content that displays in the Security and Patch Manager window's item list. You can use filters to streamline a lengthy list.

- **New:** Opens the Filter Properties dialog where you can configure a new filter's settings.
- **Edit:** Opens the Filter Properties dialog where you can modify and save the selected filter.
- **Delete:** Removes the selected filter permanently from the database.
- **Use filter:** Applies the selected filter to the current item list. The applied filter persists when you click different groups in the tree view.

About the Filter properties dialog

Use this dialog to create or edit security content list filters. You can filter by operating system, security risk severity, or any combination of both.

- **Filter name:** Identifies the filter by a unique name. This name appears in the Filter drop-down list.
- **Filter operating systems:** Specifies the operating systems whose definitions you want to display in the item lists. Only those items associated with the operating systems you select are displayed.
- **Filter severities:** Specifies the severities whose definitions you want to display in the items lists. Only those items whose severity matches the ones you select are displayed.

About the Download updates dialog

Use this dialog to configure settings for downloading security and patch content updates, proxy server, patch file download location, spyware autofix, and antivirus updates and backups.

After you specify the types of content updates you want to download and the other options on the tabs of the Download updates dialog:

- To perform an immediate download, click **Update Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog. If you click **Close**, you'll be prompted whether you want to save the settings.
- To schedule a download security and patch content task, click **Schedule update** to open the **Scheduled update information** dialog, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks.

To save your changes on any tab of this dialog, click **Apply**.

The **Download updates** dialog contains the following tabs:

- "About the Updates tab" on page 724
- "About the Proxy settings tab" on page 725
- "About the Patch location tab" on page 726
- "About the LANDesk Antivirus tab" on page 726

Security content downloading considerations

Security Suite content subscriptions

A basic LANDesk Management Suite installation allows you to download and scan for LANDesk software updates, and to create and use your own custom definitions. For all other security content types, such as platform-specific vulnerabilities, spyware, etc., you must have a LANDesk Security Suite content subscription in order to download the associated definitions.

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Task-specific settings and global settings

Note that only the definition types, languages, and definition and patch download settings are saved and associated with a specific task when you create it. Those three settings are considered task specific.

However, all of the settings on the other tabs of the Download updates dialog are global, meaning they apply to all subsequent security content download tasks. Global settings include: patch download location, proxy server, spyware autofix, security alerts, and antivirus. Any time you change a global setting it is effective for all security content download tasks from that point on.

About the Updates tab

- **Select update source site:** Specifies the LANDesk Security content server that is accessed to download the latest definitions, detection rules, and associated patches to your database. Select the server nearest your location.
- **Definition types:** Identifies which security and patch content definitions are updated. Only those definition types for which you have a subscription are available. The more definition types you select, the longer the download will take.

After you've downloaded security content, you can use the **Type** drop-down list in the main Security and Patch Manager tool window to determine which definition types are displayed in a list. For information on using the list options, see "Type drop-down list" on page 324. For information on how the security scanner works for each different type, see "How Security and Patch Manager scans for different content types" on page 348.

- **Languages:** Identifies the language versions of the selected definition types that are updated.

Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

When downloading content for any platform (with the appropriate security content subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.

- **Download patches for definitions selected above:** Automatically downloads patch executable files to the specified download location (see Patch Location tab), according to one of the following download options:
 - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).
 - **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerabilities, security threats, and LANDesk software updates currently residing in the Scan group.
- **Enable automatic patch deployment using Process Manager:** Lets you configure the LANDesk Process Manager database that is required for using the integrated automatic patch deployment feature.
- **Configure Process Manager:** Opens the Automating Patch Deployment dialog that describes the integrated capability between LANDesk Process Manager and the Security and Patch Manager tool that allows you to create a workflow to automates patch deployment to target devices on your LANDesk network. You also have the option of viewing a tutorial that steps you through this procedure. LANDesk Process Manager includes online help that you can access any time for detailed information about its features and how to use them.
- **Put new definitions in Unassigned group (unless overridden by definition group settings):** Automatically places new definitions and associated detection rules in the Unassigned group instead of in the default Scan group. Select this option if you want to be able to manually move content in and out of the Scan group in order to customize the security scan. (**Note:** Definitions that are selected to be placed in the Alert group (in the **Configure Alerts** dialog, are automatically placed in the Scan group even if this option is selected). For the blocked application type, definitions are downloaded to the Unassigned group by default, not the Scan group. You don't have to select this option if you're downloading only blocked application definitions
- **Definition group settings:** Opens the Definition group settings dialog where you can create, manage, and select definition groups. You can use definition group settings to automate how security definitions (content) that match specified type and severity criteria are downloaded, their scan status, and the download location.

About the Proxy settings tab

If your network uses a proxy server for external transmissions (such as Internet access), use this tab to enable and configure the proxy server settings. Internet access is required for both updating vulnerability information, and for downloading patch files from appropriate Web services.

- **Use proxy server:** Enables the proxy server option (by default, this option is off). If you enable a proxy server, you must fill in the address and port fields below.
- **Server:**
 - **Address:** Identifies the IP address of your proxy server.
 - **Port:** Identifies the port number of your proxy server.

- **HTTP based Proxy:** Enables the proxy server, if it's an HTTP-based proxy (such as Squid), so that it will successfully connect to and download patches from FTP sites. (Patches hosted at some FTP sites cannot be downloaded through an HTTP-based proxy unless you first enable this option).
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
 - **Username:** Enter a valid username with authentication credentials to the proxy server.
 - **Password:** Enter the user's password.

About the Patch location tab

Use this tab to specify where patch executables are downloaded.

- **UNC path where patches are stored:** Specifies where patch files are downloaded. The default location is the core server's \LDLogon\Patch folder. You can enter a different UNC path to download patches, but you must ensure access to that location by entering valid authentication credentials in the fields below.
- **Credentials to store patches:** Identifies a valid username and password for accessing a location other than the core server. If you're downloading patches to the default location on the core server, the username and password fields are not applicable.
- **Web URL where clients access patches:** Specifies a Web address where devices can access downloaded patches for deployment. The default location is the core server's \LDLogon\Patch folder. This location will normally be the same as the UNC path specified above.
- **Test settings:** Performs a connectivity test to the specified Web URL.
- **Reset to default:** Restores both the UNC path and the Web URL to the default location, which is the core server's \LDLogon\Patch folder.

About the LANDesk Antivirus tab

Use this tab to configure download options for LANDesk Antivirus virus definition files. Keep in mind this tab applies only to actual virus definition files that are used by LANDesk Antivirus; it does not apply to the antivirus scanner detection content (Antivirus updates) that are available in the definition list on the **Updates** tab.

For detailed information, see "About the LANDesk Antivirus tab on the Download updates dialog" on page 649.

About the Definition properties dialog

Use this dialog to view properties for downloaded content definition types, including vulnerabilities, spyware, security threats, software updates, etc. You also use this page to create your own custom definitions.

This information is read-only for downloaded definitions. For custom definitions, the fields on this dialog are editable. You can enter identification, attribute, and detection rule details information for a custom definition by using the available fields on this dialog and on the detection rule properties dialog. For more information, see "Creating custom definitions and detection rules" on page 341.

Use the left and right arrow buttons (<, >) to view the previous or next definition's property information, in the order they are currently listed in the main window.

The Definition properties dialog contains the following tabs:

- "About the Definition: General tab" on page 727
- "About the Definition: Description tab" on page 728
- "About the Definition: Dependencies tab" on page 728
- "About the Definition: Custom Variables tab" on page 728

About the Definition: General tab

- **ID:** Identifies the selected definition with a unique, vendor-defined alphanumeric code (or user-defined in the case of a custom definition).
- **Type:** Identifies the selected item as a vulnerability, security threat, custom definition, etc.
- **Publish Date:** Indicates the date the selected definition was published by the vendor (or created by a user).
- **Title:** Describes the nature or target of the selected definition in a brief text string.
- **Severity:** Indicates the severity level of the definition. For downloaded content, this severity level is assigned by the vendor. For a custom definition, the severity is assigned by whoever created the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown. Use this information to evaluate the risk posed by the definition, and how urgent scanning and remediation are for your network.
- **Status:** Indicates the status of the definition in the Security and Patch Manager window. The three status indicators are: Scan, meaning the selected item is enabled for the next security scan; Don't Scan, meaning it won't be scanned; and Unassigned, meaning it is in a temporary holding area and won't be scanned. For more information about these three states/groups, see "Understanding and using the Security and Patch Manager tool window" on page 321.
- **Language:** Indicates the language of the platform identified by the definition. For custom definitions, INTL is the default value meaning the definition is language independent, and can't be edited.
- **Category:** Indicates a more specific category within an individual security content type (see above).
- **Detection Rules:** Lists the detection rules associated with the selected definition. Note that **Downloaded** indicates whether associated patch files are downloaded to the local repository, and **Silent Install** indicates whether the patch installs without user interaction.

You can right-click a detection rule to download its associated patch (or patches), disable/enable the detection rule for security scanning, uninstall its associated patches, or view its properties. You can also double-click a detection rule to view its properties.

If you're working with a custom definition, click **Add** to create a new detection rule; click **Edit** to modify the selected rule; or click **Delete** to remove the selected rule. For more information on custom definitions, see "To create custom detection rules" on page 342.

About the Definition: Description tab

- **Description:** Provides additional details about the selected definition. This information is provided by vendor research and test notes (or by the user who created the custom definition).
- **More information at:** Provides a HTTP link to a vendor-specific (or user-defined Web page), typically a support site, with more information about the selected definition.
- **More information for CVE ID:** (Applies only to vulnerabilities) Provides the CVE ID (name) for the selected vulnerability, plus a link to the CVE Web page for that specific CVE ID. For more information, see [Using CVE names](#).

About the Definition: Dependencies tab

This tab displays only if the selected definition has an associated prerequisite definition, or if another definition depends on the selected definition before it can run. You can use this tab to make sure your security scan task contains all the definitions necessary to operate properly before scanning devices.

A dependency relationship can exist only for the following security definition types:

- **Prerequisites:** Lists any definitions that have to be run BEFORE the selected definition can be checked for on devices. If any of the definitions in this list aren't included in your scan task, the selected definition won't be detected by the security scanner.
- **Dependencies:** Lists any definitions that won't be detected by the security scanner until AFTER the selected definition is run. Note that the selected definition will be scanned for even if these definitions aren't included in your security scan task. However, if you want your scan task to successfully detect a definition in this list, the selected definition must be run first.

About the Definition: Custom Variables tab

This tab displays ONLY if the selected security definition includes settings or values that can be modified. Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected).

Edit Custom Variables right required

In order to edit custom variable settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Every security definition with customizable variables has a unique set of specific values that can be modified. In each case however, the **Custom Variables** tab will show the following common information:

- **Name:** Identifies the custom variable. The name can't be modified.

- **Value:** Indicates the current value of the custom variable. Unless the variable is read-only, you can double-click this field to change the value.
- **Description:** Provides additional useful information about the custom variable from the definition publisher.
- **Default value:** Provides the default value if you've changed the setting and want to restore it to its original value.

To change a custom variable, double-click the **Value** field, and either select a value if there's an available drop-down list, or manually edit the value, and then click **Apply**. Note that some variables are read-only and can't be edited (this is usually indicated in the description).

Custom variable override setting information can be viewed in the device's Inventory view.

Custom variable override settings

In some situations you may want to ignore a custom variable setting, or in other words create an exception to the rule. You can do this with a feature called custom variable override settings. Custom variable override settings let you decide which custom variables to essentially ignore when scanning devices so that they are not detected as vulnerable and are not remediated even if they meet the actual conditions of a definition's detection rules. You can create as many custom variable override settings as you like, and apply them to devices using a **Change settings** task. For more information, see "About the Custom variable override settings dialog" on page 751.

About the Download associated patches dialog

Use this dialog to download patch executable files that are required to remediate the selected vulnerability but that are not currently available on the core server (or in some other specified patch repository location). Required patches must reside in the designated patch location in order for a managed device with a detected vulnerability to be remediated successfully.

- **Name:** Indicates the name of the patch executable file.
- **Definitions:** Indicates the vulnerability which is associated with this patch file.
- **Downloaded:** Shows whether the patch file has been downloaded or not.
- **Can download:** Indicates whether the patch can be automatically downloaded, or whether it has to be downloaded by a Security and Patch Manager process.
- **Show currently required patches only:** Displays only those patch files that are required to remediate the selected vulnerability at this time. In other words, the list will include patches that have superceded earlier patches, not the earlier patches.
- **Show all associated patches:** Displays a comprehensive listing of all of the associated patches for the selected vulnerability, whether they have been superceded or not.
- **Download:** Click to download the patch files from the update source site.
- **Cancel:** Cancels the download operation.

About the Detection rule properties dialog

Use this dialog to view detection rule properties for downloaded security content, or to create and edit custom detection rules.

This information is read-only for detection rules belonging to downloaded definitions. For custom definitions, the fields on the pages of this dialog are editable. You can specify detection rule settings and configure the options on each page in order to create custom detection rules. Furthermore, if the custom detection rule allows remediation, you can add special commands that run during remediation (patch install or uninstall).

