LANDesk® System Manager 8.7

Installation and Deployment Guide

LANDesk®

v8.5

Contents

Overview

This guide walks you through the process of installing and deploying LANDesk® System Manager, a product that helps reduce the total cost of ownership by making it easier to manage a computer and troubleshoot common computer problems.

Here's what you'll learn about in this overview:

What's in this release

With the growth of the computer industry, computer systems have become more complex and difficult to manage. The time spent maintaining and repairing a computer through its years of operation can increase its Total Cost of Ownership (TCO) far beyond the initial purchase price. LANDesk® System Manager can help reduce TCO by making it easier to manage a computer and troubleshoot common computer problems.

- **View system inventory:** System Manager provides extensive information about the computer's hardware and software configuration.
- **Monitor a computer's health:** System Manager reports when the computer is in a warning or critical health state, reporting on items such as temperature, voltage, free memory, and disk space.
- **Receive alerts for system events:** System Manager can use various alert methods to notify you of problems.
- **Monitor real-time or historic performance:** System Manager lets you monitor the performance of various system objects such as drives, processors, memory, and services. You can set alert actions to trigger notification when a specified counter crosses an upper or lower threshold a predetermined number of times.
- **Monitor current processes and services:** System Manager allows you to view current services and their statuses, or to set alert actions to notify you of changes to service status.
- **Remotely power off, power on, and reboot computers:** System Manager enables remote power management from the administrator console for systems that support it.
- **Scheduled task view:** View or reschedule all agent deployment, discovery,
- **Enhanced OS support:** Manage all devices in your heterogeneous environment from a single console. Supports Windows 2000, 2003, and XP Professional, Red Hat Linux, SUSE Linux, HP-UX, and AIX. See Phase 1: System requirements for more information.
- **Intel* AMT and Intelligent Platform Management Interface (IPMI) support:** System Manager supports hardware-based management components that provide the ability to remotely manage networked devices in any system state through out-of-band (OOB) communication. As long as the device is connected to a corporate network and has stand-by power, you can access inventory, view remote diagnostic information, and remotely reboot the system.

- **Blade server support:** Support for blade servers and blade chassis management modules (CMMs) including both management and inventory functions.
- **Scripting tool:** You can schedule and execute custom tasks on devices
- **Task scheduler:** A single database schema with improved data integrity and scalability allows you to access a rich set of information about managed devices (including full integration with Management Suite). Part of this single schema is the task scheduler. You can now view all tasks (discovery, agent configuration, in a common window. From this window, you can reschedule, modify the schedule, or make the schedule to be recurring.
- **Role-based administration:** Configure user access to tools and network devices based on user administrative role in your organization. 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.
- **Unmanaged device discovery:** Discover devices on your network though a variety of methods. The product identifies servers running Windows or Linux, blade servers and blade chassis, IPMI-enabled servers, Intel AMT-enabled servers, as well as other network devices. Schedule device discovery so you can constantly be aware of new devices. You can also generate reports on the unmanaged devices on your network.
- **Enhanced security:** A certificate-based security model allows devices to communicate only with authorized core servers and consoles.
- **Software distribution:** Automate the process of installing software applications or distributing files to devices.
- **Reports:** Predefined service reports are available for planning and strategic analysis.
- **Scheduled task support:** Provide multiple logins for the scheduler service to authenticate with when running tasks on devices that don't have agents. This is especially useful for managing devices in multiple Windows domains.

Product basics

System Manager manages devices running several different operating systems, including Windows 2000 Pro SP4, Windows XP Pro SP1, Windows* 2000/2003 servers, Red Hat Enterprise Linux v3 servers, SUSE Linux 9 servers, HP-UX and AIX servers, and it provides a common interface for managing the devices of these network operating systems. It can co-exist with other LANDesk products, too, such as LANDesk® Management Suite and LANDesk® Server Manager.

Product terms

- **Core server:** The center of a management domain. All the product's key files and services are on the core server. A management domain has only one core server. A core server can be a new server or a repurposed server.
- **Console:** The browser-based console that is the main product interface.
- Core database: The product creates an MSDE database on the core server to store management data.
- **Managed devices:** Devices in your network that have product agents installed. "Devices" include desktop computers, servers, laptop/mobile computers, blade chassis, and so forth. A core server can manage thousands of devices.
- **Public:** Items (such as groups, distribution packages, or tasks) that are visible to all users. When a user modifies a Public item, the modification remains Public. Public groups are created by a user with Administrator rights.

- **Private or User:** Items that are created by the currently logged-in user. They are not visible to other users. Private or User items appear under the **My delivery methods**, **My packages**, and **My tasks** trees. Users with Administrator rights can see Private groups and User packages and tasks.
- **Common:** An item visible to other users. When a user assumes ownership of a Common item (by modifying it), the item branches into two items: the Common item remains, and a User item is saved in the Users folder. The User instance of the item is no longer visible to other users. A user can mark any task that is visible to them as Common, thus sharing it with other users. Once a user clears the Common option of the item's properties, the task is only visible in the user's User tasks group.

How does the product fit into my network?

This product uses the infrastructure of your existing network to establish connections with the devices it manages. The job of managing your existing devices is greatly simplified, whether you manage a small network or a large enterprise environment.

Using System Manager with Management Suite or Server Manager

If you have System Manager and wish to use it with Management Suite or Server Manager, you must use the core server activation utility to provide a valid user name and password for the product with which you want to use System Manager. A System Manager / Management Suite installation gives you three consoles to work with: the Management Suite Windows 32 and Web consoles, and the System Manager Web console. The Server Manager console includes three navigation items (Alerting, Monitoring, and Logs) that contain functionality that cannot be found in the Management Suite two consoles.

If you deploy Management Suite, the Management Suite installation removes the System Manager agent on managed devices, and vice-versa. When running Management Suite with System Manager, the Management Suite configuration feature includes monitoring options.

Installing System Manager with Management Suite or Server Manager already installed

If you already have Management Suite or Server Manager installed on your core server and want to add System Manager, you use the same installation you did for the original Management Suite or Server Manager installation.

1. Open autorun.exe.
2. Click **Install Now**.
3. Select a language, and click **OK**.
4. The Welcome screen displays. Click **Next**.
5. Select **Modify** (if necessary) and click **Next**.
6. Click LANDesk® System Manager, and click **Next**.
7. Follow the screen instructions of the wizard.

Core server system requirements

As you consider which server you'll set up as your core server, review these system requirements and confirm that your server meets or exceeds the requirements listed in Phase 1: System Requirements. The pre-requisite checker does this for you automatically.

A dedicated core server is strongly recommended
Because of the traffic that passes through the core server to manage your domain, we strongly recommend that each core server is dedicated to hosting the product.

If you install other products on the same server, you may experience short- and long-term resource issues.

Don't install the core server components on a primary domain controller, backup domain controller, or Active Directory controller.

Installation and deployment strategies

When installing using the Autorun from the product media, the installation program automatically verifies that your core complies with these requirements before installation. Installing and deploying a system-wide application to a heterogeneous network requires a deliberate methodology and significant planning *before* you run the setup program. This guide includes strategies for setting up the product. Before deploying it, you need to briefly characterize your management needs.

Deployment strategy considerations

Deployment is the process of expanding your management capabilities to servers that you want to include in the domain. In this guide, deployment is discussed in "phases."

The phased deployment strategy offers you a structured approach to enabling management on devices. This approach is based on two simple principles:

- First, deploy those product components that have the least impact on your existing network and progress to those components that have the most impact.
- Second, deploy the product in well-planned stages, rather than deploying all services at once, which may complicate any required troubleshooting.

This guide is organized sequentially to help you deploy the product. Begin with the first chapter, "Phase 1: Designing your management domain" later in this guide. You should then continue sequentially through each phase.

Overview of installation and deployment

This guide groups installation and deployment tasks into the following phases. Each phase has a corresponding section in this guide that walks you through that part of the installation. The chapter is designed to help you start using the product quickly by configuring services, running the console, discovering devices, moving the devices into the My devices list, and configuring the

managed devices for actions. It is designed to be succinct, assuming that you will consult the rest of the book for detail. Some of the procedures in this guide are repeated in the Getting started chapter.

Phase 1 summary

During phase 1 of the installation, you design your management domain by completing these tasks:

- Gather network information
- Confirm that your network meets system requirements

For details, refer to "Phase 1: Designing your management domain" later in this guide.

Phase 2 summary

During phase 2, you install the product by completing these tasks:

- Install the core server

For details, refer to "Phase 2: Installing the core and console" later in this guide.

