

LANDesk® Management Suite 8.7

LANDesk Management Gateway 3.0
Deployment and user's guide



»»
LANDesk®



Table of Contents

Overview.....	3
What is the LANDesk Management Gateway?.....	3
Using the Management Gateway	3
How many connections can it handle?	4
Is it secure?	5
Setup	7
LANDesk Management Gateway setup overview.....	7
Setup phases	7
Phase 1: Setting up the LANDesk Management Gateway server	8
Setup configurations	8
Hardware requirements	9
Setting up the Management Gateway	9
Phase 2: Configuring the core server.....	11
Phase 3: Activating the Management Gateway	12
Activating with a LANDesk Software account.....	12
Activating with a trial-use license	12
Manually activating	13
Phase 4: Configuring managed devices	14
Reference	17
Using the Management Gateway administrator console	17
Network settings	17
Gateway control	18
User accounts	18
Logging in to the Management Gateway Web console	19
Managing core certificates	20
Managing client certificates	21
Configuring the Gateway service	22
Configuring system settings	23
Configuring firewall settings	24
Managing users.....	25
Configuring e-mail settings.....	27
Viewing reports.....	28
Software distribution and patch management.....	29
Remote control	30

TABLE OF CONTENTS

Appendices	31
Appendix 1: Frequently asked questions (FAQ)	31
Appendix 2: Troubleshooting	33
Connectivity problems.....	33
Other problems	35
Appendix 3: Supported NICs and controllers.....	36
Supported NICs	36
Supported controllers.....	36

Copyright and trademark notice

Copyright © 2005 - 2006 LANDesk Software, Ltd. All rights reserved.

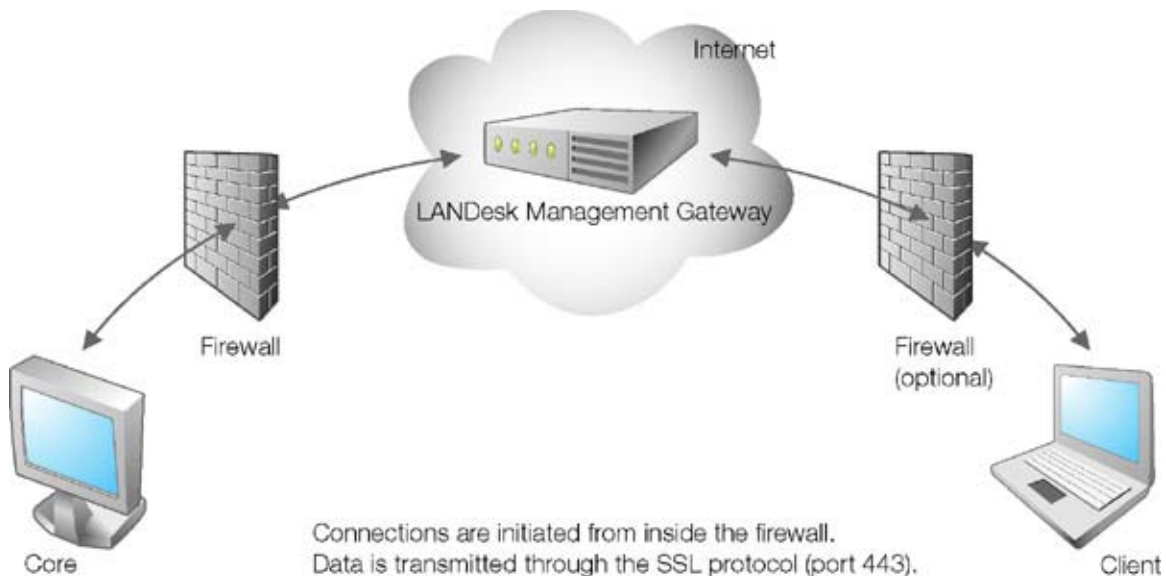
LANDesk® is a registered trademark of LANDesk Software, Ltd.

*Other brands and names may be claimed as the property of others.

Overview

What is the LANDesk Management Gateway?

The LANDesk Management Gateway lets you use LANDesk Management Suite (version 8.6 or later) or LANDesk Server Manager (version 8.6 or later) to manage devices not connected to the local network, without the need to punch holes in the firewall. The LANDesk Management Gateway is an Internet appliance that uses patented technology to help provide secure communication and functionality over the Internet. It acts as a meeting place where the core console and managed devices are linked through their Internet connections—even if they are behind firewalls or use a proxy to access the Internet. Using a secure SSL tunnel, the LANDesk Management Gateway continuously routes bi-directional data between the two computers as long as they are connected. The SSL data is not decrypted at the LANDesk Management Gateway, so there is no “hole” in the protocol where the data isn't encrypted. This provides security, allows a larger number of connections by minimizing CPU utilization, and eliminates the need for complex synchronization between the connections—when data is received, it is sent on to its destination without delay.