You can use the left and right arrow buttons (<, >) to view property information for the previous or next detection rule in the order they are currently listed in the main window.

The Detection rule properties dialog contains the following pages:

- "About the Detection rule: General information page" on page 730
- "About the Detection logic: Affected platforms page" on page 730
- "About the Detection logic: Affected products page" on page 731
- "About the Detection logic: Files used for detection page" on page 731
- "About the Detection logic: Registry settings used for detection page" on page 732
- "About the Detection logic: Custom script page" on page 732
- "About the Patch information page" on page 734
- "About the Detecting the patch: Files used for installed patch detection page" on page 735
- "About the Detecting the patch: Registry settings used for installed patch detection page" on page 735
- "About the Patch install commands page" on page 735
- "About the Patch uninstall commands page" on page 737

About the Detection rule: General information page

- **Name:** Displays the name of the detection rule.
- **State:** Indicates whether the detection rule is set to scan or not to scan. These two states correspond to the Scan and Don't Scan groups (under Detection Rules in the Security and Patch Manager window).
- **ID:** Shows the ID of the definition associated with this rule.
- **Title:** Shows the title of the definition associated with this rule.
- **Description:** Shows the description of the definition associated with this rule.
- **Comments:** Provides additional information from the vendor, if available. If you're creating or editing a custom definition, you can enter your own comments.

Detection logic pages

The following pages refer to the detection logic used by the selected detection rule to determine whether the vulnerability definition (or other definition type) exists on a scanned device.

About the Detection logic: Affected platforms page

Identifies the operating systems the security and patch scanner will run on to check for this rule's associated definition. In other words, only devices matching the selected platforms will attempt to process this rule. At least one platform **MUST** be selected. If a target device is running a different operating system, the security scanner quits.

About the Detection logic: Affected products page

- **Products:** Lists the products you want to check for with the detection rule to determine whether the associated definition exists on scanned devices.. Select a product in the list to view its name, vendor, and version information. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If none of the specified associated products are found on the device, the security scan quits. However, if no products are specified, the scan proceeds to the files check.

If you're creating or editing a custom detection rule, click **Configure** to open a new dialog that lets you add and remove products in the list. The list of available products is determined by the security and patch content you've updated via the LANDesk Security service.

- **Name:** Provides the name of the selected product.
- **Vendor:** Provides the name of the vendor.
- **Version:** Provides the version number of the selected product.

About the Detection logic: Files used for detection page

- **Files:** Lists the file conditions (existence, version, date, size, etc.) that are used to determine whether the associated definition exists on scanned devices. Select a file in the list to view its verification method and expected parameters. If all the file conditions are met, the device is not affected. Said another way, if any of these file conditions are NOT met, the vulnerability is determined to exist on that device. If there are no file conditions in the list, the scan proceeds to the registry check.
If you're creating or editing a custom detection rule, click **Add** to make the fields editable, allowing you to configure a new file condition and expected values/parameters. A rule can include one or more file conditions, depending on how complex you want to make it. To save a file condition, click **Update**. To delete a file condition from the list, select it and click **Remove**.
- **Verify using:** Indicates the method used to verify whether the prescribed file condition is met on scanned devices. For example, a detection rule can scan for file existence, version, date, size, and so on. The expected parameters that appear below the verification method are determined by the method itself (see the list below).

If you're creating or editing a custom detection rule, select the verification method from the **Verify using** drop-down list. As stated above, the parameter fields are different for each verification method, as described in the following list:

Note that the **Search for file recursively** option applies to all the file verification methods except for the MSI methods, and causes the scan to search for files in the specified path location and any existing subfolders.

- **File Existence Only:** Verifies by scanning for the specified file. Parameters are: Path (location of the file on the hard drive), including the filename, and Requirement (must exist or must not exist).
- **File Version:** Verifies by scanning for the specified file and its version number. Parameters are: Path, Minimum Version, and Requirement (must exist, must not exist, or may exist).

Note that for the File Version, Date, and Size parameters, after specifying the file path and name, you can click the **Gather Data** button to automatically populate the appropriate value fields.

- **File Date:** Verifies by scanning for the specified file and its date. Parameters are: Path, Minimum Date, and Requirement (must exist, must not exist, or may exist).
- **File Size and/or Checksum:** Verifies by scanning for the specified file and its size or checksum value. Parameters are: Path, Checksum, File size, and Requirement (must exist, must not exist, or may exist).
- **MSI Product ID installed:** Verifies by scanning to ensure the specified MSI product is installed (a product installed by the Microsoft Installer utility). Parameters are: Guid (the product's global unique identifier).
- **MSI Product ID NOT installed:** Verifies by scanning to ensure the specified MSI product isn't installed. Parameters are: Guid.

About the Detection logic: Registry settings used for detection page

- **Registry:** Lists the registry key conditions that are used to determine whether the associated vulnerability (or other type) exists on a scanned device. Select a registry key in the list to view its expected parameters. If any of these conditions are NOT met, the vulnerability is determined to exist on that device.

Important: If there are no registry conditions in the list, AND there were no file conditions on the Files tab, the scan fails. In other words, a detection rule must have at least one file or registry condition.

If you're creating or editing a custom detection rule, click **Add** to make the fields editable allowing you to configure a new registry key condition and expected parameters. A rule can include one or more registry conditions. To save a registry condition, click **Update**. To delete a registry condition from the list, select it and click **Remove**.

- **Key:** Identifies the registry key's expected folder and path.
- **Name:** Identifies the expected name of the key.
- **Value:** Identifies the expected value of the key.
- **Requirement:** Indicates whether the registry key must or must not exist on target devices.

About the Detection logic: Custom script page

Use this page if you want to write a custom VB script that checks for any other conditions on scanned devices. The security scanner agent's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.

Click the **Use editor** button to open your default script editing tool, associated with this file type. When you close the tool you're prompted to save your changes in the Custom Script page. If you want to use a different tool you have to change the file type association.

About the custom vulnerability's product properties: General information page

Use these dialogs when creating a custom vulnerability definition that includes a custom product.

You can enter a name, vendor, and version number, and then define the detection logic that determines the conditions for the vulnerability to exist.

These dialogs are similar to the properties dialogs for downloaded published vulnerability definitions. Please see the corresponding sections above.

This page includes the following options:

- **Affected products:** Lists products that are affected by this custom vulnerability definition.
- **Available products:** Lists all downloaded products.
- **Filter available products by affected platforms:** Restricts the list of available products to only those that are associated with the platforms you've selected on the Detection logic: Affected platforms page.
- **Add:** Opens the Properties dialog where you can create a custom product definition.

About the custom vulnerability's product: Detection logic page

The following pages refer to the detection logic used by the selected detection rule to determine whether the vulnerability definition (or other definition type) exists on a scanned device.

These dialogs are similar to the detection logic dialogs for downloaded known OS and application vulnerability definitions published by vendors that are described above. For information about the options, see the corresponding sections above.

About the custom vulnerability's product: Detection logic: Files used for detection page

See the Detection logic: Files used for detection page above.

About the custom vulnerability's product: Detection logic: Registry settings keys used for detection page

See the Detection logic: Registry settings used for detection page above.

About the custom vulnerability's product: Detection logic: Custom detection script page

See the Detection logic: Custom script page above.

About the Patch information page

Use this page to define and configure the rule's associated patch file (if one is required for remediation) and the logic used to detect whether the patch is already installed. You can also configure additional patch file install or uninstall commands for customized remediation.

This page and the ones under it refer to the patch file required to remediate a vulnerability. These pages are applicable only if the selected detection rule allows remediation by deploying a patch file. If the detection rule is limited to scanning only, or if the security content type doesn't use patch files for remediation, as in the case of security threats, or spyware, then these pages are not relevant.

- **Repaired by patch, or detection only:** Click one of these options to specify whether the detection rule will just check for the presence of the associated definition (detect only), or if it can also remediate that definition by deploying and installing the required patch.
- **Patch download information:**
 - **Patch URL:** Displays the full path and file name of the patch file required to remediate the selected definition if detected. This is the location from where the patch file is downloaded.
 - **Auto-downloadable:** Indicates whether the patch file can be automatically downloaded from its hosting server. You can use this option with custom detection rules if you want to prevent patch files from being downloaded via the rule's shortcut menu. For example, you may need to prevent automatic patch download if there's a firewall that blocks access to the hosting server.
 - **Download:** If you're creating or editing a custom detection rule that performs remediation, and you've entered a patch filename and URL, you can click **Download** to attempt to download the patch file at this time. You can download the patch file at a later time if you prefer.
- **Repair information:**
 - **Unique filename:** Identifies the unique executable filename of the patch file. Note that it is strongly recommended that when you download a patch file, you create a hash for the patch file by clicking **Generate MD5 Hash**. (Most, if not all, known vulnerability's associated patch files should have a hash.) The patch file must be downloaded before you can create a hash. A hash file is used to ensure the integrity of the patch file during remediation (i.e., when it's deployed and installed on an affected device). The security scanner does this by comparing the hash code created when you click the Generate MD5 Hash button with a new hash it generated immediately before attempting to install the patch file from the patch repository. If the two hash files match, remediation proceeds. If the two hash files do not match, indicating the patch file has changed in some way since being downloaded to the repository, the remediation process quits.
 - **Requires reboot:** Indicates whether the patch file requires a device reboot before completing its installation and configuration processes on the device.
 - **Silent install:** Indicates whether the patch file can complete its installation without any end user interaction.

Detecting the patch pages

The following pages refer to the detection logic used by the rule to check if the patch is already installed on devices.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

About the Detecting the patch: Files used for installed patch detection page

This page specifies the file conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Files page for definition detection logic (see above). However, the logic works conversely when detecting patch installation. In other words, when checking for a patch installation, all of the file conditions specified on this page must be met in order to determine an installation.

About the Detecting the patch: Registry settings used for installed patch detection page

This page specifies the registry key conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Registry settings page for definition detection logic (see above). However, the logic works conversely in this case. In other words, when checking for a patch installation, all of the registry conditions specified on this page must be met in order to determine an installation.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

Patch installation and removal pages

The following pages let you configure additional commands that run when the patch is installed on or uninstalled from affected devices.

This option is available only for custom definitions that allow remediation.

These commands are useful if you need to program specific actions on target devices to ensure successful remediation. Additional commands aren't required. If you don't configure any additional commands, the patch file executes by itself by default. Keep in mind that if you do configure one or more additional commands, you must also include a command that executes the actual patch file with the Execute command.

About the Patch install commands page

Use this page to configure additional commands for a patch install task. The available commands are the same for patch install and uninstall.

- **Commands:** Lists commands in the order they will run on target devices. Select a command to view its arguments. You can change the order of commands with the **Move Up** and **Move Down** buttons. To remove a command from the list, select it and click **Remove**.
- **Add:** Opens a dialog that lets you select a command type to add to the Commands list.

- **Command Arguments:** Displays the arguments that define the selected command. An argument's values can be edited. To edit any argument, double-click its **Value** field, and then type directly in the field. For all the command types, you can also right-click in the **Value** field to insert a macro/variable into the argument.

The following list describes the commands and their arguments:

- **Copy:** Copies a file from the specified source to the specified destination on the hard drive of the target device. This command can be used before and/or after executing the patch file itself. For example, after extracting the contents of a compressed file with the Unzip command, you may want to copy files from one location to another.

The arguments for the Copy command are: Dest (full path where you want to copy the file), not including the filename and Source (full path, and file name, of the file you want to copy).

- **Execute:** Runs the patch file, or any other executable file, on target devices.

The arguments for the Execute command are: Path (full path, and file name, where the executable file resides; for the patch file, you can use the %SDMCACHE% and %PATCHFILENAME% variables), Args (command-line options for the executable file; note this field is not required), Timeout (number of seconds to wait for the executable to terminate before continuing to the next command in the list, if the Wait argument is set to true), and Wait (true or false value that determines whether to wait for the executable to terminate before continuing to the next command in the list).

- **ButtonClick:** Automatically clicks a specified button that displays when an executable file runs. You can use this command to program a button click if such interaction is required by the executable.

In order for the ButtonClick command to work properly, the Wait argument for the preceding Execute command must be set to false so that the executable doesn't have to terminate before continuing to the button click action.

The arguments for the ButtonClick command are: Required (true or false value indicating whether the button must be clicked before proceeding; if you select true and the button can't be clicked for any reason, remediation quits; if you select false and the button can't be clicked, remediation will continue), ButtonIDorCaption (identifies the button you want clicked by its text label, or its control ID), Timeout (number of seconds it takes for the button you want clicked appears when the executable runs), and WindowCaption (identifies the window or dialog where the button you want clicked is located).

- **ReplaceInFile:** Edits a text-based file on target devices. Use this command if you need to make any modifications to a text-based file, such as a specific value in an .INI file, before or after executing the patch file to ensure that it runs correctly.

The arguments for the ReplaceInFile command are: Filename (full path and name of the file you want to edit), ReplaceWith (exact text string you want to add to the file, and Original Text (exact text string you want to replace in the file).