Phase 3 summary

During phase 3 of the installation, you discover devices on your network and deploy the product agents. You can push the agents from the console or pull them from the server share.

For details, refer to "Phase 3: Deploying the agents to devices" later in this guide.

Getting started

Overview

Welcome to LANDesk® System Manager, a stand-alone device management application that maximizes your valuable time by letting you quickly and efficiently manage your devices, thus saving you and your organization time and money. System Manager lets you manage your devices in a central location, group them for actions (such as power cycling, vulnerability assessments, or configuring alerts), remotely troubleshoot any problems, keep your network secure, and keep your devices updated with the latest patches.

This guide's purpose is to help you start using System Manager quickly. Setting up the product for first-time use requires several key steps, including: configuring services, running the console, discovering devices, moving the devices into the **My devices** list, and configuring the managed devices for actions.

System Manager is a Web application, allowing you to access it using your browser so you can manage your servers from a remote workstation. It behaves like many of the Web applications which you are accustomed to, but it also contains several advanced Windows-type controls to enhance your usability experience. For example, you can hover the mouse pointer over a control and then double-click it or right-click it (just as you would in a Windows application). For example, in the **My devices** list, you can double-click a device name to access its specific information, or right-click to see available actions.

The steps below guide you through getting System Manager up and running, discovering devices on your network, selecting the servers to move to your **My devices** list, deploying agents, and then targeting those devices for various tasks.

Running the installation program

During the install, on the Autorun page, select LANDesk® System Manager. Specific installation instructions can be found in Phase 2 of the *Installation and Deployment Guide*.

After you have installed System Manager, you are ready to start using it. The sections below tell you how to complete several required tasks: running the core activation utility, configuring

services, discovering computers, specifying which devices to actively manage by moving the devices the **My devices** list, grouping devices, adding users, and deploying agents. Once these tasks are completed, you are ready to begin exploring how the robust feature set of System Manager can help you manage your devices.

Activating the core server

You won't be able to run the product until you have activated the core server. Activating the core server ensures your product is a valid, licensed copy.

Use the Core Server Activation utility to:

- Activate a new System Manager core server for the first time
- Update an existing System Manager core server

Each core server uses a unique authorization certificate.

This utility runs automatically on the first reboot.

With your core server connected to the Internet,

1. Click **Start | All Programs | LANDesk Core Server Activation**. The username and password are filled in.
2. Click **Activate**.

The core communicates with the Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, System Manager communicates with the license server automatically not requiring any intervention by you. If the core is not connected to the Internet, follow the on-screen instructions and email the authorization file to licensing@landesk.com for manual activation.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any changes made manually to this file will invalidate the contents and the next usage report to the Software licensing server.

- The Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.
- You can also activate the core server or update the node count by e-mail. Send the file with the .TXT extension located under Program Files\LANDesk\Authorization to licensing@landesk.com. LANDesk customer support will reply to the e-mail with a file and instructions on copying the file to the core server to complete the activation process.

Adding users

System Manager users can log in to the console and perform specific tasks for specific devices on the network. You manage users through the role-based administration feature. Role-based administration lets you assign product users special administrative roles based on their rights and scope. *Rights* determine the product tools and features a user can see and utilize. *Scope*

determines the range of devices a user can see and manage. You can create a variety of users and customize their rights and scope to fit your management requirements. For example, you can create a user who fills the Help Desk role by giving this user the rights necessary for this role, such as allowing the user to remote control certain devices on the network. More detail is available in the Role-based Administration chapter of the System Manager *Users Guide*.

When you install the product, two user accounts are automatically created (see below). If you want to add more users, you can do so manually by adding new users to the local LANDesk Management Suite group on the core server. System Manager Users appear (click Users in the left navigation pane) after they have been added to the LANDesk Management Suite group on the core server. Once created, click Users in the Web console to view current users and to modify each user's rights and scope.

There are two default users in the Users group. One of the users is the Default Administrator. This is the administrative user who was logged in to the server when the product was installed.

The other default user is the Default Template User. This user contains a template of user properties (rights and scope) that is used to configure new users when they are added to the Management Suite group. In other words, when you add a user to that group in the Windows NT environment, the user inherits the rights and scope currently defined in the Default Template User properties. If the Default Template User has all rights selected and the Default All Machines Scope selected, any new user placed in the LANDesk Management Suite group will be added to the Users group with rights to all of the product tools and access to all devices.

You can change the property settings for the Default Template User by selecting it and clicking Edit in the Web console. 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 (see steps below). The Default Template User cannot be removed.

When you add a user to the local Windows group LANDesk Management Suite, The user's name, scope, 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 ONLY an Administrator can view User groups).

Conversely, if you remove a user from the LANDesk Management Suite group, the user no longer appears in the Users list. The user's account still exists on the core server and can be added back to 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.

Refresh the Users frame in the System Manager console by pressing **F5**. To learn how to add a user or domain group to the LANDesk Management Suite group or how to create a new user account, please see "Adding Product Users" in the Role-based Administration chapter of the System Manager *User's Guide*.

To add a user or domain group to the LANDesk Management Suite group

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. Click **Add**, then type or select a user (or users) from the list.

4. Click **Add**, and then **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.

If user accounts do not already exist on the server, you must first create them on the server.

To create a new user account

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.

Add the user to the LANDesk Management Suite group to have them appear in the Users group in the console.

Configuring services and credentials

To securely manage devices on your network, you must provide System Manager with the necessary device credentials. Use the Configure Services utility on the core (SVCCFG.EXE) to specify the required operating system, Intel* AMT, and IPMI BMC credentials. You can also specify additional settings, such as inventory defaults, PXE holding queue settings, and LANDesk database settings.

Use Configure Services to configure:

- The database name, user name, and password. (Set at installation time.)
- Credentials for scheduling jobs to the managed devices. (You can enter more than one set of administrator credentials.)
- Credentials for configuring IPMI BMCs. (You can enter only one set of BMC credentials.)
- Credentials for configuring Intel AMT-enabled devices. (You can enter only one set of Intel AMT credentials.)
- Server software scan interval, maintenance, days to keep inventory scans, and login history length.
- Duplicate device ID handling.
- Scheduler configuration, including scheduled job and query evaluation intervals.
- Custom job configuration, including remote execute timeout.

1. At the core server, click **Start | All Programs | LANDesk | LANDesk Configure Services**.
2. Click the **Scheduler** tab.
3. Click the **Change Login** button.
4. Enter the credentials you want the service to use on the managed devices, typically a domain administrator account.
5. Click **Add**. Add additional credentials as necessary, if the managed devices do not all have the same administrator user name accounts enabled.

6. Click **Apply**.
7. If you have IPMI-enabled servers in your environment, click the **BMC Password** tab. Type a password in the **Password** text box, retype the password in the **Confirm password** text box, then click **OK**. (All managed IPMI servers must share the same BMC user name and password.)
8. If you have Intel AMT-enabled devices, click the **Intel AMT Configuration** tab. Type the currently configured Intel AMT user name in the **User name** text box and the currently configured password in the **Password** text box. Retype the password in the **Confirm password** text box, then click **OK**.
9. Set any other settings as desired, such as software scan intervals.
10. Click **OK** to save the changes.

Click **Help** on each Configure Services tab for more information.

Running the console

System Manager includes a full range of tools that let you view, configure, manage, and protect the devices on your network. The console is the entry point by which you can use these tools.

The top pane in the console displays the server you are logged in to and the user you are logged in as. The **My devices** list is the main window of the console and is the starting point for most functions. The left-hand pane shows available tools. The right-hand pane in the console displays dialogs and screens which allow you to complete management tasks.

The convenience of the console is that you can perform all of its functions from a remote location, such as your workstation, freeing you from the need to take additional trips to the server room or to go to each managed device individually to perform routine maintenance or troubleshoot problems.

Launch the console one of three ways:

- On the core server, click **Start | All Programs | LANDesk | System Manager**.
- In a browser at a remote workstation, type the URL http://coreserver/LDSM.

Discovering devices

Use the **Discovery configurations** tab to create new discovery configurations, edit and delete existing configurations, and schedule a configuration for discovery. Each discovery configuration consists of a descriptive name, the IP ranges to scan, and the discovery type.

Once you create a configuration, use the **Schedule discovery** dialog to configure when it will run.

1. In the left navigation pane, click **Device discovery**.
2. In the **Discovery configurations** tab, click the **New** button.
3. Fill in the fields described below. When you have finished, click the **Add** button, and click **OK**.

The text below describes the parts of the **Discovery configuration** dialog box.