The LANDesk Management Gateway runs LDLinux, a customized version of the Linux 2.6.12 kernel. It uses standard messaging, Web, and database services. It also logs connection information (such as connection time, bytes transmitted, and identification information) to the server's hard drive. The program itself uses minimal hard disk space; most disk space is used for logging purposes.

Using the Management Gateway

LANDesk Management Gateway enables functionality including software distribution, patch management, inventory scanning, and remote control. When using the LANDesk Management Gateway in conjunction with LANDesk Management Suite or LANDesk Server Manager, communication through the Management Gateway must *always* be initiated by the managed device. In other words, managed devices can send data to the core and can request data from the core, but the core cannot “push” unrequested data to managed devices. Because the core

cannot push anything to the managed devices through the Management Gateway, you will need to configure managed devices with this in mind. Also note that managed devices connecting through the Management Gateway can only connect with the core server.

How many connections can it handle?

The actual number of connections that a single LANDesk Management Gateway server can host depends on both the type and activity of the connections. For example, a larger number of modem connections can be served in comparison to the number of active high-speed connections because a modem connection is limited by its baud rate regardless of how much screen activity is occurring.

As a general rule, LANDesk Management Gateway can support 4000 concurrent connections. However, a number of factors affect the practical limit of concurrent connections:

- Remote control does not require a great deal of data transmission. A larger number of concurrent remote-control connections can be made than can be made for more data-intensive tasks.
- Tasks such as inventory scans and patching can require a great deal of data transmission. A smaller number of concurrent connections can be made for these types of tasks than can be made for remote control. To reduce the need for a high number of concurrent connections, you can schedule managed devices to do inventory scans at different times.
- Any hardware upgrades that improve the performance of your network should also improve the performance of the Management Gateway.

Is it secure?

Connections through the LANDesk Management Gateway make use of digital certificates and a novel, dual-SSL session architecture. Sessions are initiated by the managed device, which first communicates with the LANDesk Management Gateway itself. The second SSL session encloses the entire route, end-to-end, allowing data to be transferred between the managed device and console computers. This second SSL session eliminates the need for the LANDesk Management Gateway to do any decrypting or re-encrypting of data. This increases session security and reduces the resource load on the LANDesk Management Gateway itself. Data is decrypted only when it arrives at the destination.

Are firewall changes required?

If your firewall is set up to allow secure Internet transactions using port 443 and SSL, using the LANDesk Management Gateway will not make any changes in your firewall, nor will it change how your firewall behaves. The LANDesk Management Gateway uses standard protocols to work through firewalls, proxies, and NAT routers, without requiring any infrastructure changes and without opening any ports.

The LANDesk Management Gateway itself uses the firewall built into the Linux protocol stack (iptables). The rules for this firewall deny communications on all ports except those required for the LANDesk Management Gateway's communication. There is also a list of denied address ranges—internal addresses that are not valid on the Internet.

The LANDesk Management Gateway can also be set up in a DMZ (or “De-Militarized Zone”) environment that does not have direct access to the Internet. The DMZ is simply a LAN that is isolated from the Internet and an organization's intranet by a set of firewalls. The DMZ firewall rules allow more access to the hosts in the DMZ than would normally be allowed to hosts inside of an intranet, but still much less than direct access to the Internet. If the internal addressing on the DMZ LAN is in a range that is denied by the LANDesk Management Gateway's internal firewall (such as 172.168.x.x), the firewall configuration files can be modified to allow the needed address or address range. Obtain expert help before modifying any configuration on the LANDesk Management Gateway.

SUMO

LANDesk Management Gateway uses SUMO, a checksum scanner, to protect against viruses, Trojans, or unauthorized system changes by detecting changes on the system. The SUMO database is created as part of the installation process, and vital areas on the Management Gateway, such as the Web pages and the system binary directories, are checked every few minutes. If SUMO finds a discrepancy, it sends an e-mail notification to the administrator. The SUMO database is self-checked and does not require maintenance.

LANDesk Management Gateway logging

One of the best attack deterrents is the use of audit trails. While an audit trail does not prevent attacks, it does make it easier to determine when and how an attack has occurred. The LANDesk Management Gateway logs activity and connection information, which is easily accessible in report form.

Blocking connections

Administrators can block or delete computers from the list of managed devices which have been granted certificates to connect through the LANDesk Management Gateway. These blocked computers can be unblocked later, if so desired.