- **StartService:** Starts a service on target devices. Use this command to start a service required for the patch file to run, or to restart a service that was required to be stopped in order for the patch file to run.

The arguments for the StartService command are: Service (name of the service).

- **StopService:** Stops a service on target devices. Use this command if a service must be stopped on a device before the patch file can be installed.

The arguments for the StopService command are: Service (name of the service).

- **Unzip:** Unzips a compressed file on target devices. For example, you can use this command if remediation requires more than one file be run or copied on target devices.

The arguments for the Unzip command are: Dest (full path to where you want to extract a compressed file's contents on a device's hard drive), and Source (full path and filename of the compressed file).

- **WriteRegistryValue:** Writes a value to the registry.

The arguments for the WriteRegistryValue are: Key, Type, ValueName, ValueData, WritelfDataEmpty

About the Patch uninstall commands page

Use this page to configure additional commands for a patch uninstall task. The available commands are the same for patch install and uninstall. However, the Patch uninstall commands page includes two unique options:

- **Patch can be uninstalled:** Indicates whether the patch file can be uninstalled from remediated devices.
- **Original patch is required for uninstall:** Indicates whether the original patch executable file itself must be accessible on the core server in order to uninstall it from scanned devices.

For information on the commands, see "About the Patch install commands page" on page 735.

About the Purge security and patch definitions dialog

Use this dialog to completely remove definitions (and their associated detection rules) from the core database.

Requires the LANDesk Administrator right

A user must have the LANDesk Administrator right in order to perform this task.

You may want to remove definitions if they have become obsolete, are not working properly, or if the related security risk has been totally resolved.

This dialog contains the following options:

- **Platforms:** Specifies the platforms whose definitions you want to remove from the database.

If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition and its detection rule information to be removed.

- **Languages:** Specifies the language versions of the selected platforms whose definitions you want to remove from the database.

If you've selected a Windows or Macintosh platform, you should specify the languages whose definition information you want to remove. If you've selected a UNIX or Linux platform, you must specify the Language neutral option in order to remove those platform's language independent definition information.

- **Types:** Specifies the content types whose definitions you want to remove.
- **Purge:** Completely removes definition and detection rule information for the types you've selected that belong to the specified platforms and languages you've selected. This information can only be restored by downloading the content again.
- **Close:** Closes the dialog without saving changes and without removing definition information.

About the Create security scan task dialog

Use the **Create security scan task** dialog to create and configure a task that runs the security and patch scanner on target devices.

On-demand security and compliance scans

You can also run an immediate security or compliance scan on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), and either click **Security and Patch scan** and select a scan and repair setting, or click **Compliance scan**, and then click **OK**.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the security and patch scan task.
- **Create a scheduled task:** Adds the security and patch scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the security and patch scan task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Scan and repair settings:** Specifies scan and repair settings used for the scan task. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, user interaction, and the security content types scanned. Select a scan and repair setting from the drop-down list to assign it to the security scan task you're creating. You can click **Edit** to modify the options for the selected scan and repair setting. You can also click **Configure** to create a new scan and repair setting. For more information, see "About the Configure scan and repair (and compliance, and firewall) settings dialog" on page 739.

About the Configure scan and repair (and compliance, and firewall) settings dialog

Use this dialog to manage your scan and repair (and compliance, and firewall) settings. Once configured, you can apply settings to security scan tasks, compliance scan tasks, repair tasks, uninstall tasks, and reboot tasks.

This dialog contains the following options:

- **New:** Opens the settings dialog where you can configure the options pertaining to the specified settings type.
- **Edit:** Opens the settings dialog where you can modify the selected setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename.
- **Delete:** Removes the selected setting from the database.

Note: the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.)

- **Close:** Closes the dialog, without applying a setting to the task.

About the Scan and repair settings dialog

Use this dialog to create and edit scan and repair settings. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, user interaction, and the content types scanned.

Note on compliance scan settings

The information on this dialog can also apply to compliance scans, with the **Compliance** tab taking the place of the **Scan** tab. See the About the Compliance tab section below for details about the specific settings that apply to compliance scans.

Note on reboot task settings

The settings on the **Reboot** tab of this dialog can also be used for a reboot only task.

You can create as many scan and repair settings as you like and edit them at any time. For example, you can configure a scan and repair setting with a specific notification and reboot scenario for desktop devices, and another scan and repair setting with different reboot options for servers. Or, you can configure an scan and repair setting for Windows vulnerability scanning, and another one for spyware scanning, etc.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks.

Scan and repair settings

- **Name:** Identifies the setting with a unique name. This name appears in the settings drop-down list on a security task dialog.

The settings dialog contains the following tabs:

- "About the Scan and repair settings: General tab" on page 740
- "About the Scan and repair settings: Scan tab" on page 741
- "About the Scan and repair settings: Compliance tab" on page 741
- "About the Scan and repair settings: Repair tab" on page 742
- "About the Scan and repair settings: MSI tab" on page 742
- "About the Scan and repair settings: Reboot tab" on page 743
- "About the Scan and repair settings: Networking tab" on page 743
- "About the Scan and repair settings: Pilot tab" on page 744

About the Scan and repair settings: General tab

- **Show progress when running:** Enables the security and patch scanner to display information on end user devices while it is running. Click this option if you want to show scanner activity, and if you want to configure other display and interaction options in this dialog. If you don't click this option, none of the other tabs on this dialog are available to configure, and the scanner runs transparently on devices.
- **Allow user to cancel scan:** Shows a Cancel button on the Security and Patch Manager dialog on the end user device. Click this option if you want the end user to have the opportunity to cancel a scan operation. If this option is not checked, the dialog doesn't have a Cancel button and the end user can't stop the scan.
- **When no reboot is required:**
 - **Require end user input before closing:** For a scan or repair task that doesn't require a reboot in order to complete its full operation, click this option if you want the scanner to prompt the end user before its display dialog closes on the device. If you select this option, and the end user does not respond the dialog remains open which could cause other scheduled tasks to timeout.
 - **Close after timeout:** For a scan or repair task that doesn't require a reboot, click this option if you want the scanner's display dialog to close after the duration you specify.
- **Scan for:** Specifies which content types you want to scan for with this scan task. You can select either a custom group (preconfigured) or specific content types. You can select only those content types for which you have a LANDesk Security Suite content subscription. Also, the actual security definitions that are scanned for depends on the contents of the Scan group in the Security and Patch Manager window. In other words, if you select vulnerabilities and security threats in this dialog, only those vulnerabilities and security threats currently residing in their respective Scan groups will be scanned for.
- **Enable autofix:** Indicates that the security and patch scanner will automatically deploy and install the necessary associated patch files for any vulnerabilities or custom definitions it detects on scanned devices. This option applies to security scan tasks only. In order for autofix to work, the patch file must also have autofix enabled.

About the Scan and repair settings: Scan tab

- **Scan for:** Specifies which content types you want to scan for with this scan task. You can select either a custom group (preconfigured) or specific content types. You can select only those content types for which you have a LANDesk Security Suite content subscription. Also, the actual security definitions that are scanned for depends on the contents of the Scan group in the Security and Patch Manager window. In other words, if you select vulnerabilities and security threats in this dialog, only those vulnerabilities and security threats currently residing in their respective Scan groups will be scanned for.
- **Immediately repair all detected items:** Indicates that any security risk identified by this particular group scan will be automatically remediated.
- **Enable autofix:** Indicates that the security and patch scanner will automatically deploy and install the necessary associated patch files for any vulnerabilities or custom definitions it detects on scanned devices. This option applies to security scan tasks only. In order for autofix to work, the patch file must also have autofix enabled.

About the Scan and repair settings: Compliance tab

Note that the options on the Compliance tab apply to compliance security scans only.

- **Frequently scan the Compliance group:** Runs a frequent security scan based on the contents of the Compliance group. The basic frequent security scan is defined in the initial agent configuration, but you can override it with the options on this tab. You can specify to run the compliance security scan only when a user is logged into the managed device.
- **Scan after IP address change:** Performs a compliance security scan whenever the IP address changes on target devices. For example, if a laptop is reconnected to your network and receives a different IP address than before.
- **Disable the frequent security scanner in Agent configuration:** Indicates that a frequent security scan set up via the device's agent configuration will be turned off, and the frequent scan settings defined here will be used for a compliance security scan instead.
- **Enable autofix:** Indicates that the security scanner will automatically deploy and install the necessary associated patch files for any vulnerability definitions it detects on scanned devices. This option applies to security and compliance scan tasks only. In order for autofix to work, the must also have autofix enabled.
- **Immediately repair all detected items:** All detected vulnerabilities are remediated, even if their associated patches do not have autofix enabled.
- **Enforce current IP Security configuration after scan:** Ensures that IP Security-enabled devices that are scanned for security compliance using this setting subsequently use the current IP Security policy once the scan is finished.
- **Enforce 802.1X supported scan:** Ensures that 802.1X-enabled devices that are scanned for security compliance using this setting are either allowed access or quarantined based on their being compliant or non-compliant to the custom security policy.

- **If a virus cannot be removed or quarantined (LANDesk Antivirus only):** The following two options apply to LANDesk Antivirus only and provide a method for you to have an antivirus scan trigger or initiate a full security scan that checks target devices configured with this setting for compliance with your current security policy. In other words, whether the device is healthy or unhealthy. You can select one or both of the options below. The action described by these options occurs any time a virus is detected on the device and can't be removed or quarantined. (**Note:** As a prerequisite for performing this type of scan, you must first add the predefined AV-110 antivirus definition to the Compliance group. You should also add any other definitions you want to use to define your security policy to the Compliance group.)
 - **Immediately scan devices for compliance:** If a virus is detected and can't be removed or quarantined, a compliance security scan (by the security scanner, not the antivirus scanner) is initiated right away.
 - **Perform network access control check to determine if device is unhealthy:** If a virus is detected and can't be removed or quarantined, a network access control check is initiated immediately by LANDesk NAC.

About the Scan and repair settings: Repair tab

- **Prompt user before repairing, installing or uninstalling a patch:** Click this option if you want a prompt to appear on the end user device, with message and interaction controls as configured with the options below. If you don't click this option, the operation will proceed automatically without prompting the end user.
- **Allow user to cancel before starting repair, install or uninstall:** Click this option if you want the end user to have the opportunity to cancel a patch file repair operation.
- **Message:** Type a message in this box that will appear in the security and patch scanner's display dialog on the end user device WHEN a security scan task detects any of the specified definitions on the scanned device. You can customize this message depending on the type of security scan you're running.
- **If no end user response:**
 - **Wait for user response:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely.
 - **After timeout, automatically:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and perform the patch file operation or close without performing the operation, after the duration you specify.
- **Maximum percent of bandwidth to use when downloading:** Specify the bandwidth percentage you want to be used for the patch file download from the patch repository to scanned devices. You can use this setting to balance network traffic for large patch file deployments.
- **Start repair even if reboot is already pending:** Indicates that remediation will begin without waiting for the reboot operation.

About the Scan and repair settings: MSI tab

Use this tab if a patch file needs to access its originating product installation resource in order to install any necessary supplemental files. For example, you may need to provide this information when you're attempting to apply a patch for Microsoft Office or some other product suite.

- **Original package location:** Enter the UNC path to the product image.

- **Credentials for original package location:** Enter a valid user name and password to authenticate to the network share specified above.
- **Ignore the /overwriteoem command-line option:** Indicates the command to overwrite OEM-specific instructions will be ignored. In other words, the OEM instructions are executed.
- **Run as Information: Credentials for running patches:** Enter a valid user name and password to identify the logged in user for running patches.

About the Scan and repair settings: Reboot tab

- **When deciding whether to reboot:** Specify how you want the security and patch scanner to act when a scan or repair task tries to reboot a device for any reason. You can select for the device to never reboot, reboot only if needed, or always reboot.
- **When rebooting:**
 - **Prompt user before rebooting:** For when a reboot occurs, click this option if you want the security and patch scanner to prompt the end user. If you select this option, you can configure the accompanying reboot options below.
 - **Allow user to defer reboot:** Shows a defer button on the reboot prompt on the end user device. Specify the deferral time span and the number of times the end user can defer the reboot. The deferral (or snooze time) begins with the next local scheduler poll.
 - **Allow user to cancel reboot:** Shows a cancel button on the reboot prompt on the end user device.
 - **Reboot message:** Type a message in this box that will appear in the security and patch scanner's display dialog on the end user device WHEN a security scan task prompts the end user before attempting to reboot the device.
 - **Wait for user response:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely. If there's no response, the prompt remains open.
 - **After timeout, automatically:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and either reboot, snooze, or close the prompt without rebooting, after the duration you specify.

About the Scan and repair settings: Networking tab

Use this tab to identify an alternate core server that can be used for security scanning and remediation if the main core server is not available.

- **Communicate with alternate core server:** Enables communication with an alternate server.
- **Server name:** Enter the name of a valid, licensed LANDesk core server.

Note: The syntax for the servername field should be: <servername>:<port number> where port number is the secure port 443 for SSL transmission. If you enter only a servername, without specifying port 443, it defaults to port 80 which is the standard HTTP port.