- **Configuration name:** Type a name for this configuration. Give the configuration a meaningful name so you can easily remember the configuration.
- **Standard network scan:** Looks for devices by sending ICMP packets to IP addresses in the range you specify. This is the most thorough search, but also the slowest. By default, this option uses NetBIOS to gather information about the device.

  The Network scan option has an **IP fingerprint** option where device discovery tries to discover the OS type through TCP packet responses. IP fingerprint requires additional discovery time while the product verifies device-specific information.

  The network scan allows you to optionally scan using SNMP. Click **Configure** to enter information about your SNMP configuration.
- **LANDesk CBA discovery:** Looks for the standard management agent (formerly known as the common base agent [CBA] in Management Suite) on devices. The standard management agent allows the core server to discover and communicate with clients on the network. This option discovers devices that have product agents on them. Routers block standard management agent and PDS2 traffic. In order to run a standard CBA discovery across multiple subnets, the router must be configured to allow directed broadcast across multiple subnets.
  The CBA discovery option also has a **LANDesk PDS2 discovery** option, where device discovery looks for the LANDesk Ping Discovery Service (PDS2) on devices. LANDesk Software products such as LANDeskSystem Manager, Server Manager, and LANDesk Client Manager use the PDS2 agent. Select this option if you have devices on your network with these products installed. CBA discovery is not supported for Linux machines, but if you choose PDS2, Linux machines with an agent installed can be discovered.
- **IPMI:** Looks for IPMI-enabled servers. IPMI is a specification developed by Intel,***** H-P,* NEC,* and Dell* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access these features regardless of whether the device is turned on or not, or what state the OS may be in. Please keep in mind that if the Baseboard Management Controller is not configured, it will not respond to ASF pings which the product uses to discover IPMI. This means that you will have to discover it as a normal computer. When you push the client, ServerConfig will scan the system and detect it is IPMI and configure the BMC.
- **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 devices with Intel Active Management Technology support. Devices can be discovered as Intel AMT devices only after you have accessed the Intel AMT Configuration Screen on the device and changed the manufacturer's default password to a secure password.
- **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.
- **Subnet mask:** Enter the subnet mask for the IP address range you want to scan.
- **Add:** Adds the IP address ranges to the work queue at the bottom of the dialog.
- **Clear:** Clears the IP address range fields.
- **Edit:** Select an IP address range in the work queue and click **Edit**. The range appears in the text boxes above the work queue, where you can edit the range and add the new range to the work queue.
- **Remove:** Removes the selected IP address range from the work queue.
- **Remove all:** Removes all IP address ranges from the work queue.

Now that you have configured a discovery configuration, you can schedule when to discover devices connected to your network.

Scheduling and running the discovery task

Use the **Schedule** button on the **Discover devices** tab to display the **Schedule discovery** dialog. Use this dialog to schedule when a discovery will run. You can schedule a discovery task to run immediately, at some point in the future, make it run periodically as a recurring task, or run it just once and never worry about doing it again.

Once you schedule a discovery task, see the Discovery tasks tab for discovery status. Scheduling a recurring discovery task assists you by automatically discovering new devices that come up on the network.

The **Schedule discovery** dialog has these options.

- **Leave unscheduled:** Leaves the task unscheduled but keeps it in the Discovery configurations list for future use.
- **Start now:** Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start at scheduled time:** Starts the task at the time you specify. If you click this option, you must enter the following:
    - **Time:** The time you want the task to start
    - **Date:** The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
    - **Repeat every:** If you want the task to repeat, select whether you want it to repeat Daily, Weekly, or Monthly. If you pick Monthly and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.

To schedule a discovery task

1. In the left navigation pane, click **Discovered devices**.
2. On the **Discovery configurations** tab, select the configuration you want and click **Schedule**. Configure the discovery schedule and click **Save**.
3. Monitor the discovery progress in the **Discovery tasks** tab. Click **Refresh** to update the status.
4. When the discovery completes, click **Unmanaged** to view all discovered devices in the upper **Discovered devices** pane (the pane does not refresh automatically).

Viewing discovered devices

Discovered devices are categorized by device type in the **Discovered devices** pane. The **Computers** folder is displayed by default. Click the folders in the left pane to view devices in different categories. Click Unmanaged to view all devices returned by the discovery.

- Blade server chassis appear in the **Chassis** folder.
- Standard enterprise devices appear in the **Computers** folder.
- Routers and other devices appear in the **Infrastructure** folder.
- Intel AMT-enabled devices appear in the **Intel AMT** folder.
- IPMI-enabled servers appear in the **IPMI** folder.

- Non-categorized devices appear in the **Other** folder.
- Printers appear in the **Printers** folder.

Note: Some Linux servers appear with the generic "Unix" as the operating system name (or even sometimes show as Other). When the standard management agent is deployed, these servers will update their OS name entry in the **My devices** list and display a full inventory.

To view discovered servers

1. In the Device discovery page, in the left pane, click **Computers** or another type of device you want to view. The results are displayed in the right pane.
2. To filter the results, click the **Filter** icon, type at least a portion of what you are searching for, and click **Find**.

Assigning names

When doing a network scan discovery, some servers return with blank node name (or host name). This occurs most frequently with servers running Linux. You must assign a name to the device before you can use Manage to move it to the My devices list.

1. In the Device discovery page, click the device with a blank name. (You must click the blank area in the node name column.)
2. Click **Assign name** on the toolbar.
3. Type in the name and click **OK**.

When you install a product agent on a device, it automatically scans the host name and updates the core database with the correct information.

Moving devices to the My devices list

Once discovered, you must manually target the devices you wish to manage and move them to the My devices list. Moving the device does not install any software to the device. It only makes the device available for querying, grouping, and sorting in the My devices list. You can "target" specific devices for specific actions, a model similar to the "shopping cart" model in many Web applications.

1. In the **Device discovery** view, click the device you want to move to the **My devices** list. You can select multiple devices by pressing SHIFT+click or CTRL+ click.
2. Click the **Target** button.
3. Click the **Manage** tab.
4. Select **Move targeted devices**.
5. Select **Manage out-of-band-enabled devices agentless (without using an OS-specific agent)**. If the devices can be managed out of band, and you do not want to deploy a management agent to them.

The BMC Password you configured in Configure Services is used to communicate with the BMC. You must set the same password in Configure Services and the BMC of the target machine before the move will succeed.

6. Click **Move**.

The devices are moved to the **My devices** list and their information is moved to the database. Once the information is in the database, you can run queries and reports on it, configure thresholds for alerts, and many other vital management tasks.

After you select devices in the **Device discovery** view you can also go directly to the **Manage** tab (without targeting the devices). If you do this, select **Move selected devices** in step 4 above.

Grouping devices for actions

You may want to organize your devices into groups, such as by geographic location or function, so you can perform actions on them more quickly. For example, you may want to group all devices that are running Windows 2000.

1. **In the My devices list, click Private groups or Public groups, then click Add group.**
2. Type a name for the group in the **Group name** box.
3. Click the type of group you want to create.
    - **Static:** Devices that are manually added to the group. They remain in the group until they are removed or until you no longer manage them (such as when they are removed from your scope)
    - **Dynamic:** Devices that meet one or more criteria as defined by a query. For example, a group may contain all servers that are currently in a Warning state. They remain in the group as long as they match the criteria defined for the group. Devices are automatically added to dynamic groups when they meet the group query criteria.
4. When you are finished, click **OK**.
5. To add devices to a static group, click devices in the right pane of the **My devices** list, click **Move/Copy**, select the group, and click **OK**.

Configuring devices for management

Discovering devices alone does not necessarily make them available for management tasks. Before you can fully manage devices with the console and receive health alerts, you need to install management agents on them. You can choose to install the default agent configuration (which installs all management agents) or customize your own agent configuration to install on your devices. (The agent configuration must include the monitoring agent to receive health alerts.)

You can install management agents in any of the following ways:

- Target devices in the **My devices** list, then schedule an agent configuration task to remotely install agents on the devices. (steps below)
- At the keyboard of the device you wish to manage, map to the core's LDlogon share (\\coreserver\ldlogon) and run SERVERCONFIG.EXE (for devices running Windows). See "Pulling the agents" in the Device Agent Installation and Configuration chapter of the System Manager *User's Guide*.
- Create a self-extracting device installation package. Run this package locally on the device to install the agents. This must be done while logged in with administrative privileges. See "Installing Agent with an Installation Package" in the Device Agent Installation and Configuration chapter of the System Manager *User's Guide*.

To push the agent:

1. Press Ctrl+click to select the device(s) you wish to target, then click **Target**.
2. In the left navigation pane, click **Agent configuration**, right-click the configuration you want to push, and click **Schedule task**.
3. In the left pane, click **Target devices**, and click the **Add target list** button.
4. Click **Schedule task**, click **Start now** to start the task immediately or **Start later** and set the task's start date and time, and click **Save**.