Setup

LANDesk Management Gateway setup overview

The LANDesk Management Gateway is a secure Internet appliance; setup requires a strong knowledge of Internet, networking, and hardware setup issues, including:

- The network location for the Management Gateway installation
- How to connect an Internet appliance
- Differences between public and private addresses
- Name resolution mechanisms
- How to boot from a CD-ROM

Note: To use the LANDesk Management Gateway in conjunction with LANDesk Server Manager, you must perform a *dual installation*, installing both LANDesk Server Manager and LANDesk Management Suite. See the LANDesk Server Manager *Installation and Deployment Guide* for information on dual installation.

Setup phases

Setting up the LANDesk Management Gateway consists of four phases which must be completed in the following order:

- **Phase 1:** Set up and install the Management Gateway server. This is a dedicated machine that acts as a secure Internet server to manage connections and route data between the core and managed devices.
- **Phase 2:** Configure the core server to use the Management Gateway. This configuration must be done from the console on the core server.
- **Phase 3:** Activate the Management Gateway with valid licensing information.
- **Phase 4:** Configure managed devices to connect through the Management Gateway. For managed devices that will only request remote control support through the Management Gateway, this step consists simply of installing or reinstalling the LANDesk Management Suite client software. On other managed devices, you must run **BrokerConfig.exe** after installation.

Phase 1: Setting up the LANDesk Management Gateway server

Setup is accomplished using the bootable installation CD. No special Linux knowledge is required for setup.

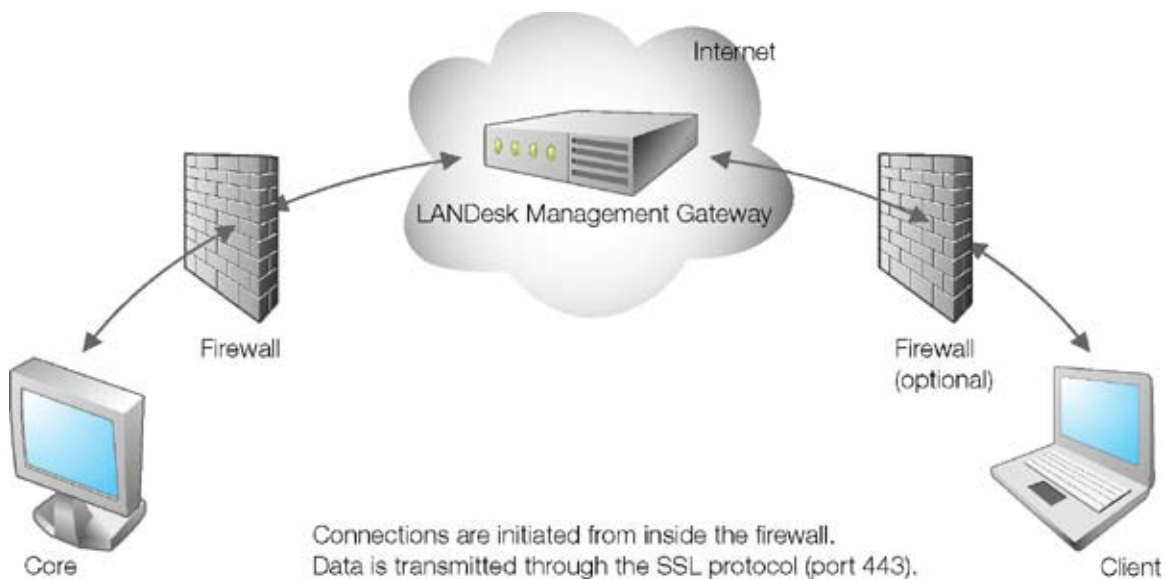
Notes:

- It is not necessary to preinstall an operating system or any software.
- You will need a static IP address, netmask, and default gateway to configure the Gateway network.
- Remember to record the IP address and other network information you use when setting up the LANDesk Management Gateway. Keep this information for future reference.
- After setup, do not make changes to the Management Gateway server by any means other than the Management Gateway interface or the Management Gateway Web interface.