About the Scan and repair settings: Pilot tab

Use this tab to create and configure a pilot group for testing security definitions before performing a wider deploying on your entire network.

- **Periodically scan and repair definitions in the following group:** Enables the pilot security scan features. Once you've checked this option, you need to select a custom group from the drop-down list.
- **Change settings:** Opens the Schedule scan dialog where you can define the parameters for the security scan. Click the Help button for details

About the Schedule periodic pilot scan and repair dialog

This dialog is shared by several LANDesk management tasks. For details about the options on this dialog, see "About the Schedule dialog" on page 719.

About the Definition group settings dialog

Use this dialog to create, edit, and select settings that control how and where security definitions are downloaded based on their type and/or severity.

This dialog contains the following options:

- **Definition type and severity filters:** Lists definition group settings.
- **Type:** Shows the definition type for the selected group setting.
- **Severity:** Shows the definition severity for the selected group setting.
- **Status:** Shows the status (Do not scan, Scan, and Unassigned) for definitions that match the group settings when they're downloaded. Status corresponds to the group nodes in the Security and Patch Manager tree view. Unassigned is the default status.
- **Group(s):** Shows the group or groups where the security definitions matching the type and severity criteria specified above are placed. You can add and delete as many custom groups as you like.
- **Autofix:** If you've specified that downloaded security definitions are set to Scan status (placed in the Scan group), select this option if you want the vulnerabilities to have autofix enabled.

About the Definition filter properties dialog

Use this dialog to define a definition group settings. These settings control how and where security definitions are downloaded based on their type and/or severity.

This dialog contains the following options:

- **Filter:** Defines which security content (definitions) will be place in the group or groups selected below.
 - **Definition type:** Select the definition type you want to download with your desired status and location.
 - **Severity:** Select the severity for the specified definition type. If the type matches but the severity does not, the definition will not be filtered by this setting.

- **Action:** Defines what you want to do with the downloaded definitions and where you want them placed.
 - **Set status:** Select the status for the downloaded definitions. Options include: Do not scan, Scan, and Unassigned.
 - **Set autofix:** Select autofix if the status is Scan and you want the security risk to be fixed automatically upon detection.
 - **Put definition in custom groups:** Select one or more groups with the Add and Delete buttons. You can select any of the custom groups you've created, the Alert group, the Compliant group, and several of the available security industry groups.

About the Security and patch information dialog

Use this dialog to view detailed security and patch information for selected devices. You can view a device's scan results, detected security definitions, missing and installed patches (or software updates), and repair history.

Use the **Clear** button to remove all scan information from the database for the selected devices.

You can also right-click a vulnerability (or other security content type) in this view and directly create a repair task, or enable/disable the autofix option for applicable security content types.

Displayed information is based on the selected security content type

The group names and information fields that display on this page are dynamic, depending on the security content type you select from the **Type** drop-down list. For example, if you select vulnerabilities, the following information fields display:

- **Missing Patches (Vulnerabilities Detected):** Lists all of the vulnerabilities detected on the device by the last scan.
- **Installed Patches:** Lists all of the patches installed on the device.
- **Repair History:** Shows information about the remediation tasks attempted on the device. This information is helpful when troubleshooting devices. To clear this data, click **Purge Repair History**, specify the devices and time range settings, and then click **Purge**.
- **Vulnerability Information:**
 - **Title:** Displays the title of the selected vulnerability.
 - **Detected:** Indicates whether the selected vulnerability was detected.
 - **First detected:** Displays the date and time the vulnerability was initially detected on the device. This information can be useful if you've performed multiple scans.
 - **Reason:** Describes the reason why the selected vulnerability was detected. This information can be useful in helping you decide whether the security risk is serious enough to prompt immediate remediation.
 - **Expected:** Displays the version number of the file or registry key the vulnerability scanner is looking for. If the version number of the file or registry key found on the scanned device matches this number, the vulnerability does not exist.
 - **Found:** Displays the version number of the file or registry key found on the scanned device. If this number is different than the Expected number above, the vulnerability exists.
- **Patch Information:**

- **Patch Required:** Displays the file name of the patch executable required to remediate the selected vulnerability.
- **Patch Installed:** Indicates whether the patch file has been installed.
- **Last action date:** Displays the date and time the patch was installed on the device.
- **Action:** Indicates whether the last action was an install or an uninstall.
- **Details:** Indicates whether the deployment/installation was successful. If an installation failed, you must clear this status information before attempting to install the patch again.
- **Clear:** Clears the current patch installation date and status information for the selected device. Clearing this information is necessary in order to attempt to deploy and install the patch again.

About the Create compliance scan task dialog

Use the **Create compliance task** dialog to create and configure a task that runs the security scanner to check target devices specifically for compliance with your security policy based on the contents of the Compliance group.

On-demand security and compliance scans

You can also run an immediate security or compliance scan on one or more target devices. Right-click the selected device (or up to 20 multi-selected devices), and either click **Security and Patch scan** and select a scan and repair setting, or click **Compliance scan**, and then click **OK**.

This dialog contains the following options:

- **Task name:** Enter a unique name to identify the compliance scan task.
- **Create a scheduled task:** Adds the compliance scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Target machines that have not reported since:** Limits the compliance scan to only those managed devices that haven't reported security scan results since the date you specify.
- **Start now:** Sets the scheduled scan task to begin as soon as the task is added to the Scheduled tasks window so that you don't have to manually configure scheduling options.
- **Create a policy:** Adds the compliance scan task as a policy to the Scheduled tasks window, where you can configure the policy options.

About the Create reboot task dialog

Use this dialog to create and configure a generic reboot task.

A reboot task can be useful when you want to install patches (without rebooting) as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

- **Task name:** Identifies the task with a unique name.
- **Create a scheduled task:** Creates a reboot task in the Scheduled tasks window when you click **OK**.
- **Create a policy:** Creates a reboot policy when you click **OK**.

- **Scan and repair settings:** Specifies which scan and repair settings' reboot configuration is used for the task to determine reboot requirements and action on target devices. Select a scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

About the Create repair task dialog

Use this dialog to create and configure a repair (remediation) task for the following definition types: vulnerabilities, spyware, LANDesk software updates, custom definitions, and security threats with an associated patch. The schedule repair option is not applicable to blocked applications.

This dialog includes the following tabs:

- "About the Create repair task: General tab" on page 747
- "About the Create repair task: Patches tab" on page 748

About the Create repair task: General tab

- **Task name:** Identifies the repair task with a unique name. The default is the name of the selected definition or the custom group. You can edit this name if you prefer.
- **Repair as a scheduled task:** Creates a security repair task in the Scheduled tasks window when you click **OK**.
- **Split into staging task and repair task:** (Optional) Allows you to create to separate tasks in the Scheduled tasks tool; one task for staging the required patch files in the target device's local cache; and one task for actually installing those patch files on the affected devices.
 - **Select computers to repair:** Specifies which devices to add to the scheduled repair task. You can choose no devices, all affected devices (devices where the definition was detected by the last security scan), or only the affected devices that are also selected (this last option is available only when you access the Schedule repair dialog from within a device Security and patch information dialog).
 - **Use Multicast:** Enables Targeted Multicast for patch deployment to devices. Click this option, and click **Multicast Options** if you want to configure multicast options. For more information, see "About the Multicast options dialog" on page 748.
- **Repair as a policy:** Creates a security repair policy when you click **OK**.
 - **Add query representing affected devices:** Creates a new query, based on the selected definition, and applies it to the policy. This query-based policy will search for devices affected by the selected definition, and deploy the associated patch.
 - **Download patch only from local peers:** Restricts patch deployment so that it will only take place if the patch file is located in the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, the patch file must currently reside in one of these two places.
 - **Download patch only (Do not repair):** Downloads the patch file to the patch repository but does not deploy the patch. You can use this option if you want to retrieve the patch file in a staging scenario for testing purposes before actual deployment.

- **Scan and repair settings:** Specifies which scan and repair setting is used for the repair task to determine whether the security and patch scanner displays on devices when it is running. Select an scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

About the Create repair task: Patches tab

Use this tab to show either required patches only or all associated patches for the selected vulnerability. (**Note:** The fields on this page are the same as the fields on the "About the Download associated patches dialog" on page 729.)

To download patches directly from this tab, if they have not already been downloaded and placed in the patch repository, click **Download**.

About the Multicast options dialog

Use this dialog to configure the following Targeted Multicast options for a scheduled security repair task:

- **Multicast Domain Discovery:**
 - **Use multicast domain discovery:** Select this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
 - **Use multicast domain discovery and save results:** Select this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
 - **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery that saved the results.
- **Have domain representative wake up computers:** Use this option if you want computers that support Wake On LAN technology to turn on so they can receive the multicast.
- **Number of seconds to wait after Wake on LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

The options below let you configure task-specific Targeted Multicast parameters. The defaults should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time.
- **Limit the processing of machines that failed multicast:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the Custom Job dialog would process no more than 20 computers at a time that failed the multicast. The Custom Job dialog will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the Custom Job dialog won't perform the distribution portion of the task for any computer that failed multicast.

- **Number of days the files stay in the cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged.
- **Number of days the files stay in multicast domain representative cache:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets.

This value is only used when the domain representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN.

- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above.

About the Uninstall patch dialog

Use this dialog to create and configure an uninstall task for patches that have been deployed to affected devices.

- **Task name:** Identifies the task with a unique name. The default is the name of the patch. You can edit this name if you prefer.
- **Uninstall as a scheduled task:** Creates an uninstall patch task in the Scheduled tasks window when you click **OK**.
 - **Select targets:** Specifies which devices to add to the uninstall patch task. You can choose no devices, all devices with the patch installed, or only the devices with the patch installed that are also selected (this last option is available only when you access the Uninstall Patch dialog from within a device Security and Patch Information dialog).
- **If the original patch is required:**
 - **Use Multicast:** Enables Targeted Multicast for deploying the uninstall patch task to devices. Click this option, and click **Multicast Options** if you want to configure the multicast options. For more information, see "About the Multicast options dialog" on page 748.
- **Uninstall as a policy:** Creates an uninstall patch policy in the Scheduled tasks window when you click **OK**.
 - **Add query representing affected devices:** Creates a new query, based on the selected patch, and applies it to the policy. This query-based policy will search for devices with the selected path installed and uninstall it.
- **Scan and repair settings:** Specifies which scan and repair setting is used for the uninstall task to determine whether the security and patch scanner displays on devices, reboot options, MSI location information, etc. Select an scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

About the Change settings task dialog

Use this dialog to create and configure a task that changes the default settings on target devices for one or more LANDesk services. The LANDesk services you can change are:

- 802.1X support settings
- Compliance security settings (applies only to compliance security scans)
- Configure Windows firewall settings
- Custom variable override settings
- Host Intrusion Prevention System (HIPS) settings
- LANDesk Antivirus settings
- Scan and repair settings

With a change settings task you can conveniently change a managed device's default settings (which are written to the device's local registry) without having to redeploy a full agent configuration.

- **Task name:** Enter a unique name to identify the task.
- **Create a scheduled task:** As the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **802.1X support settings:** Specifies 802.1X network access control settings on target devices. You can use LANDesk 802.1X to enforce your compliance security policy on managed devices that support 802.1X, by running compliance security scans, granting or blocking access depending on device health status (compliance), quarantining unhealthy (non-compliant) devices, and performing remediation.
- **Compliance security settings:** Specifies compliance settings used for compliance scan tasks. Compliance settings determine when and how a compliance scan takes places, whether remediation occurs automatically, and/or what to do when LANDesk Antivirus detects a virus infection on target devices.
- **Configure Windows firewall settings:** Specifies Windows firewall settings on target devices. You can enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs).
- **Custom variables override settings:** Specifies custom variable override settings used on target devices when they're scanned for security definitions that include custom variables (such as security threats and viruses). Custom variable override settings let you specify setting values you want to ignore or bypass during a security scan. This is very useful in situations where you don't want a scanned device to be identified as vulnerable according to a definition's default custom variable settings. Select a setting from the drop-down list. From the drop-down list, you can also select to remove the custom variable override settings from target devices. The **Remove custom variable settings** option lets you clear a device so that custom variable settings are in full affect. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Custom variable override settings dialog" on page 751.
- **Host Intrusion Prevention System (HIPS) settings:** Specifies HIPS settings used for HIPS protection on target devices. For more information, see "Configuring LANDesk HIPS protection options with HIPS settings" on page 501.
- **LANDesk Antivirus settings:** Specifies antivirus settings used for antivirus scan tasks. Antivirus settings determine whether the LANDesk Antivirus icon appears in the device system tray, availability of interactive options to end users, email scan and real-time protection enabling, file types to scan, files and folders to exclude, infected file quarantine and backup, scheduled antivirus scans, and scheduled virus definition file updates. Select a setting from the drop-down list. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Antivirus settings dialog" on page 653.

- **Scan and repair settings:** Specifies scan and repair settings used for security scan tasks. Scan and repair settings determine whether the scanner displays on devices while running, reboot options, user interaction, and the security content types scanned. Select a setting from the drop-down list. Click **Edit** to modify the options for the selected setting. Click **Configure** to create a new setting. For more information, see "About the Scan and repair settings dialog" on page 739.