You can view the status of the task in the **Configuration tasks** tab.

Installing agents on Linux servers

You can also remotely deploy and install management agents on Linux servers remotely by SSH. Your Linux server must be configured correctly for this to work. See "Installing Server Agents" in the Device Agent Installation and Configuration chapter of the *System Manager User's Guide.*

Setting alerts

When a problem or other event occurs on a device (for example, if the device is running low on disk space, you can send an alert). You can customize these alerts by choosing the severity level or threshold that will trigger the alert. Alerts are sent to the console and can be configured to perform specific actions. You can set alerts for many different types of events or potential problems. The product comes configured with a default alert ruleset that is installed to a managed device when the monitoring component is installed. This ruleset of alerts provides health status feedback to the console. This default ruleset includes alerts for items such as:

- Disk added or removed
- Drive space
- Memory usage
- Temperature, fans, and voltages
- Performance monitoring
- IPMI events (on applicable hardware)

To learn more about alerting, please see the Alert configuration chapter in the System Manager *User's Guide*.

What's next?

This Getting Started Guide describes only a fraction of the features available in Server Manager, (like device discovery and agent configuration). The companion guides (the *Installation and Deployment Guide* and the *Users Guide*) can provide more in-depth information on all the product's features. Some of these features include:

by remotely controlling a managed device,

Software updates: Establish ongoing patch-level security on the managed devices across your network. You can automate the repetitive processes of maintaining current vulnerability information, assessing vulnerabilities for the various operating systems running on your managed

devices, downloading the appropriate patch executable files, remediating vulnerabilities by deploying and installing the necessary patches on affected devices, and verifying successful patch installation.

Alerting: Ensure that you are alerted if any of your devices reach a particular threshold. Related to the Monitoring feature, Alerting can notify you in many different ways. For example, if you need to know when the storage on your devices reaches 95% of capacity, you can choose how you want to be alerted (the agent can send e-mail or pager messages, reboot or shut down a device, or add information to the alert log).

Queries: Make your management tasks easier by searching for and organizing devices in the core database based on specific system or user criteria. You can query the list of managed devices for those which match the criteria you specify (such as all located in the corporate office or all with 256K of RAM) and group them for actions. These groups can be static (the members of the group can only be changed manually) or dynamic (the members change when devices meet or fail to meet specified criteria).

Software distribution: Create tasks to distribute software packages (one or more MSI files, an executable, a batch file, Linux RPM files, or a package created with LANDesk package builder) to target devices.

Monitoring: Monitor a device's health status by using one of the supported types of monitoring (direct ASIC monitoring, in-band IPMI, out-of-band IPMI, CIM, and so forth). Monitoring lets you keep track of many pieces of data on your devices, such as usage levels, OS events, processes and services, historical performance, and hardware sensors (fans, voltages, temperatures, etc.). Alerting is a related feature that uses the monitoring agent to initiate specific actions.

Reporting: Generate a wide variety of specialized reports that provide critical information about the managed devices on your network. Server Manager uses an inventory scanning utility to add devices (and collected hardware and software data about those devices) to the core database. You can view and print this inventory data from a device's inventory view, as well as use it to define queries and group devices together. The reporting tool takes further advantage of this scanned inventory data by collecting and organizing that data in useful report formats, which can be helpful in gathering and formatting data for regulatory reports.

Unmanaged device discovery: Find devices that aren't being managed by the console. Discovery is the first step to managing new devices on your network. You can set up a discovery task to scan for new machines every month.

Software license monitoring: Track overall license usage and compliance. The software license monitoring agent gathers data (such as the total minutes of usage, the number of launches and the last launch date of all installed applications on a device) and stores this data in the device's registry. You can use the data to monitor product usage and denial trends. The 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.

OS Deployment: Deploy OS images to devices on your network by using the PXE-based deployment tool. This allows you to image devices with empty hard drives or unusable operating systems. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet. OS deployment streamlines new device provisioning without requiring additional end user or IT interaction once the process starts.

Phase 1: Designing your management domain

In phase 1, you gather information about your network infrastructure and make decisions that help you customize your management domain.

In this phase you'll learn about:

- Gathering network information
- Selecting your core server
- The core database
- Planning your security and organization model
- System requirements

Gathering network information

Identify and collect all critical information about your network as it relates to System Manager. Specifically, you need to:

- Determine device configurations
- Select your core server

Selecting your core server

The core server is the center of a management domain. All the key files and services are contained on the core server. Physically, it can be a new or repurposed server.

You can run the administrator console from a browser on a remote workstation, where you conduct management activities such as managing alerts, querying the core database, or creating custom scripts.

Make sure that the server you select for your core server meet the system requirements. Refer to System requirements later in this phase.

Planning placement of program files

During installation, you can specify where you want to install the program files. Accept the default destination directories unless you have compelling reasons to change them. If you choose to modify the destination directory, the destination directory path cannot contain double-byte characters.

The default destination directory for core server files is:

```
C:\Program Files\LANDesk\ManagementSuite
```

The core database

System Manager installs an MSDE database on the core server. Each MSDE database has a 2 GB database size limit. The number of servers this database supports depends on your network's inventory scan file size.

You'll likely see performance issues with MSDE when the database has more than five concurrent things to do. For example, if five System Manager administrators are accessing the database at exactly the same time.

Core / client security

This product uses a certificate-based authentication system. During the core installation, Setup creates a certificate for that core. Clients look for that certificate when communicating with the core, and clients can't communicate with a core for which they do not have a certificate.

Devices will only communicate with core servers that the device has a matching trusted certificate file for. Each core server has its own certificate and private keys, and by default, the client agents you deploy from each core server will only talk to the core server from which the software is deployed.

Planning a scope

Role-based administration is a powerful feature for feature security management. Access the role-based administration tools in the console by clicking Users in the left pane. You must be logged in with administrative rights.

Role-based administration provides advanced device management capability by letting you add users to your system and assign those users rights and scopes. Rights determine the tools and features a user can see and use (see "Understanding rights" in the System Manager User's Guide). Scope determines the range of devices a user can see and manage (see "Creating scopes" in the System Manager User's Guide).

You can create roles based on users' responsibilities, the management tasks you want them to perform, and the devices you want them to see, access, and manage. Access to devices can be restricted to a geographic location such as a country, region, state, city, or to a specific group or type of server.

To implement and enforce this type of role-based administration across your network, simply set up current users, or create and add new users as product users, and then assign the necessary rights (to product features) and scope (to managed devices).

The core server uses scopes to limit the devices that console users can see. Multiple scopes can be assigned to a user, and one scope can be used by multiple users. You can base scopes on one of these methods:

- (Default) **All Machines Scope:** Users can see all devices.
- **Based on a Query:** Users can see the devices that fit the selected criteria of a specific query assigned to them by the administrator.
- **Based on a Group:** Users can see the devices that meet the group criteria.

For more information on scopes, see the System Manager *User's Guide*.

System requirements

Make sure that you meet the following system requirements before you install. The pre-requisite checker does this for you.

Core and database servers

Make sure that all of your core and database servers meet the requirements in the overview.

- Windows 2000 Server or Advanced Server with SP 4, Windows Server 2003 Standard or Enterprise edition x86 SP1, or Windows 2003 R2
- Microsoft Data Access Components (MDAC) 2.8 or higher
- Microsoft .NET Framework 1.1
- Internet Information Services (IIS)
- IIS support for ASP.NET v1.1 scripting
- Internet Explorer 6.0 SP1 or higher
- Microsoft NT File System (NTFS)
- The Windows server you use for your core server must be installed as a standalone server, not as a primary domain controller (PDC), backup domain controller (BDC), or Active Directory controller.
- SNMP must be installed, and SNMP and SNMP trap services must be started
- 200 MB of space available on the system drive, and 900 MB of space available on at least one drive
- Administrator privileges
- LANDesk client is either the correct version or not installed

Core server requirements
The Windows pagefile should be at least 12 + *N* (where *N* is the number of megabytes of RAM on the core server). Otherwise, product applications may generate memory errors.

It is recommended that you have 1 gigabyte of memory on the core machine if you plan to install both Management Suite and Server Manager products on the same core server.

All product services hosted on one server

For smaller management domains, you can install the core server and the core database on one server. For these networks, you may want to consider using the default Microsoft MSDE database, which is generally easier to maintain. This is the only database option for System Manager.