About the Configure custom variable override settings dialog

Use this dialog to manage your custom variable override settings. Once configured, you can apply custom variable override settings to a change settings task and deploy it to target devices to change (or remove) their default custom variable override settings.

Custom variables overrides lets you configure exceptions to custom variable values. In other words, with custom variable override settings you can ignore or bypass a specific custom variable condition so that a scanned device is not determined to be vulnerable.

This dialog contains the following options:

- **New:** Opens the Custom variable override settings dialog where you can configure the options.
- **Edit:** Opens the settings dialog where you can modify the selected custom variable override setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename.
- **Delete:** Removes the selected setting from the database.

Note the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new change settings task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.

- **Close:** Closes the dialog, without applying a setting to the task.

About the Custom variable override settings dialog

Use this dialog to create exceptions to custom variable settings. Some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Typically, antivirus definitions also have custom variable settings.

With custom variables you can fine-tune security threat scanning by modifying one or more setting's values so that the scanner checks for conditions you define, and therefore determines a device to be vulnerable only if that condition is met (i.e., the value you specify is detected). Custom variables are a global setting, so when you scan for a security definition that includes a custom variable it will always be determined to be vulnerable if that custom variable condition is met.

Edit Custom Variables right required

In order to edit custom variable settings, and configure custom variable override settings, a LANDesk user must have the Edit Custom Variables role-based administration right. Rights are configured with the **Users** tool.

Custom variable override setting information can be viewed in the device's Inventory view.

About the Alert settings dialog

Use this dialog to configure security-related alerting for scanned devices, including both vulnerability and antivirus alerting.

The Alert settings dialog contains the following tabs:

Definitions tab

Use this tab to configure security alerting. If you've added security definitions to the Alert group, Security and Patch Manager will alert you whenever any of those definitions is detected on any scanned device.

- **Minimum alert interval:** Specifies the shortest time interval (in minutes or hours) in which alerts for detected vulnerabilities are sent. You can use this setting if you don't want to be alerted too frequently. Set the value to zero if you want instant, real-time alerting to occur.
- **Add to Alert group:** Indicates which vulnerabilities, by severity level, are automatically placed in the Alert group during a content download process. Any definition placed in the Alert group is also automatically placed in the Scan group by default (in order to include those definitions in a security scan task).

Antivirus tab

Use this tab to configure antivirus alerting.

- **Minimum alert level:** Specifies the shortest time interval (in minutes or hours) in which alerts for detected viruses are sent. You can use this setting if you don't want to be alerted too frequently. Set the value to zero if you want instant, real-time alerting to occur.
- **Alert on:** Indicates which antivirus events generate alerts.

About the Rollup core settings dialog

Use this dialog to enable and configure automatic forwarding of the latest security scan results to a rollup core server on your network. Security (vulnerability) data forwarding allows you to view real-time vulnerability status for all of your managed devices in a large, distributed enterprise network without having to manually retrieve that data directly from the primary core server.

Every time the security scanner runs it writes a scan results file to a folder called VulscanResults on the core server and notifies the LANDesk Security web service, which adds the file to the core database. If the rollup core settings are enabled and a valid rollup core is identified, the rollup core reads the scan results file into its own database, providing faster access to critical vulnerability information.

The Rollup core settings dialog contains the following options:

- **Send scan results to rollup core immediately:** Enables immediate forwarding of security scan results to the specified core server, using the method described above.
- **Use default rollup URL:** Check this box if you want the default URL to be used when the scan results file is sent from the core server to the rollup core. Enter the name of the core server, and then check this box to automatically insert the script and Web address in the **Rollup URL** field.
- **Rollup core name:** Identifies the rollup core you want to receive the latest security scan results from the core database.
- **Rollup URL:** Specifies the Web address of the rollup core receiving the security scan results and the destination folder for the scan results file on the rollup core. The rollup URL can either be automatically inserted by checking the **Use default rollup URL** checkbox, or you can manually edit the field by clearing the checkbox and entering the URL you want.

About the Select columns dialog

Use this dialog to configure data columns for item lists in the Security and Patch Manager tool window. You decide which data columns are displayed so that you can sort through long lists of downloaded security definitions and quickly and easily find the information you need for a specific task or situation.

Using the CVE ID data column

LANDesk security products support the CVE (Common Vulnerabilities and Exposures) naming standard. With Security and Patch Manager you can search for vulnerabilities by their CVE names, and view CVE information for downloaded vulnerability definitions. For more information about the CVE naming convention, LANDesk compatibility with the CVE standard, and how to use CVE identification to find individual vulnerabilities in Security and Patch Manager, see [Using CVE names](#).

By adding and removing data columns, and moving them up and down in the list (to the left and to the right in the column view), you ensure that important, relevant information is front and center.

- **Available columns:** Lists the data columns that are currently not displayed in the Security and Patch Manager tool window, but are available to add to the Selected Columns list.
- **Selected columns:** Lists the data columns that are currently displayed in the Security and Patch Manager window. The data columns display in a downloaded security definition list from left to right in the same order as they appear here from top to bottom.
- **Defaults:** Restores the default displayed data columns.

About the Configure firewall settings dialogs

Use these dialogs to configure firewall settings. Windows firewall settings are associated with a change settings task to enable/disable the firewall, and configure firewall settings including exceptions, inbound rules, and outbound rules (for services, ports, programs) on target devices running the following Windows platforms:

- Windows 2003/XP
- Windows Vista

This dialog contains the following options:

- **Current exceptions:** Lists programs, ports, and services whose connection/communication is NOT being blocked by the firewall. The firewall prevents unauthorized access to devices, except for the items in this list.
- **Add program:** Lets you add a specific program to the exception list to allow communication.
- **Add port:** Lets you add a specific port to the exception list to allow communication.
- **Edit:** Lets you edit to the selected exception's properties, including the scope of affected devices.
- **Delete:** Removes the selected exception from the list.
- **OK:** Saves your changes and closes the dialog.
- **Cancel:** Closes the dialog without saving your changes.

Windows firewall security threat definitions

Additionally, LANDesk Security provides predefined security threat definitions that let you scan for, detect, and configure firewall settings on managed devices running specific Windows platforms. The following security threat definitions let you scan for and modify firewall settings:

- **ST000102:** Security threat definition for the Windows firewall on Windows 2003 SP1; Windows XP SP.
- **ST000015:** Security threat definition for the Internet Connection Firewall on Windows 2003 SP1; Windows XP SP2.

The Windows firewall security threat properties includes custom variables that let you configure Windows firewall settings. You can use these security threat definitions to scan for your specified settings and return a vulnerability condition if those settings are not matched. You can then use the customized definition in a repair task in order to turn on or off the firewall as well as change or reconfigure the firewall settings on the scanned device.

About the Gather historical information dialog

Use this dialog to compile data about scanned and detected vulnerabilities on managed devices. This information is used for security and patch reports. You can either gather the data immediately or create a task to collect the data for a specified period of time.

This dialog contains the following options:

- **Task name:** Identifies the gather historical information task with a unique name.
- **Keep historical data for:** Specifies the amount of time (in days) for which data will be collected. You can specify 1 day to 3,000 days.
- **Gather now:** Immediately collects the current data.
- **Create task:** Adds the task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Purge:** Completely removes data collected to this point.

Software distribution help

Using the Distribution package dialog

The **Distribution package** dialog (**Tools | Distribution | Distribution package**) stores information in the database that describes the package that you want to distribute. The data contains the settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, installation options, and so on. Once created, this information is called a "distribution package."

Before using this dialog, put the package on your distribution server. You'll need to browse for the package and provide information on any package prerequisites or additional files. Once you've created a distribution package for your package, you can associate it with a delivery method (**Tools | Distribution | Delivery methods**) to deploy it to devices.

About the Package information page

Use this page to enter the package name and your package's primary file. If your package consists of a single file, add it here. If your package has multiple files, add the main file in your package, for example, the file that starts the install. You can add supporting additional files on the **Additional files** page.

To use the file browser, type a Web share or file path in the box next to the **Go** button. Clicking **Go** displays the destination in the **Primary file** box. You can continue navigating there. When browsing for the file, double-click the file you want to be the primary file. This adds the filename to the package path next to the Go button.

- **Name:** The name you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Package owner:** You can select **Public** if you want all console users to see this package, otherwise, you can select your own username so that only you can see it. Administrators can select a specific user, in addition to **Public**.
- **Description:** The description you enter here appears in the **Distribution packages** and **Delivery methods** dialogs.
- **Primary file:** The main file in this package.
- **Go:** Starts browsing the path you entered next to the Go button.
- **Up:** Goes up one folder level from the current location you're browsing.

Using environment variables

Support for putting the environment variable directly into the package path isn't supported in Management Suite, though expansion will still work with previously created custom scripts. To support environment variables for the new SWD architecture, the "PreferredPackageServer" registry value should be set to the environment variable to be used. This environment variable will then be expanded to define the server from which the package should be retrieved.

About the Install/Uninstall options page

Use this page to specify the package type. You have several options depending on the package you're deploying. Not all package types have these options.

- **Install:** Specifies that you want to use an installation package to install software.
- **Uninstall:** Specifies that you want to use an installation package to remove software. When this flag is set, the script removes everything that was installed with the installation script.
- **Command line:** (Not available for SWD, Macintosh, or Linux packages). The command line you want passed to the primary file you specified. Software distribution automatically adds the basic parameters for the type of package you're distributing. For more information, see [Using package command lines](#).

The command line field also allows you to pass values from the device's database entry to the command line. You can use this to pass unique parameters to batch files and executables that you distribute. The command line field can contain a parameter such as %Computer.Device Name% that will call up the computer device name from the database for each targeted device and pass that parameter as part of the execution process. The parameters must be in BNF format and delimited by percent symbols. Examples of valid BNFs are as follows:

- % Computer.Display Name% : The network display name of the computer.
- % Computer.Network.TCPIP.Address% : The IP address of the computer.
- % Computer.OS.Name% : The operating system name of the computer.

You can see the BNF values for database attributes in the create query dialog.

Using package command lines

When creating a Distribution Package, there is an option to include a command line. In the case of an MSI package, this field can only be used to specify a list of MSI Properties in this format: property1=value1 property2=value2 property3=value, and so on. One example of an MSI Property is TRANSFORMS.

The command line switches that are documented in MSI-related documentation, such as /q, /f, and so on, are actually msiexec command line switches. Only msiexec understands them. When LANDesk distributes an MSI package, it calls the MSI APIs directly. It does not use msiexec. Therefore, it isn't possible to specify msiexec command line switches in the command line field.

For many of the options that would be enabled with a command line switch when using msiexec, equivalent functionality is provided in through the delivery methods and distribution package tools. For others, no equivalent functionality is provided because it isn't needed.

Below is a list of some msiexec command-line switches and how equivalent functionality is provided (or not) in the LANDesk interface:

- **/q:** to control the user feedback options during an installation, use the **Feedback** options in the distribution package tool.
- **/a:** Administrative installation would be meaningless under LANDesk. It needs to be performed manually by the administrator. Therefore, no equivalent functionality is provided in LANDesk.

- **/f:** reinstall an MSI package. LANDesk will always reinstall the primary packages, so this option is implied. Note: If you don't want to reinstall, simply deploy the msi application as a dependent package instead of the primary package. If you don't have another package to make primary, you can create a package to deploy an empty batch file and make the MSI a dependent package. Then detection will take affect for the MSI application and it will only be installed on devices that it isn't already installed on.
- **/x:** uninstall an MSI package. Equivalent functionality is provided by the uninstall option in the distribution package tool.
- **/j:** advertise an MSI package. LANDesk implements similar concepts through policy-based delivery and the local device software deployment portal.
- **/l:** logging. Sdclient.exe gathers status and creates log files on the device by default.
- **/p:** install a patch; used to patch administrative images. Equivalent functionality is provided under LANDesk through Patch Manager and also with software distribution and dependent packages. Note: Deploy the latest patch as the primary package and set up a dependency chain for the MSI application and/or other patches.

About the Additional files page

If your package consists of multiple files, you can add them on this page. To use the file browser, type a Web share or file path in the box next to the Go button. Pressing the Go button displays the destination in the **Available** files box. You can continue navigating there. Select files in the **Available files** box and click >> to add them to the **Additional files** list. This adds them to the package.

- **Add additional files...:** The additional files you want to be part of your package.
- **Auto detect:** This option is available for MSI packages. It parses the primary MSI file for external file references and adds those automatically.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.
- **Go:** Starts browsing the path you entered next to the Go button.
- **Up:** Goes up one folder level from the current location you're browsing.

Using the Dependent packages page

Dependent packages are packages that must already be on the device in order for the package you're configuring to install. If they're not on the device, dependent packages are installed automatically. MSI and SWD packages are detected automatically through the appropriate registry keys on the device. For other package types, the package detection method depends on what you select on the detection page.

If you add an existing package with a dependency as a dependant package to the package you're creating, that existing dependency will also be added to the new package.