Limitation considerations

Your server should at least meet these system requirements before you install the core and database:

- Pentium 4 processor

- 4 GB of free disk space on 10K RPM or faster drives
- 768 MB+ of RAM

Managed server computers

This product supports these server operating systems (not all operating systems are supported equally):

- Microsoft Windows 2000 Server (with SP4)
- Microsoft Windows 2000 Advanced Server (with SP4)
- Microsoft Windows 2000 Professional (with SP4)
- Microsoft Windows 2003 Server R2
- Microsoft Windows 2003 Server Standard Edition x86 (with SP1)
- Microsoft Windows 2003 Server Standard x64 Edition (with SP1)
- Microsoft Windows 2003 Server Enterprise Edition x86 (with SP1)
- Microsoft Windows 2003 Server Enterprise x64 Edition (with SP1)
- Microsoft Windows XP Professional (with SP2)
- Microsoft Windows XP Professional x64 (with SP2)
- Windows Small Business Server 2000 (with SP4)
- Windows Small Business Server 2003 (with SP1)
- Red Hat Enterprise Linux v3 (ES) 32-bit - U6
- Red Hat Enterprise Linux v3 (ES) EM64t - U6
- Red Hat Enterprise Linux v3 WS 32-bit - U6
- Red Hat Enterprise Linux v3 WS EM64t - U6
- Red Hat Enterprise Linux v3 (AS) 32-bit - U6
- Red Hat Enterprise Linux v3 (AS) EM64t - U6
- Red Hat Enterprise Linux v4 (ES) 32-bit - U3
- Red Hat Enterprise Linux v4 (ES) EM64t - U3
- Red Hat Enterprise Linux v4 (AS) 32-bit - U3
- Red Hat Enterprise Linux v4 (AS) EM64t - U3
- Red Hat Enterprise Linux v4 WS 32-bit - U3
- Red Hat Enterprise Linux v4 WS EM64t - U3
- 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
- HP-UX 11.1
- Unix AIX

Linux managed server computers

Below is a list of the firewall and RPM prerequisites for enabling Linux devices for management.

Firewall

In order to initially install the management agent and configure a Linux server to communicate with the core (using the "Push" method), SSH connections must be allowed to pass through the Linux server's local firewall:

22 - TCP only

In order for the agents to be able to communicate with the Core server(s) (for inventory scans, software distribution, vulnerability updates, and so forth), the Linux server's local firewall must be configured to allow communication on the following ports:

9593 - TCP only

9594 - TCP only

9595 - both TCP and UDP

In order to communicate with the management agent, the Linux server's local firewall must be configured to allow communication on the following ports:

6780 - TCP only

Required RPMs (version # or later)

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

REDHAT_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)

Product port usage

Introduction

When using this product in an environment that includes firewalls (or routers that filter traffic), you may need to adjust firewall or router configurations to allow the product to operate. This section describes the ports used by the various product components. The information here focuses on information you need to configure routers and firewalls, leaving out ports only used locally (within individual subnets).

Background information on firewall rules

This information applies to setting up firewall rules. If you aren't familiar with the subject, this section provides some general background information on the main concepts.

Firewall rules

"Opening a port" is not a precise term. You can't just go to a firewall and "open port x." Opening a port is shorthand for setting up a firewall rule. Firewall rules describe what traffic will or will not be allowed through the firewall. Firewall rules don't filter traffic on port number only. Rules can be based on protocols, source and destination port numbers, direction (inbound / outbound), source and destination IP addresses, and other things.

A typical firewall rule looks like this: "allow inbound traffic on TCP port 9535." For using this product, this rule is needed to support remote control. The rule is based on three elements:

1. The protocol (TCP or UDP)
2. The port number
3. The direction (inbound or outbound)

These three elements are required to set up firewall rules.

Source and destination ports, dynamic ports

There are always two ports involved in TCP or UDP communication. Any TCP or UDP packet is from a source port to a destination port. Firewall rules can be based on the source port, the destination port, or both. Ports listed in documents such as this one are always destination ports.

Well-known ports such as 5007 (used by the inventory service) refer to only one side of the communication. The other side of the communication is using a dynamic port. Dynamic ports are assigned automatically by the operating system in the range 1024-5000.

Firewalls and UDP traffic

To allow TCP traffic through a firewall, a single rule is sufficient, such as to allow inbound TCP connections to port 5007. Once the TCP connection is established, data can flow both ways through the connection.

UDP traffic is different because it is connectionless. For example, by default the core server will "ping" devices at UDP port 38293 before starting a task. A firewall rule that allows outgoing UDP packets to port 38293 will allow packets from the core server to a device outside the firewall, but not the device's response packets.

A rule that allows both outgoing and incoming packets to port 38293 won't work either because only one side of the communication is listening on the well-known port. The other side is using a dynamic port. Because the core server's outgoing packets are from a dynamic port to port 38293, the device's response packets are from port 38293 to the same dynamic port, not to port 38293. To allow two-way communication, a rule is needed that allows UDP packets with source port or destination port = 38293. Such a rule is usually acceptable on the intranet, but not on an external firewall (because it would allow inbound packets to all UDP ports).

For this reason, UDP traffic is usually not considered "firewall friendly". Coming back to the example, there is an alternative to UDP port 38293: TCP port 9595. When managing devices across a firewall, you probably want to configure the product to use the TCP port.

Ports used

Port	Direction	Protocol	Service
31770	console to device, device to core	TCP	communication between console and device

Port	Direction	Protocol	Service
6787	console to device	TCP	communication between console and device
9595	console to device	UDP	discovery
9595	console to device	TCP	agent configuration
623	console to device	UDP	ASF, IPMI discovery
9535	console to device	TCP	remote control

This product needs to discover nodes with the management agent installed before it can manage them. UDP port 9595 is used for discovery. You can also manually add individual devices to the console, but this still requires the device to respond to a "ping" on UDP port 9595. Communication between the console and the device uses TCP ports 31770 and 6787. Traffic on the latter port is HTTP-based. UDP port 623 is used for ASF (alert standard forum) discovery. In addition, this product uses TCP port 9535 for remote control. IPMI discovery is a linked with ASF discovery and uses the same port (udp/623).

Phase 2: Installing the core server

This phase focuses on installing the core server.

In this phase, you'll learn about:

- Installing the core server
- Activating the core server
- Deploying to Windows devices
- Deploying to Linux devices

The installation of the components outlined in this phase requires about 30-60 minutes.

Installing the core server

To install the core server

Before starting the install, it is recommended that you close other applications and save any open files. At the Windows 2000/2003 server you've selected to be your core server:

1. Insert the product media into the drive or run AUTORUN.EXE from your installation image. The Autorun screen displays.
2. Click **Check prerequisites and install**.
3. The system requirements checker runs to verify that the server meets minimum system requirements. Make sure all requirements pass. If any do not pass, click **Fail** on the failed requirement's link for links or information regarding installing the failed requirement.
4. Click **Install now** to run the Setup program.
5. Select the language you want Setup to install. Click **OK**.
6. A Welcome screen appears. Click **Next** to continue.
7. On the License Agreement screen, if you agree click **I accept the terms in the license agreement** to continue. Click **Next**.
8. Accept the default destination folder, or specify a custom destination folder, and click **Next**. The destination folder path cannot contain double-byte characters. If you change this folder, remember to substitute your path for any paths you see in the product documentation.
9. Enter an MSDE database password. Remember this password or write it down. Click **Next** to continue.
10. Enter an organization and certificate name for the core server's security certificate. This information helps name and describe the certificate. Click **Next**.
11. On the Ready to Install page, click **Install**. The product will start installing.
12. The **Installation Wizard Completed** dialog appears when Setup is done.
13. Click **Finish**.
14. Setup will prompt you to restart the server. You must click **Yes** to finish Setup. When the server restarts, you'll notice after you log in that Setup will run for a few more minutes while it finishes the installation. Setup won't prompt you for any more information during the first reboot.

When installing an MSDE core database on a Windows 2003 Server, Windows may interrupt the Setup and ask if it's OK to open SETUP.EXE. If you see this prompt, click Open or the product won't be installed correctly.
If you want to install Intel Platform Extensions for LANDesk Software, follow the wizard that opens after the Server Manager installation.

Activating the core server

You must activate the core server before you can use System Manager products on that server. You can activate the core server either automatically by the Internet or manually by e-mail. You may need to reactivate a core server in the event that you significantly modify its hardware configuration.

On a periodic basis, the activation component on the core server will generate data regarding:

- The precise number of devices you're using
- The non-personal encrypted hardware configuration
- The specific LANDesk Software programs you're using (collectively, the "server count data?)

No other data is collected or generated by the activation. The hardware key code is generated on the core server using non-personal hardware configuration factors, such as the size of the hard drive, the processing speed of the computer, and so on. The hardware key code is sent to LANDesk in an encrypted format, and the private key for the encryption resides only on the core server. The hardware key code is then used by LANDesk Software to create a portion of the authorized certificate.

After installing a core server, the Core Server Activation utility (**Start | All Programs | LANDesk | Core Server Activation**) runs at first boot to activate the core with the OEM-supplied user name and password.

You can upgrade from System Manager to Server Manager or Management Suite by using the core activation utility. Please see Using System Manager with Management Suite or Server Manager.

After you've activated a core server, you can use the console's **Preferences | License** dialog to view the product licensing information. With the Intel OEM license, you are authorized to run a product agent on every Intel-branded server or main board.

About the Core Server Activation utility

Use the Core Server Activation utility to activate a new server for the first time. Start the utility by clicking **Start | All Programs | LANDesk | Core Server Activation**. If your core server doesn't have an Internet connection, see "Manually activating a core or verifying the server count data" later in this section.

Each core server must have a unique authorized certificate.

Periodically, the core server verifies licensing by generating the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the

LANDesk Software licensing server. This file is in XML format and is digitally signed and encrypted. Any changes made manually to this file invalidates the contents and the next usage report to the LANDesk Software licensing server.

The core communicates with the LANDesk Software licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Note that the Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the server count manually, as described later in this section.

Activating the core server

To activate a server

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core server** using your LANDesk contact name and password.

The contact name and password are filled out automatically.

Manually activating a core or verifying the server count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send server count data. You'll then see a message prompting you to send activation and server count verification data manually through e-mail. E-mail activation is a simple and quick process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

To manually activate a core or verify the server count data

1. When the core prompts you to manually verify the server count data, it creates a data file called activate.txt in the "\Program Files\LANDesk\Authorization Files" folder. Attach this file to an e-mail message and send it to licensing@landesk.com. The message subject and body don't matter.
2. LANDesk Software will process the message attachment and reply to the mail address you sent the message from. The LANDesk Software message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

Logging in to the console

After setup is finished, you've rebooted the core server, and the core has been activated, start the console by opening a browser and typing the server's address in the following format: http://servername/ldsm. (At the core server, click Start | All Programs | LANDesk | System Manager) Once the console starts, you'll see the console login window. You may be prompted to enter the credential of the account that installed LDSM in order to log in. Only members of the LANDesk Management Suite group on the core server can log on. By default, Setup added the user you were logged in as when you installed the core to the LANDesk Management Suite group. If you want other users to be able to access the console, add them to this group.

The first time you launch the console in a browser it may take up to 90 seconds to display. This delay happens because the server has to do a one-time compile of some code. The console will launch much faster after the first time.

Deploying to Windows devices

This product supports a scheduled, push-based configuration method, allowing you to deploy agents remotely.

To enable a push-based configuration of Windows 2000/2003 servers not already running the standard management agent, you must supply the proper login credentials as follows:

1. On the core server, click **Start | All Programs | LANDesk |** LANDesk **Configure Services**, then click the **Scheduler** tab.
2. Click **Change login**.
3. In the **User name and Password** fields, specify a domain administrator account (in the format domain\username).
4. Stop and restart the scheduler service.
5. From the Web console, target the desired devices, then click **Agent configuration > Scheduled task** to deploy the configurations.

You can specify the domain administrator when configuring Windows 2000/2003 members that belong to the same domain as the core server. To configure Windows 2000/2003 servers in other domains, you must set up trust relationships. Remember that the account identified in step 3 above is also the account under which the scheduler service will run on the core server. Make sure the account has the **Log on as a service** right.

If a push configuration fails and displays a message that says "Cannot Find Agent," try the steps listed below to identify the problem. These steps mimic the scheduler's actions during a push configuration.

1. Find the user name under which the scheduler service is running.
2. On the core server, log in with the username you found in step 1.
3. Map a drive to \\server name\C$. (This step is the one most likely to fail. It may fail for two reasons. Most likely, you don't have administrative rights to the server. If this user name doesn't have administrative rights, it's possible that the server's administrative share (C$) is disabled.)
4. Create a directory \\server name\C$\$ldtemp$ and copy a file into it.
5. Use the Windows Service Manager and try starting and stopping services on the server.

If the device is IPMI-enabled, you must provide the BMC password. Use the **BMC password** tab of **Configure services** to create a password for the IPMI Baseboard Management Controller (BMC).

1. 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.

If the device is Intel* AMT-enabled, you must provide the Intel AMT password. Use the **Intel AMT Configuration tab** of **Configure services** to create or change the password on Intel* Active Management Technology-enabled devices.

To configure an Intel AMT password

1. In the **Intel AMT configuration** tab, type the current user name and password. These must match the user name and password as configured in the Intel AMT Configuration Screen (which is accessed in the computer BIOS settings).
2. To change the user name and password, complete the **New Intel AMT Password** section.
3. Click **OK**. This change will be made when the client configuration is run.

Note: The new password must be a strong password, meaning that the password

- Is at least seven characters long
- Contains letters, numbers and symbols
- Has at least one symbol character in the second through sixth positions
- Is significantly different from prior passwords
- Doesn't contain names or user names
- Isn't a common word or name

Deploying to Linux devices

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 Linux install (Red Hat 3 and 4, and SUSE) includes the RPMs that the Linux standard management agent requires. If you select the monitoring agent in Agent configuration, you need an additional RPM, sysstat.

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 tarball(s), .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 tarball(s), 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.

You must also configure the scheduler service on the core to use the SSH authentication credentials (username/password) on your Linux server. The scheduler service uses these credentials to install the agents on your servers. Use the Configure services utility to enter the SSH credentials you want the scheduler service to use as alternate credentials. 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.

After you've configured your Linux servers and added Linux credentials to the core server, you must add 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 Discover devices.

To discover your Linux servers

1. In 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 OK once you've added your discovery IP ranges.
2. Schedule the discovery task that you just created by clicking it and clicking **Schedule**. When the task finishes, verify that the discovery process found the Linux servers you want to manage.
3. In Device discovery, select the servers you want to manage, click **Target** to add the selected devices to the Target list. Click the **Manage** tab in the lower half of the window. Click **Move selected devices** and click **Move**. This adds the servers to the **My devices** list, so you can target them for deployment.

To create a Linux agent configuration

1. In Agent configuration, click **New**.
2. Enter a configuration name, click HP-UX or Linux Server Edition, and click **OK**.
3. Select the configuration you just created and click **Edit**.
4. Select the agents you want.
5. In the Inventory tab, select the options and the scanner frequency interval that you want. The installation script will add a cron job that runs the scanner at the interval you select.
6. Click **Save changes**.

To deploy your agent configuration, select it in Agent configuration and click **Schedule task**. Configure the task and monitor the task progress in Configuration tasks.

Note: You will not receive any health information on a Linux machine until after the inventory scanner completes its first scan after installation.

To pull a Linux agent configuration

1. Create a temporary directory on your Linux machine (for example, /tmp/ldcfg), and copy the following into the directory:
    1. All files from the LDLOGON\unix\linux directory.
    2. Copy the shell script named after the configuration (<configuration name>.sh) into the temporary directory.

3. Copy the *.0 file named after the configuration into the temporary directory. The * represents eight characters (0-9, a-f).
4. Copy all files listed in the <configuration name>.ini file into the temporary directory. To identify these files, search the .INI file for "FILExx", where xx is a number. Most of the entries you find will have been copied to the client in step 1, but you will find .XML files that must be copied. The filenames should be left intact, with the following exceptions:
    - alertrules\<any text>.ruleset.xml should be renamed to internal.ruleset.xml
    - monitorrules\<any text>.ruleset.monitor.xml should be renamed to masterconfig.ruleset.monitor.xml

2. If the machine is an IPMI/BMC machine (with Monitoring included in the installation), type the following on a command line:

```
export BMCPW="(bmc password)"
```

3. Running as root, execute the shell script for the configuration. For example, if you named the script "pull," use the full path used below:

```
/tmp/ldcfg/pull.sh
```

4. Remove the temporary directory and all its contents.

Note: Please be aware that if you push or pull an agent out to a Linux machine, then run

```
./linuxuninstall.sh -f ALL
```

to clean it and then push or pull again, the file with the GUID is the only file left on the machine after this operation is completed.

The -f option deletes all directories owned by the product. Please see the Linux uninstall documentation for additional information.

Phase 3: Phased deployment

In phase 3, you'll learn about phased deployment. *Deployment* is the process of expanding your management capabilities to the devices you want to include in your management domain.