- **Available packages:** Lists the public packages you have created using the **Distribution package** window. Only public packages can be dependent. Select the packages you want to be dependent and click >>.
- **Dependent packages:** Lists the packages you've selected to be dependent.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.

Understanding Linux software dependencies

When you click **Save** in a Linux package's **Distribution package-properties** dialog, software distribution parses the primary RPM and any dependent RPMs you selected for dependencies those RPMs require. These dependencies then appear in the **Missing libraries** dialog. Checking a dependency in this dialog tells software distribution to not prompt you about it again. You can check dependencies you know are installed on managed devices. This dialog is for your information only. If a dependency is missing on a target device and you didn't specifically include that dependency as a dependent package, the RPM probably won't install successfully.

Using the Prerequisites page

The prerequisites page allows you to specify prerequisites for package installation. You can do this through a query or through an additional file/program that runs on devices and returns an errorlevel code. A non-zero code prevents the package from installing.

Prerequisites run on devices in the target list. If a device on the target list fails a prerequisite, the package won't be installed on it. The failure details are in the distribution task's log.

Prerequisites are especially useful in organizations where one person creates packages and another person distributes them. The distributor might not be aware of package system requirements that the creator does know about. In cases like these, the package creator can create a query that includes package requirements like operating system or amount of memory.

For the additional file option, you can select a file that's in the package's additional files list. You can then specify a command line you want the file to run with.

- **Choose a query:** Select an existing query that you want to use to filter targeted devices.
- **Run additional file:** If you want to run a file on devices, check this option.
- **Choose an additional file:** Enter the file you want devices to run. This file is run before any other package files.
- **Command line:** If the file you specified needs a command line, enter it here.

Using the Accounts page

Use the Accounts page to select the type of user account to use to distribute the package.

- **LocalSystem account:** The account of the device.
- **Current user's account:** The account of the current user. A user must be logged into the device, or the distribution package task will fail.

Using the Detection page

Use this page to detect dependent packages or applications that weren't installed through Management Suite. A match on one or more criteria prevents dependent packages from installing. This page doesn't affect the primary package. You can use these detection methods:

- File exists
- File version

- File size and/or checksum
- File date
- Registry key exists
- Registry value exists
- Matching registry value

You can add multiple criteria. When you select a criteria from the list, the options for that criteria appear below the list. Enter the necessary information and click **Add**. Repeat as necessary.

Using the Uninstall Association page

Use the Uninstall association page to associate an uninstall package to a software deployment policy package. This will automatically uninstall the software from the client when the machine or user is removed from the target list or query. **Note:** Uninstall packages are only used with policy-based deployment.

- **Type:** Select the type of package you want to use to uninstall the package. The Available distribution packages list will display only the packages of the type you specify.
- **Current:** The currently selected package.

Using the SWD package options page

Use this page to set what happens when an SWD package is already installed on a device. If you have applications that aren't responding to a normal package heal, the full reinstall option might work better. Healing tends to take less time than a full reinstall.

When you create an SWD package, you can create it with or without a package installation interface that users see. If the package has an interface, you can choose whether the package installation status dialog appears on top of their existing applications or whether there should be a solid blue installation background that masks the desktop while the package is installing.

- **Heal (repair) the package:** This option only updates registry keys and replaces program files that the agent detects as different than those in the installation package.
- **Perform a full reinstall of the package:** This option completely reinstalls the package, replacing all files and recreating all registry keys.
- **When feedback is enabled, override the above setting and let the user decide:** Allows users to choose between heal or reinstall. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.
- **When feedback is enabled, display the background screen:** Displays the solid blue background screen. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.

Using the Delivery methods dialog

The **Delivery methods** dialog (**Tools | Distribution | Delivery methods**) defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push or policy-based distributions. Don't create a delivery method every time you want to distribute a package. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.

Before using this dialog, create the distribution package (**Tools | Distribution | Distribution packages**) that you want to deliver.

About the Description page

Use this page to describe the delivery method you're creating and to set the number of devices you want to distribute to simultaneously.

- **Name:** The name for your delivery method.
- **Owner:** The name of the person who originally created the package. You can't change this field.
- **Description of delivery method:** The description you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Number of computers for distribution:** Controls the maximum number of devices that can simultaneously receive the software distribution.

About the Network usage page

Use this page to control how the package and package files are sent to managed devices. You have these options:

- **Use multicast to deploy files:** Uses LANDesk Targeted Multicast to send files to multiple devices simultaneously.
- **Use run from source to deploy files:** Doesn't copy files locally before installing them. Instead, the primary package file is executed directly from the package download location. This option works with all package types on UNC package shares. For HTTP shares, this option only works with SWD and MSI package types. You can use this option with application installs that require a specific folder structure. This option will use preferred servers, but it won't try running the package from a peer.
- **Use download from source to deploy files:** Each device downloads package files from the package server before using them. This option doesn't take advantage of Targeted Multicast.

About the Bandwidth page (under the Network usage page)

Use this page to control the network bandwidth that the package requires for deployment. You don't have to select any of these options if you want all selected devices to receive the package regardless of their bandwidth.

Bandwidth control is important for devices that have a slow WAN or a dialup connection. You usually won't want to deploy a multi-megabyte package to devices on slow links. Choose from the following options:

- **Require a non-RAS network connection:** This option enables the bandwidth requirement. Select one of the following:
 - **Allow any non-RAS network connection:** This option enables WAN and LAN devices to receive the package.

- **Only allow a high-speed network connection:** This option enables only LAN devices to receive the package.
- **Limit remote downloads (per subnet) to one device at a time:** Use this to reduce the network bandwidth consumed on a subnet.
 - **Maximum percentage of bandwidth to use:** When you've selected limit remote downloads, you can further limit bandwidth by adjusting the maximum percentage of the target device's network bandwidth to use for the distribution.

If you're using PDS to detect network connection speed, high-speed and low-speed connections return the same information. For accurate detection of high-speed network connections, you need to use ICMP.

ICMP sends ICMP echo requests of varying sizes to the remote computer and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. However, not all routers or computers support forwarding or responding to ICMP echo requests. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup) connections.

If your network isn't configured to allow ICMP echo requests, you can select PDS. If you're using PDS, the **Only allow a high-speed network connection** option won't give you accurate control.

About the Download page (under the Network usage page)

Use this page to configure bandwidth throttling and packet delays.

- **Peer download (only install from cache or peer):** Only allow packages to download if they are in the local cache or on a peer in the same multicast domain. This option conserves network bandwidth, but for the package installation to be successful, the package must be in one of these two places.
- **Dynamic bandwidth throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage to use** at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. This option forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you're reinstalling or repairing an SWD package or an MSI package, you may not want to use the **Dynamic bandwidth throttling** option because these package types normally only download the files they need.
- **Minimum available bandwidth percentage to use:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the device. For example, if there were one other application consuming network bandwidth on the device during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the device application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.

- **Delay between packets when downloading from a peer:** This option specifies the delay between packets for peers on the same subnet. You can use this delay to force distributions to be faster or slower. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.
- **Delay between packets when downloading from the source:** Specifies the delay between the package source and device destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

About the Multicast domains page (under the Network usage page)

This page appears only when you've selected Multicast as the distribution type. Use this page to configure multicast options.

- **Use multicast domain discovery:** Use this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
- **Use multicast domain discovery and save results:** Use this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
- **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery and save the results.
- **Domain representatives wake up devices:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the Multicast Options dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Number of seconds to wait for Wake On LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About domain discovery

Domain discovery is only necessary on networks with subnets that can see each other's multicast traffic. If your subnets don't see each other's traffic, you can save time by first saving the results of a domain discovery and then selecting **Use results of last multicast domain discovery** so Targeted Multicast doesn't do a domain discovery before each job.

If your network subnets do see each other's multicast traffic, you can help Targeted Multicast work faster by pre-discovering your domains with the `multicast_domain_discovery.ini` script included in the `ManagementSuite\Scripts` folder. This script doesn't do anything on target devices. Run this script from the **Scheduled tasks** window against a target list that spans your network. This will save the domain discovery results for future use. You may want to run this script periodically before large sets of multicast distributions.

If you selected **Use cached file** in **Configure | Services | Multicast**, Targeted Multicast will go through a discovery process even if you selected **Use results of last multicast domain discovery**. Targeted Multicast needs to do this to find out which potential multicast domain representatives have the file in their cache.

About the Multicast limits page (under the Network usage page)

Use this page to configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time. The default is 5.
- **Maximum number of devices that failed multicast to process simultaneously:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the scheduled task handler would process no more than 20 computers at a time that failed the multicast. The scheduled task handler will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the scheduled task handler won't perform the distribution portion of the task for any computer that failed multicast. The default is 240.
- **Number of days the files stay in the device's cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged. The default is 2.
- **Number of days the files stay in cache on multicast domain representatives:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged. The default is 14.

About the Multicast packet timing page (under the Network usage page)

Use this page to configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets. This value is only used when the representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN. The default is 1.
- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above. The default is 200.

About the Reboot page

Use this page to configure whether the computer is rebooted after the software has been installed or removed. You have three options:

- **Never reboot:** Devices won't reboot after a package installation. If you select this setting and your package requires a reboot, devices may encounter errors running the application until they do reboot. If the package is an SWD package, this option overrules any settings in the package. If the package is a generic executable or an MSI package, the package setting may overrule this option.
- **Reboot only if needed:** Devices will reboot if the package requires it.
- **Always reboot:** Devices will reboot regardless of whether the package requires it or not.

About the Feedback and timing page

Use this page to help determine how much the user sees during the installation or removal of the software. You have these options:

- **Hide all feedback from user:** This option hides the installation from the user as much as the software distribution package allows. If you created the software distribution package to be silent, this option ensures that it will be silent. If the software distribution package has been created with user-interaction, this option can't guarantee that all user-interaction will be eliminated.
- **Display progress to user:** This option enables you to choose one of the following:
 - **Allow user to cancel:** This option enables the user to cancel the action: either an installation or removal. Generally, for application policies, this isn't recommended.
 - **Display full package interface:** This option controls whether the package installs silently (disabled) or if it prompts the user for feedback when necessary (enabled).
 - **Show successful or failed status to end user:** When checked, displays a dialog after the package installs that shows whether the install succeeded or failed.
- **Run the package immediately:** Installs the package immediately without allowing any deferral options.
- **Allow the user to delay running the package:** Enables deferral options so users can delay package installations. This can help users who are in the middle of a task that a package installation might interfere with.
 - **Delay until next login automatically:** When checked, package installation is delayed until the next login without prompting users. After the next login, users will see the deferral dialog if you check **User selects how long to delay**.
 - **User selects how long to delay:** This option is disabled unless **Display progress to user** is selected. Checking this option enables the **More deferral options** page.

About the More deferral options page (under the feedback and timing page)

Use this page to configure package deferral limits and timeout options. The options on this page are enabled by clicking **User selects how long to delay** on the **Feedback and timing** page. You have these options:

- **Amount of time user can defer the package:** Select the number of hours, minutes or seconds that packages will be deferred if the user clicks **Wait** in the deferral dialog.
- **User deferral is limited:** When checked, limits the number of times users can click **Wait** when the deferral dialog appears.
 - Number of times user can delay: The delay limit.
- **Wait for user response before continuing:** When selected, the deferral dialog appears and waits for user response, regardless of the deferral time you specified. If users wait too long to respond or nobody is at the computer, the task can time out and fail.
- When user feedback is expected you will be able to choose the default action to take from a dropdown list. Click the radio button beside the dropdown list and select **Cancel**, **Run the package**, or **Delay**. You can then enter the amount of time the deferral dialog waits for a response before completing the action you selected.
 - **Amount of time before install/removal starts automatically:** The amount of time before the dropdown list's action is completed.

About the custom message page (under the feedback and timing page)

Use this page if you want to configure a custom message for the deferral dialog. This dialog only appears if you allow deferrals. The HTML page source for the deferral pages is on the core server in the LDLogon\html\ folder.

- **Use customized HTML pages:** Uses the HTML pages in the core server's LDLogon\html\ folder.
- **Include a custom message on the deferral dialog:** Adds text you enter (including HTML formatting) to the deferral dialog, replacing the standard text that normally gets inserted. The dialog can still show the **Wait**, **Cancel**, and **Install now** buttons with text describing what clicking each button does.

About the Deployment timing page

Use this page to control when the package is deployed after arriving at the device. You don't have to select any of these options if you want the package to be deployed as soon as you have scheduled it.

If you want your devices to have some control, you have these options:

- **Delay installation/removal until next login:** This option delays the deployment until the next time any user logs in to the computer.
- **Allow end user to delay installation/removal:** This option enables the user to delay the task. You can customize this option by configuring the following:
- **Use custom message:** If you enable this option, you can specify a custom delay message.
- **Amount of time before install/uninstall starts automatically:** This option enables you to specify how long to wait for the user to enter a delay time. The default is to wait for 60 seconds. If the user fails to interact with the request for a delay time within this specified time, the deployment begins.

About the Type and frequency of policy page

This page appears for policy-based delivery types and affects how target devices act when they receive the policy:

- **Required:** The policy-based delivery agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.
- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **As desired:** Can be installed by users at any time.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.