You deploy this product by loading product agents and services onto devices. This allows you to manage them from a single, central location.

In Phase 3 you'll learn about:

- The phased deployment strategy
- Checklist for configuring devices
- Deploying to Windows devices
- Understanding the device configuration architecture

The phased deployment strategy

Phased deployment is based on three principles:

1. Deploy the components to devices that are less utilized or have the least impact on your existing network first; then progress to the devices that are most utilized or have the most impact.
2. Confirm that the functionality of each managed device is stable before deploying more agents.
3. Proceed through the deployment of the product in well-planned phases, rather than deploying agents to all types of devices at once, which may complicate any required troubleshooting.

If you've completed the first two phases, you're ready to begin this final phase of deploying the product to your devices.

Checklist for configuring devices

To configure devices, you can deploy agents remotely from the Web console or install them from the managed device. In order to a push-based configuration, you must configure the services of any IPMI or Intel* AMT machines. You can use the Configure Services applet to configure the following services for any of your core servers and databases. To launch the Configure Services applet, on the core server, click **Start | Program Files | LANDesk | LANDesk Configure Services**. Use the BMC password or the Intel AMT configuration tabs.

- **Push-based configuration:** Use agent configuration to define a device configuration. Supply the necessary credentials for Intel AMT or IPMI machines via Configure services (see "Configure services" in the *User's Guide*. Target the desired devices, then schedule a task to push the configuration to the devices. See "Configuring agents" in the *User's Guide*.

- **Manual configuration:** From the managed device, map a drive to the core server's LDLogon share and run SERVERCONFIG.EXE, the server configuration program. The components that are deployed to the device must be selected interactively.

Obviously, manual configuration is not practical in a large environment when installing to and configuring devices. In most cases, you will push agents to your managed devices. Please note that product installation does not install agents on the core automatically; you must also install agents to the core, then manually reboot the core.

Regardless of the way you're configuring devices, make sure you've used Agent configuration in the console to create the device configuration you want to deploy.

Windows XP Professional SP2 or 2003 SP1 systems require manual configuration of the firewall in order for full product functionality. Specify the following settings for those devices:
Managed Servers:

File and Printer Sharing - TCP 139, 445; UDP 137,138 (Agent push won't work without this)

Software distribution - TCP 9594, 9595 (Agent push won't work without this)

Advanced - ICMP - "Allow incoming echo request" (the device cannot be discovered if this is not enabled.)

Core Server:

Inventory - 5007

To specify these settings, on the managed device, click **Start | Control Panel | Security**.
This product comes with a default agent configuration that includes: the standard management agent, software update, and monitoring agents.

You can create new configurations that include only the components you wish to install, or (for OEM version only) add the Intel Active System Console to the default agent configuration. Please note that the process of deploying agents is not cumulative; any deployment uninstalls all existing agents. To deploy a new agent to a configuration, you must include it with all previous agents you want in the configuration.

To create a device configuration

1. In the left navigation pane, click **Agent configuration**.
2. Click **New**.
3. Type a name for the new configuration in the Configuration name box.

Type a name that describes the configuration you're working on, such as DBServer or Executive Office Server. This can be an existing configuration name or a new one.

4. Select **Linux server edition**, **Microsoft Windows server edition**, or **HP-UX**.
5. To manage IPMI-enabled servers without installing product software agents, check the **IPMI BMC-only** configuration if the configuration is for IPMI-compliant servers, then click **OK**.
6. Select the configuration you just created, and click **Edit**.

In the tabs, some options might be dimmed because they do not apply to the configuration you chose. For example, if you select an IPMI BMC-only Windows configuration, there are no configurable options.

7. In the **Agent** tab, select the agents you want to deploy.
    - **All:** Installs all agents on the selected device.
    - **Software update:** Installs the software update agent. With this agent installed, you can configure how the scanner runs to detect available updates.
    - **Monitoring:** Installs the monitoring agent on the selected device. The monitoring agent allows for many types of monitoring, including direct ASIC monitoring, in-band IPMI, out-of-band IPMI, Intel Active System Console, Intel AMT, and CIM.
8. **Configuration** is shown for information only
9. Select a reboot option.

Rebooting manually means that devices won't reboot even if the selected agents require a reboot. You must manually reboot the device. If the device requires a reboot, installed agents won't work correctly until the device reboots. Rebooting servers if necessary reboots devices only if a selected agent requires a reboot.

Note: Only devices that update existing 8.5 agents require a reboot.

10. In the **Inventory** tab, set the Inventory Scanner configuration settings. These are explained below.

- **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.
- **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.
- **Inventory scanner settings:** The time the inventory will run. You can select frequency, and you can specify that it always runs on startup.

If you select the inventory scanner's **Between hours of** option, you can specify an hour range that the scanner can run between. If a device logs in during the time range you specify, the inventory scan runs automatically. If the device is already logged in, once the starting hour arrives the inventory scan starts automatically. This option is useful if you want to stagger inventory scans on devices so they don't send scans all at once.

- **Always run on startup:** The inventory scanner runs every time the device is started.

11. In the **Rulesets** tab, select any monitoring and/or alerting rulesets you want included with the configuration. These rulesets are stored in the ldlogon/alertrules folder. New rulesets can be created in Monitoring or Alerting. In order for newly-created rulesets to display in the drop-down lists, you must generate the XML for the custom ruleset.
12. Click **Save changes** to save the agent configuration.

For more information about deploying to devices, see "Understanding the agent configuration architecture" at the end of this chapter.

Deploying to Windows devices

This product supports a scheduled, push-based configuration method, allowing you to deploy agents remotely.

To enable a push-based configuration of Windows 2000/2003 servers not already running the standard management agent, you must supply the proper login credentials as follows:

1. On the core server, click **Start | All Programs | LANDesk** | LANDesk**Configure Services**, then click the **Scheduler** tab.
2. Click **Change login**.
3. In the **User name and Password** fields, specify a domain administrator account (in the format domain\username).
4. Stop and restart the scheduler service.
5. From the Web console, target the desired devices, then click **Agent configuration > Scheduled task** to deploy the configurations.

You can specify the domain administrator when configuring Windows 2000/2003 members that belong to the same domain as the core server. To configure Windows 2000/2003 servers in other domains, you must set up trust relationships. Remember that the account identified in step 3 above is also the account under which the scheduler service will run on the core server. Make sure the account has the **Log on as a service** right.

If a push configuration fails and displays a message that says "Cannot Find Agent," try the steps listed below to identify the problem. These steps mimic the scheduler's actions during a push configuration.

1. Find the user name under which the scheduler service is running.
2. On the core server, log in with the username you found in step 1.
3. Map a drive to \\server name\C$. (This step is the one most likely to fail. It may fail for two reasons. Most likely, you don't have administrative rights to the server. If this user name doesn't have administrative rights, it's possible that the server's administrative share (C$) is disabled.)
4. Create a directory \\server name\C$\$ldtemp$ and copy a file into it.
5. Use the Windows Service Manager and try starting and stopping services on the server.

If the device is IPMI-enabled, you must provide the BMC password. Use the **BMC password** tab of Configure services to create a password for the IPMI Baseboard Management Controller (BMC).

1. 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.

If the device is Intel* AMT-enabled, you must provide the Intel AMT password. Use the **Intel AMT Configuration** tab of Configure servicesto create or change the password on Intel Active Management Technology-enabled devices.

To configure an Intel AMT password

1. In the **Intel AMT configuration** tab, type the current user name and password. These must match the user name and password as configured in the **Intel AMT Configuration** Screen (which is accessed in the computer BIOS settings).
2. To change the user name and password, complete the **New Intel AMT Password** section.
3. Click **OK**. This change will be made when the client configuration is run.

Note: The new password must be a strong password, meaning that the password

- Is at least seven characters long
- Contains letters, numbers and symbols
- Has at least one symbol character in the second through sixth positions
- Is significantly different from prior passwords
- Doesn't contain names or user names
- Isn't a common word or name

Verifying successful completion of agent deployment

To verify that you've successfully deployed the management agent to devices, confirm that you can do the following tasks from within the console. If you need additional information to complete these tasks, refer to the chapters in the *System Manager User's Guide* that correspond to the respective features.

Inventory

- In the **My devices** list, double-click a device, then view the list of installed agents.
- Perform an inventory query.
- Select a device, then click **Inventory** to view data for that device.
- Modify a Windows device's WIN.INI file, rescan the device, then verify that changes were recorded within the CHANGES.LOG.

Deploying devices from the command line

You can control what components are installed on devices by using command-line parameters with SERVERCONFIG.EXE.

You can launch SERVERCONFIG.EXE in standalone mode. It's located in (system drive)\Program Files\LANDesk\ManagementSuite\LDLogon on the core server. SERVERCONFIG.EXE can also be found in the \\coreservername\LDLogon share, which is readable from any Windows 2000/2003 server.

Understanding the agent configuration architecture

Understanding SERVERCONFIG.EXE

SERVERCONFIG.EXE is the product's device configuration utility. It configures Windows servers for management in three steps:

1. SERVERCONFIG determines whether the computer has been previously configured by another LANDesk product. If it has, SERVERCONFIG removes the older files and reverses any other changes.
2. SERVERCONFIG looks for a hidden file called CCDRIVER.TXT to decide whether the server needs to be (re)configured. (The decision process SERVERCONFIG goes through is covered below.) If the device doesn't need to be (re)configured, SERVERCONFIG exits.
3. If the device does need to be (re)configured, SERVERCONFIG loads the appropriate initialization file (SERVERCONFIG.INI) and executes the instructions contained in it.

If you run SERVERCONFIG.EXE a second time and select different agents than the first execution, the agents from the first execution will be deleted. You will need to select each agent you need with each new running of SERVERCONFIG.EXE, even though you have installed the agents previously.

The following command-line parameters are available for SERVERCONFIG.EXE:

Parameter	Description
/I=	Components to include (quotation marks included): "Common Base Agent" "Inventory Scanner" "Alerting" "Vulnerability scanner" "Server Monitor" "Active System Console" You can combine these on the same command line. For example, Example: SERVERCONFIG.EXE /I="Mirror Driver" /I="Vulnerability scanner"
/IP	Configure using IP
/L or /Log=	Path to the CFG_YES and CFG_NO log files that log which devices were and were not configured
/LOGON	Execute [LOGON] prefixed commands
/N or /NOUI	Do not display the user interface

/NOREBOOT	Don't reboot device when done
/P	Ask for user permission to execute
/REBOOT	Force reboot after running
/TCPIP	Same as IP (see above)
/X=	Components to exclude Example: SERVERCONFIG.EXE /X=SD
/CONFIG=	/CONFIG]= Specifies a device configuration file to use in place of the default SERVERCONFIG.INI file. For example, if you've created configuration files called NTTEST.INI, then use this syntax: SERVERCONFIG.EXE /CONFIG=TEST.INI The custom .INI files should be in the same directory as SERVERCONFIG.EXE and note that the /config parameter uses the filename without the 95 prefix.
/? or /H	Display help menu

Deploying the standard management agent

The standard management agent is a required agent, and is the underlying protocol of the product.

Deploying the Vulnerability scanner

The vulnerability scanner agent performs both scan and repair operations. The **Schedule security tasks** button creates a task which launches vulscan.exe with no parameters. When launched with no parameters, vulscan figures out where its core is by accessing the registry key "hklm\software\intel\landesk\LDWM", value "CoreServer". It then requests the latest list of vulnerability information to scan for, performs the scan, and submits the results to the core. The results are placed into the Detected updates list. Detected updates must be downloaded to the core. Updates can be patched through the remediation process. If the remediation process successfully installs one or more patches, it will re-scan and submit new results to the core. This is for LANDesk updates and OEM updates.

Deploying the inventory scanner

You can use the inventory scanner to add devices to the core database and to collect devices' hardware and software data. The inventory scanner runs automatically when the device is initially configured. The scanner collects hardware and software data and enters it into the core database. After that, the hardware scan runs each time the device is booted, but the software scan only runs at an interval you specify.

Deploying the Monitoring agent

The monitoring agent allows for many types of monitoring, including direct ASIC monitoring, in-band IPMI, out-of-band IPMI, Intel AMT, and CIM.

Deploying the Active System Console

Installs the agent that allows for the Active System Console to be accessed from System Manager through the interface or through the menus. This agent is installed only on devices with Intel boards; if you include this agent in a deployment to a non-Intel board it will not be installed.

Uninstalling the core server

Just as there's a specific strategy you should follow to deploy the different components, there's a corresponding strategy for uninstalling the components.

The following sections show you how to properly uninstall each component. You must uninstall the components in this order:

1. Uninstall product agents from devices.
2. Uninstall the core server.

Uninstalling product agents from devices

The first step to uninstall product software from your network is to uninstall its agents from your devices.

To uninstall agents from servers

1. Log in at the server with administrative rights.
2. Map a drive to the core server's ManagementSuite shared folder.
3. Open a command prompt, change to the ManagementSuite folder's drive letter, and enter the following:

uninstallwinclient.exe

4. The uninstall will run silently, removing all agents.

You can also select Start, Run, then type *core name*\LANDesk\ManagementSuite\uninstallwinclient.exe.

To remove the Linux agent completely from a Linux server

1. In the ManagementSuite shared folder, find the linuxuninstall.tar.gz file and copy it to the Linux box.
2. Execute this file, using the x, z, and f options. The command line should read

tar xzf linuxuninstall.tar.gz

3. After the file is executed, run ./linuxuninstall.sh from the command line.

For help on this file, run it with the -h option. **Note:** Please be aware that if you push or pull an agent out to a Linux machine, then run

./linuxuninstall.sh -f ALL

to clean it and then push or pull again, this process creates duplicate database entries for the same machine with the same name and IP because the machine's GUID is deleted.

The -f option deletes all directories owned by the product. Please see the Linux uninstall documentation for additional information.

The only file remaining after the uninstall is the /etc/ldiscnux.conf file. This file was left there to facilitate keeping the database from being cluttered with duplicate devices. If you are not going to be putting this device back into the database, you may safely delete the file. UninstallWinClient.exe is in the ManagementSuite shared folder. Only administrators have access to this share. This program uninstalls product agents on any device it runs on. It's a Windows application that runs silently without displaying an interface. You may see two instances of the server in the database you just deleted. One of these instances would contain historical data only, while the other would contain data going forward.

Note: By default, Uninstallwinclient.exe reboots the device after uninstalling the agents. To avoid the reboot, you can add the /noreboot switch to the command line.

Uninstalling the core server

The final step in uninstalling the product from your network is to uninstall the software on the core server. Before you do so, make sure you've uninstalled the product software agents from your servers.

To uninstall the core server

1. Go to the core server.
2. Click **Start** | **Settings** | **Control Panel,** then double-click **Add/Remove Programs**.
3. If it is installed, select Intel Platform Extensions for LANDesk software and click **Add/Remove**.
4. To uninstall product software, select LANDesk software.
5. Click **Add/Remove**.

Uninstalling the core database
You need to manually uninstall the core database.

Uninstalling the core database

By default, the core database is not uninstalled when you uninstall LANDesk® System Manager. Important: Do not uninstall the core database if you will later reinstall LANDesk® System Manager on the computer.

To uninstall the core database

1. Go to the core server.
2. Click **Start** | **Settings** | **Control Panel,** then double-click **Add/Remove Programs**.
3. To uninstall the core database, select Microsoft SQL Server Desktop Engine (LDMSDATA).
4. Click **Add/Remove**.

Database files
Removing the Microsoft SQL Server Desktop Engine does not delete the database files used LANDesk® System Manager. Aside from taking up disk space, there is no harm in leaving the database files on your computer. If you want to manually remove these database files, delete the contents of the \ProgramFiles\Microsoft SQL Server\MSSQL$LDMSDATA\Data folder.

Support

You can reach LANDesk Software's online support services on the Web (available in English only). The services contain the most up-to-date information about LANDesk Software products. You can also find installation notes, troubleshooting tips, software updates, and customer support information. Visit the Web site below, then access the product page:

http://www.landesk.com/support/index.php

You can also download the latest versions of the Release Notes and documentation, which may include information that wasn't available at the time the product was shipped. If you received System Manager from an OEM manufacturer, please contact their support service.

If you can't resolve your issue using this guide or by consulting the LANDesk Software support Web site, LANDesk Software offers a range of paid support, consulting, and partner services. For more information, see the customer support page at:

http://www.landesk.com/wheretobuy/

Before calling for customer support issues, have this information ready:

- Your name, the name of your company, and the version of the product you're using.
- The network operating system you're using (name and version).
- Any patches or service packs you've installed.
- Detailed steps to reproduce the problem.
- Steps you've already taken to troubleshoot the problem.
- Any information unique to your system that may help the Customer Support engineer understand the problem, such as what kind of database application you're using, the brand of video card you've installed, or the make and model of the computer you're using.

Language support

LANDesk® System Manager is localized in the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- English
- French
- German
- Japanese
- Portuguese (Brazil)
- Russian
- Spanish