About the downgrade page

Use this page to configure the distribution behavior when either the target operating system or the target device agents don't support the delivery methods you've chosen. For example, if you have older Management Suite agents on devices, they may not support multicast or peer download.

OS downgrade options:

- **Downgrade functionality to level of operating system:** Allows jobs to continue, though all of the delivery method options you selected may not be active.
- **Fail if operating system cannot handle default functionality:** Job fails if the operating system doesn't support the delivery method options you selected.

Device downgrade options:

- **Downgrade functionality to level of agent:** Allows job to continue though all of the delivery method options you selected may not be active.
- **Fail if agent cannot handle default functionality:** Job fails if the agents don't support the delivery method options you selected.

About the discovery page

This page allows you to choose options for device discovery. Before the scheduled task handler can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

Discovery options:

- **UDP:** Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most Management Suite device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard LANDesk agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Number of retries:** How many discovery attempts to do.
- **Discovery timeout:** How long to wait for a response with each discovery attempt.
- **Timeout for subnet broadcasts:** How long to wait for a response to subnet broadcasts.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

About the Multicast software distribution status window

This window appears on the core when there's an active Targeted Multicast distribution happening. This window shows the following information:

- **Package URL or UNC address:** This is the location of the package you're currently attempting to distribute. This line will be updated with the current file that is being transferred.
- **Status:** A real-time report on how the distribution is proceeding or, if the distribution is complete, how well the job completed.
- **Multicast domains:** The field on top shows all of the subnets and the multicast domain representatives that are being used in the distribution. When you highlight each domain representative, the lower window displays all of the computers that are receiving their distribution from that domain representative.
Each computer in the lower window contains information on how the distribution completed on that computer. There are several information fields on the far right of each computer listed, including Packets Missed, Resend Requests, and Slowdown Requests. These fields do not contain any information until after the distribution is complete.
- **Packets missed:** Shows the number of packets that the device wasn't able to obtain from the subnet representative. If this number wasn't 0, then the distribution failed.
- **Resend requests:** Shows the number of times the device had to request that packets be resent from the subnet representative. This is a good way to gauge, for example, how busy the device was when dealing with other processes during the distribution.
- **Slowdown requests:** Shows the number of times the device had to ask the subnet representative to slow the packet stream. In this case, high numbers usually indicate that a computer is having some hardware problem that is slowing the distribution. If you have a large number of computers that have a high number of slowdown requests, you should check the Delay/Packet number on the subnet representative. There's often a correlation between the Delay/Packet number and the number of slowdown requests.

This window closes automatically after 10 seconds. If you'd like the window to remain open during the entire distribution, click **Keep dialog open** and the window will stay open until you close it manually. Keeping the dialog open will stop script execution, so make sure you close the dialog when you're done.

Creating custom scripts

If you want to create a custom script from a generic template, you can use the **Create custom script** option.

To create a custom script

1. Click **Tools | Distribution | Manage scripts**.
2. In the **All other scripts** shortcut menu, click **Create custom script**.
3. Enter a **Custom script name**. Click **OK**.
4. Your default text editor opens with a document named after the Custom script name you entered. Enter the script you want and save the document in the default path (LDMAIN\scripts).

Creating file deployment scripts

If you just want to copy files to devices, you can use a file deployment script. You can transfer any type of file, including text files, to a directory you specify on the device. File deployment scripts support Targeted Multicast.

To distribute files

1. Click **Tools | Distribution | Manage scripts**.
2. In the **All other scripts** shortcut menu, click **Create file deployment script**.
3. Enter a **Script name** and **Destination directory**. Click **Next**.
4. Enter the Multicast Domain Options you want. Click **Next**.
5. Select the files you want to deploy by selecting a **Web path** or a **File share path**, entering the path, and adding the files you want to the list box. Click **Next**.
6. Read the **Finished** page summary and click **Finish**.

The following sections describe the pages and options in the **Create file deployment script** wizard.

About the Download options page

Use this page to configure bandwidth throttling and packet delays.

- **Peer download (only install from cache or peer):** Only allow packages to download if they are in the local cache or on a peer in the same multicast domain. This option conserves network bandwidth, but for the package installation to be successful, the package must be in one of these two places. One way of using this option is to first copy the package to a device on each subnet with the **Only cache the file(s) on the computer using multicast** option earlier in the wizard.

- **Dynamic bandwidth throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage** at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. This option forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you're reinstalling or repairing an ESWD package or an MSI package, you may not want to use the **Dynamic bandwidth throttling** option because these package types normally only download the files they need.
- **Minimum available bandwidth percentage to use on client:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the device. For example, if there were one other application consuming network bandwidth on the device during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the device application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.
- **Delay between packets (peer):** This option specifies the delay between packets for peers on the same subnet. You can use this delay to force distributions to be faster or slower. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.
- **Delay between packets (source):** Specifies the delay between the package source and device destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

About the Job options page

Use this page to configure how this distribution will be deployed. If you're distributing an MSI file or generic executable, you have the option to enter any command-line options that need to be passed to the file after the multicast.

- **Script uses default distribution limit:** You can limit the number of computers Targeted Multicast distributes to simultaneously. This option uses the default value you set in the **Configure | Services** dialog's **Custom Jobs** tab under **Distribute to X computers simultaneously**.
- **Script uses custom distribution limit:** Use this option to override the default for the current job by specifying a different value.
- **Only install from cache or peer:** This option prevents target computers from going beyond their subnet to install a package. Computers will first look in their multicast cache directory and if the package isn't there, they'll check with peers on their subnet for the package. If no peers have the package, the distribution fails. This option minimizes network traffic across subnets. You can use this option after you've copied a package to each subnet with the Create Scripts page's **Only cache the file(s) on the computer using multicast** option.
- **Verify file before client install:** Generates a hash (CRC) for the package you're distributing once you finish the wizard. Devices can then use this hash value to make sure the package/file they receive isn't corrupt. Depending on the size of the package/file you're distributing, you may have to wait several minutes for the hash calculation.

- **Do not attempt task completion:** Use this option to not use the task completion feature to retry failed jobs. Normally, when task completion is installed on devices, failed jobs will be retried the next time task completion runs. Failed jobs will still be logged if you use this option.

About the Multicast domain options page

This page appears only when you've selected multicast as the distribution type. Use this page to configure multicast options.

- **Use multicast domain discovery:** Use this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
- **Use multicast domain discovery and save results:** Use this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
- **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery and save the results.
- **Domain representatives wake up computers:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the **Multicast options** dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.
- **Advanced multicast options:** Use this option to set advanced options. The defaults are fine for most jobs.

About domain discovery

Domain discovery is only necessary on networks with subnets that can see each other's multicast traffic. If your subnets don't see each other's traffic, you can save time by first saving the results of a domain discovery and then selecting **Use results of last multicast domain discovery** so Targeted Multicast doesn't do a domain discovery before each job.

If your network subnets do see each other's multicast traffic, you can help Targeted Multicast work faster by pre-discovering your domains with the `multicast_domain_discovery.ini` script included in the `LDMAIN\Scripts` folder. This script doesn't do anything on target computers. Run this script from the **Scheduled tasks** window against a target list that spans your network. This will save the domain discovery results for future use. You may want to run this script periodically before large sets of multicast distributions.

If you selected **Use cached file** in **Configure | Management Suite Services | Multicast**, Targeted Multicast will go through a discovery process even if you selected **Use results of last multicast domain discovery**. Targeted Multicast needs to do this to find out which potential multicast domain representatives have the file in their cache.

About the Multicast options dialog

The file deployment script wizard has a **Multicast options** dialog where you can configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time.
- **Limit processing of machines that failed multicast...:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the **Custom job** dialog would process no more than 20 computers at a time that failed the multicast. The **Custom job** dialog will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the **Custom job** dialog won't perform the distribution portion of the task for any computer that failed multicast.
- **Number of days the files stay in the client cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged.
- **Number of days the files stay in multicast domain representative cache:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets. This value is only used when the representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN.
- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above.
- **Number of seconds to wait after Wake On LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About the Select files to deploy page

The **Select files to deploy** page appears in the file transfer script wizard.

- **Web path:** Click for packages stored on a Web server. You must include `http://` in the URL.
- **File share path:** Click for packages stored on a null-session share on a file server. This path must follow the UNC path convention, `\\servername\sharename\`.
- **Browse:** Click **Browse** to browse for the path. If you clicked **Web path**, a small browser window opens. If you clicked **File share path**, a standard browse dialog opens. If you want to browse a Web server directory in the Select Package Location browser window, you must include a trailing slash on your URL (`/`), otherwise the browser window displays an error.
- **Add:** Click **Add** to add a program directly from the path edit box once you've entered the full path and filename.
- **Remove:** Select a file you've added and click **Remove** to remove a file from the list.

About the Finished page

This page summarizes the actions you've selected for deploying the package. Before continuing, make sure your managed devices meet all the requirements listed in the warning section.

If you click **Set as Default**, the configuration options you've selected will be set as the default values for this wizard.

Click **Finish** and you can schedule the script for distribution.

Software license monitoring help

About the Alias properties dialog

Use this dialog (from the **Aliases** tree item's shortcut menu, click **Create alias**) to create an alias for a product executable. Aliasing ensures that the scanner can correctly identify device applications if their product or vendor names have changed since being installed.

If name changes occur to your device's software, use aliasing to associate new vendor or product names with the originals. The scanner will then associate the new names with any executables that match the original information in the core server's core database, ensuring that your software is accurately identified.

This feature is most useful when monitoring product licenses in the Compliance view, ensuring that the scanner can continue to identify those products.

- **Original vendor:** Enter the name of the product's original vendor.
- **Original product name:** Enter the original product name.
- **New vendor:** Enter the new vendor name.
- **New product name:** Enter the product's new name.

About the Product properties dialog

Use this dialog (from a product's shortcut menu, click **Properties**) to view and change the following:

- "About the Product properties dialog's Product tab" on page 772
- "About the Product properties dialog's Files tab" on page 773
- "About the Product properties dialog's Downgrades tab" on page 773

About the Product properties dialog's Product tab

Use this dialog (right-click a product and click **Properties**, and then the **Product** tab) to view and change the properties with the product.

- **Product name:** Shows the name of the product you're viewing.
- **Version:** Shows the product version number.
- **Publisher:** Shows the vendor that created the product.

- **Deny use of this product:** Whether SLM is denying execution for this product on devices.

About the Product properties dialog's Files tab

Use this dialog (right-click a product and click **Properties**, and then the **File** tab) to view and change the files associated with the product.

- **Vendor, Product name, File name, Version, and Size:** Information about the files that are part of this product. If you enter file size of 1, any file with that file name matches.
- **Add:** Opens the Add files to product window, where you can select from files to add.
- **Create:** Creates a new definition for a file that you can add to the product.
- **Match all files:** Whether multiple files must be on the device before a license is counted as used.

About the Product properties dialog's Downgrades tab

Use this dialog (right-click a product and click **Properties**, and then the **Downgrades** tab) to view and change the downgrades for the product.

Software license monitoring window lets you "downgrade" licenses for certain products: if you have two versions of the same product installed on your network, you can set up the older version to borrow a license from the newer version.

The Downgrades tab is divided into two halves:

- The top half, **Downgrade licensed products**, lists the products you want to be able to borrow licenses from the current product.
- The bottom half, **Upgrade licensed products**, lists products that this product can borrow licenses from.

Use these buttons to configure downgraded licenses:

- **Add button:** Click this to specify which products can borrow licenses from the product you're configuring.
- **Remove button:** Click this to remove a product from the list.
- **Move up/down buttons:** Select a downgrade licensed product and click **Move up** or **Move down** to prioritize which product will receive the borrowed licenses.

You can't configure the amount of licenses that are borrowed or loaned in this tab. Configure licenses within a product's Product licenses dialog.

About the Add files to product window

Use this window (click the **Files** item from a product's shortcut menu, then click **Add** in the **Files** tab) to specify which files should be monitored to determine when a product is running.

- **Find:** Enter the filename or search keyword you want to look for.
- **In column:** Select the inventory column you want to search in, either Vendor, Product Name, File Name, Version, or Size.

- **Discovered but not in product:** Shows files that also appear in the **To be dispositioned** list but aren't currently being monitored in the Compliance tree. Use this list to view files that you may want to begin monitoring for license compliance and usage/denial trends.
- **To be scanned:** Shows files in your core server's LDAPPL3 that the scanner can identify on devices.
- **To be dispositioned:** Shows files that have been discovered on devices, but are unknown to LDAPPL3. You must move these files into other categories before the scanner can identify them.
- **Discovered on computers:** Shows all files that have been discovered on devices, even if they're for products that aren't defined in the LDAPPL3.
- **In monitored product:** Shows files that are already being used to monitor products.
- **File information pane:** Shows files that match your Find string and the **File list** you've selected.

About the Product licenses dialog

Use this dialog, accessed from the **Manage licenses** item on a product's shortcut menu, to view and configure the license information associated with a product.

The dialog shows this information:

- **License number, Type, and Quantity:** Details on each license you've added for this product.
- **Licenses:** Total number of licenses available for this product.
- **Out of compliance:** How many installations are exceeding the amount of licenses available.
- **Loaned:** If another product can borrow licenses from this one, how many licenses this product is loaning.
- **Installations:** The number of installations detected for this product.
- **Not deployed:** The number of licenses remaining for this product.
- **Borrowed:** If this product can borrow licenses from another, the number of licenses this product is borrowing.

About the License properties dialog

Use this dialog, accessed from the Add button on the Product licenses dialog, to add or change license information.

The **License properties** dialog has three tabs:

- License
- Purchase Info
- Tracking

Use the **License** tab to configure license properties for your product.

- **License number:** Enter a number that constitutes your product license.
- **License type:** Enter a type of license you have for the product, such as: competitive upgrade, freeware, new purchase, OEM, product upgrade, public domain, shareware, unknown.

- **Quantity:** Enter the number of product licenses purchased.
- **Serial number:** Enter an additional number that may constitute your product license.

Use the **Purchase info** tab to configure purchase properties for your product license.

- **Purchase date:** Enter a date the product was purchased by your company.
- **Unit price:** Enter a price of each purchased license for the product.
- **Order number:** Enter an order number used to make the purchase.
- **Reseller:** Enter the name of purchase place.

Use the **Tracking** tab to configure tracking properties for your product license.

- **Owner:** Enter a person or department in your company responsible for storing the boxed product.
- **Location:** Enter a physical location where the boxed product is stored.
- **Note:** Enter any additional information associated with the product license, such as downgrade rights.

About the Group properties dialog

Use this dialog (from a product group's shortcut menu, click **Properties**) to view and change the following:

- [Groups](#)
- [Scopes](#)
- [Devices](#)

About the Group properties dialog's Group tab

Use the **Group** tab to edit a group's name.

About the Group properties dialog's Scopes tab

Use the **Scopes** tab to add a scope to a group. For more information on scopes, see "Using scopes with products" on page 204.

The tab lists the scopes that currently apply to products under this group. To add a scope, click **Add** and click the scope you want. If you add a scope, make sure in the Scopes tab that you remove the **Default All Machines** scope. Deleting this allows the newly selected scope to be applied.

Click the **Refresh** toolbar button and verify the scope is working the way you want it to.

About the Group properties dialog's Devices tab

Use the **Devices** tab to see the devices that are part of the scopes defined for the group. Click **Resolve** to populate the list.

About the File Properties dialog

Use this dialog (click **Inventory | Files >** and the **To be scanned** or **To be dispositioned** category, then click the **New File** toolbar button) to add files to an LDAPPL3 category.

- **Browse button:** Use this button to directly select a file. Selecting a file this way fills in the Filename and Size fields for you.
- **Filename:** Browse for or enter a filename.
- **Size (in bytes):** Enter the file's size in bytes. Don't use commas or other separators between the digits. If you enter file size of 1, any file with that file name matches.
- **Product name:** Enter the product name the file belongs to.
- **Vendor:** Enter the vendor name for the product that uses the file.
- **Version:** Enter a version name for the file.
- **Action or state:** Select what you want done with the file:
 - **To be scanned:** Add the file to this category to have the inventory scanner look for it on devices.
 - **To be dispositioned:** Add the file to this category if you want to decide later what you want to do with the file.
- **Scan method:** Since you're editing LDAPPL3 file properties, you can't change the scan method.

About the Deny file dialog

Use this dialog (click **Inventory | Files**, and from the shortcut menu for **To be denied**, click **New file**) to add a file that you want to deny access to. You can only deny access by filename.

Unmanaged Device Discovery help

The LANDesk Unmanaged device discovery (UDD) tool is accessed from the main LANDesk console (**Tools | Configuration | Unmanaged Device Discovery**). This tool provides a way for you to find devices on your network that haven't submitted an inventory scan to the LANDesk core database. UDD has multiple ways of finding unmanaged devices. This tool also provides Extended device discovery (XDD), which relies on a device agent that listens for network ARP and WAP broadcasts. The extended device discovery agent on a device then checks discovered devices for the LANDesk agent. If the LANDesk agent doesn't respond, extended device discovery displays the device in the **Computers** list. Extended device discovery is ideal in situations involving firewalls that prevent devices from responding to the normal ping-based UDD discovery methods.

The "Unmanaged device discovery" on page 216 chapter introduces this tool. In that chapter you'll find overview information, as well as step-by-step instructions on how to use all of the tool's features.

This chapter contains the following online help sections that describe the Unmanaged device discovery tool's dialogs. From the console interface, these help sections are accessed by clicking the **Help** button on their respective dialog

About the Scanner Configuration dialog

Use this dialog to customize and launch unmanaged device scans. To access this dialog, at the **Unmanaged device discovery** tool windows, click the **Scan network** toolbar button.

- **Saved configurations:** Shows the saved scanner configurations. Save a configuration by changing the settings you want, clicking **New**, naming the configuration, and with your new configuration selected, clicking **Save**.
- **CBA discovery:** Discovers devices with the CBA agent running. If your devices have CBA, this is the fastest discovery method.
 - **PDS2 discovery:** Discovers devices using the older LANDesk PDS2 agent. You can only select this option if you select **CBA discovery** first.
- **Network scan:** Discovers devices using an ICMP ping sweep. This is the most thorough and slowest discovery method.
- **NT domain:** Discovers devices in a Windows NT domain. This option uses the NT domain account information and doesn't require an IP address range, though you can specify one. Selecting this option and clicking **Configure** shows the **NT domain configuration** dialog where you can customize the NT domain discovery settings.
- **Filter by IP range** (for both NT domain and LDAP): Filters NT domain and LDAP discovery by the IP ranges specified in **Starting IP** and **Ending IP**.
- **LDAP:** Discovers devices in an LDAP directory. Selecting this option and clicking **Configure** shows the **LDAP configuration** dialog where you can customize the LDAP discovery settings.
- **IPMI:** Looks for servers enabled with Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.

- **Intel* AMT:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel AMT** folder.
- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan. UDD automatically updates this field as you type the **Starting IP**, but you can change the ending IP address manually. **Ending IP** is calculated using the value of **Subnet mask** + what is typed in **Starting IP**.
- **Subnet mask:** Enter the subnet mask for the IP address range you're scanning.
- **Add and Remove:** Adds or removes your IP address ranges from the work queue at the bottom of the dialog.
- **Schedule task:** Schedules the scan based on your settings. You can customize the start time in the **Scheduled tasks** window. Scheduled scans originate from the core server.
- **Scan now:** Starts the scan immediately based on your settings. Scans started here originate from the console you're at. Once you start the scan, a **Scan status** dialog appears showing the total number of devices found, how many existing devices were updated, and how many new unmanaged devices were added.

About the NT domain configuration dialog

Use this dialog to configure how you connect to the domain you want to scan.

- **Domain:** Enter the domain you want to scan.
- **Logon as current user:** Select this if you're logged in as a user with access to the domain you're scanning.
- **Logon as:** Select this if you aren't logged in as a user with access to the domain you're scanning. Also enter a **User name** and a **Password**.
- **Add and Remove:** Add each domain you configure and want to scan to the work queue by clicking **Add**. Click **Remove** to delete the selected domain from the work queue.

About the LDAP configuration dialog

Use this dialog to configure how you connect to the LDAP directory you want to scan.

- **LDAP://:** Enter the LDAP directory you want to scan.
- **Logon as current user:** Select this if you're logged in as a user with access to the directory you're scanning.
- **Logon as:** Select this if you aren't logged on as a user with access to the directory you're scanning. Also enter a **User name** and a **Password**.
- **Select individual OUs:** Select the OUs that you want to scan. Click **Add** to add them to the work queue. Click **Remove** to delete the selected OU from the queue.
- **Active directory path:** Shows the active directory path, if applicable.

Configuring SNMP scans

Network scan discoveries can use SNMP. Depending on your network's SNMP configuration, you may need to enter additional SNMP information in UDD. Clicking **Configure** next to the **SNMP** option shows the **SNMP configuration** dialog, which has these options:

- **Retries:** How many times UDD retries the SNMP connection.

- **Wait for response in seconds:** How long UDD should wait for an SNMP response.
- **Port:** What port UDD should send SNMP queries to.
- **Community name:** The SNMP community name UDD should use.
- **Configure SNMP V3:** UDD also supports SNMP V3. Click this button to configure SNMP V3 options in the **SNMP V3 configuration** dialog.

The **SNMP V3 configuration** dialog has these options:

- **User name:** The username UDD should use to authenticate with the remote SNMP service.
- **Password:** The password for the remote SNMP service.
- **Authentication type:** The authentication type SNMP is using. Can be **MD5**, **SHA**, or **None**.
- **Privacy Type:** The encryption method the SNMP service is using. Can be **DES**, **AES128**, or **None**.
- **Privacy Password:** The password to use with the specified privacy type. Not available if you selected a privacy type of **None**.

About the ARP (or WAP) Discovery Settings list dialog

Use this dialog to manage your ARP and WAP settings that are used for extended device discovery. Once configured, you can apply XDD settings to scan tasks.

This dialog contains the following options:

- **New:** Opens the settings dialog where you can configure the discovery method options.
- **Edit:** Opens the settings dialog where you can modify the selected setting.
- **Copy:** Opens a copy of the selected setting as a template, which you can then modify and rename. This is useful if you want to make minor adjustments to settings and save them for a specific purpose.
- **Delete:** Removes the selected setting from the database.

Note the selected setting may currently be associated with one or more tasks or managed devices. If you choose to delete the setting: devices with that setting still have it and continue to use it until a new agent configuration task is deployed; scheduled tasks with that setting still run on target devices, as do local scheduler tasks with that setting, until a new configuration is deployed.

- **Close:** Closes the dialog, without applying a setting to the task.

About the Configure ARP Discovery Settings dialog

Use this dialog to customize ARP-based extended device discovery scan settings.

- **Configuration name:** Identifies the setting with a unique name. This name appears in the settings drop-down list on the settings list dialog.
- **Duration ARP entry stats cached (in seconds):** How long devices with the extended device discovery agent keep an address in the ARP table. Devices in the ARP cache won't be pinged after the initial discovery ping. The default is 24 hours (86,400 seconds). The minimum value is 900 seconds.

- **Maximum delay before pinging an unknown device for the LANDesk agent (in seconds):** When a new ARP is recognized by a device with the extended device discovery agent, the device waits two minutes for the detected device to boot and then waits a random amount of time within the value you specify here. The agent with the shortest random wait will ping first and then UDP broadcast to the subnet that it took care of the ping for that device. If you have multiple extended device discovery agents installed, this prevents devices from generating excess traffic by all pinging at the same time. If you set this too high, unmanaged devices may leave the network before they can be pinged. If you set this too low, multiple agents may ping and report the same device. The default is one hour (3,600 seconds).
- **Frequency the cached ARP table is refreshed (in seconds):** How often the device writes the ARP cache to disk so the data isn't lost in case the device shuts off, crashes, or reboots. The default value is five minutes (300 seconds).
- **Logging level:** The local extended device discovery logging level for errors (1), warnings (2), everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xddclient.log.
- **Force logging level:** Overrides the log level setting from the core server. If you clear this option, you can set the log level manually on a particular device. This can be useful for troubleshooting a particular device without having to change the log level on all devices. This is enabled by default.
- **Extended device discovery is enabled:** When cleared, turns off XDD on all devices. The next time an extended device discovery-enabled device checks with the core for an extended device discovery configuration update, this setting takes effect. Even when discovery is disabled, the agent still checks with the core for configuration updates. This is enabled by default.

About the ARP discovery history dialog

Use this dialog to configure how the core server maintains the ARP discovery history. This history data is used for generating extended device discovery reports. The options in this dialog don't affect the discovered devices you see in the main unmanaged device discovery window. This history only applies to devices that were discovered through ARP discovery and that don't have LANDesk agents on them.

- **Maintain history for this period of days:** Clicking this option allows you to specify how many days of ARP discovery history data you want to save in the database. ARP discovery history data older than the number of days you specify will be deleted from the database during maintenance.
- **Clear entries manually:** This is the default. The ARP discovery history won't be deleted during maintenance.
- **Clear all entries now:** Click this button to immediately delete the ARP discovery history from the database.

About the Configure WAP Discovery Settings dialog

Use this dialog to configure WAP-based extended device discovery scan settings.

This dialog contains the following options:

- **Configuration name:** Identifies the setting with a unique name. This name appears in the settings drop-down list on the settings list dialog.
- **Frequency of WAP scan (in seconds):** Specifies how often the extended device discovery agent scans for WAP points.
- **Logging level:** The local extended device discovery logging level for errors (1), warnings (2), everything (3). The default level is 1- errors only. Logs are stored locally in C:\Program Files\LANDesk\LDClient\xddclient.log.
- **Force logging level:** Overrides the log level setting from the core server. If you clear this option, you can set the log level manually on a particular device. This can be useful for troubleshooting a particular device without having to change the log level on all devices. This is enabled by default.