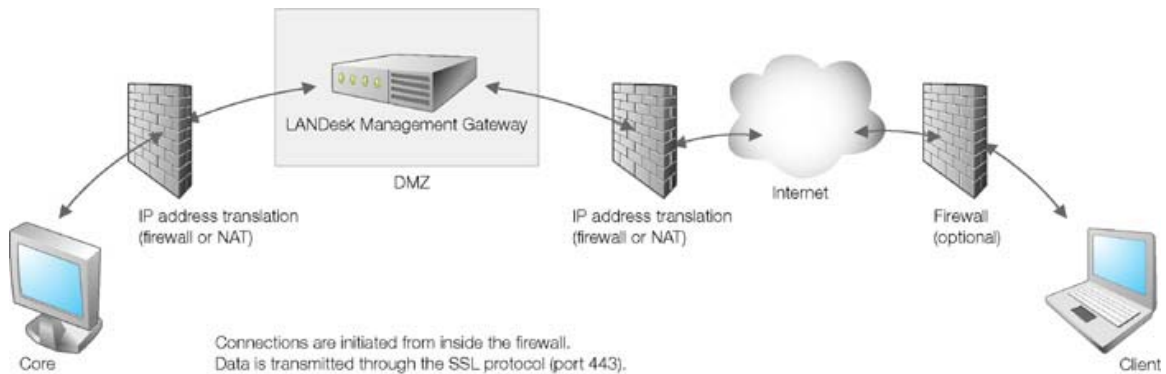
Setup configurations

Two typical setup configurations for the LANDesk Management Gateway are shown below.

Setup with direct access to the Internet



Setup within a DMZ environment



Hardware requirements

The following hardware is required for the LANDesk Management Gateway. A server that runs at a faster speed, uses multiple processors, or has more memory will be able to handle a greater number of simultaneous connections when sufficient network bandwidth is available.

- Intel Pentium® 4 processor or better (dual processors recommended)
- 1 GB RAM (2 GB recommended)
- One or more supported NICs (two or more NICs are recommended, and are required for a DMZ-type installation; one IP Address is recommended per NIC)
- Bootable CD-ROM
- 40 GB hard drive or greater
- Video card and keyboard; these are required only when using the Management Gateway console

Note: See *Appendix 3: Supported NICs and controllers* for a list of specifically supported NICs and controllers.

Setting up the Management Gateway

Caution: The installation CD erases all existing information on the hard drive to which it is installed. Make sure you have backed up any needed information before installation. Installation does not include a dual-boot option.

1. If necessary, use your system's BIOS setup program to change the boot order so your computer will search for a bootable disk in the CD drive before it boots from the hard drive.
2. Insert the LANDesk Management Gateway Installation CD into your bootable CD drive.
3. Reboot your computer.
4. Follow the on-screen installation instructions.
5. When prompted, remove the CD and reboot the system.
6. On startup, the first-boot wizard runs automatically.
7. Follow the on-screen instructions to specify a password.

8. Log in using the user name **admin** and the password you specified.
9. Configure the network settings to be used by the Management Gateway.

Phase 2: Configuring the core server

After you have completed phase 1, you must configure the core server to connect through the LANDesk Management Gateway. You must complete this step before you configure managed devices to use the Gateway.

Note: The Configure Gateway option is available only from the main console, not from any additional consoles you may have set up. Only users with the LANDesk Administrator right can modify a Gateway configuration.

1. From the console on the core server, click **Configuration | Management Gateway**.
2. On the **Gateway information** tab, specify the Gateway information.
3. If the Gateway uses an internal address that is different from its public address (for example, if you have set the Gateway up in a DMZ environment), check **Use separate internal address** and specify the internal name and internal IP address.
4. If the Gateway will use a proxy, check **Use proxy** and specify the proxy settings.
5. Click **Test settings** to test the core server connection to the Gateway.
6. If the test fails, check the information you entered and correct any mistakes, then click **Test settings** to make sure the connection works.
7. Click the **Certificates** tab.
8. Click **Post to Gateway**.
9. Click **OK** to post the certificate.

Phase 3: Activating the Management Gateway

After you have completed setup phases 1, 2, you must activate the Management Gateway with either a full license from LANDesk or with a 45-day evaluation license. You can activate a Management Gateway automatically via the Internet or manually via e-mail. You can switch from a 45-day evaluation to a paid license at any time by entering your LANDesk Software username and password from the **Online activation** page.

If you do not complete the activation process, you will be able to see and use the Management Gateway console pages, but the Management Gateway will not make connections between the core and managed devices.

Activating with a LANDesk Software account

Before you can activate a Management Gateway with a full-use license, you must have an account set up with LANDesk Software that licenses you for its use. You will need the account information (organization ID and keycode) to activate the Management Gateway. If you don't have this information, contact your LANDesk Software sales representative.

To activate a Management Gateway

1. From the Management Gateway console, click **Activation**.
2. Click **Activate now**.
3. Click **Licensed activation**.
4. Enter the **Organization ID** and **Activation keycode**.

You can view the licensing information that will be sent to LANDesk by clicking **View activation information before sending**.

5. Click **Activate**.

If the Management Gateway doesn't have direct Internet access (for example, if it has been set up between internal firewalls) it won't be able to send the activation/licensing information. Activation will fail and you will receive an "Activation Communications Error" message. If you receive this message, click the link it contains to manually activate the system. See *Manually activating* below for more information.

Activating with a trial-use license

The 45-day trial-use license activates your Management Gateway with the LANDesk Software licensing server. After the 45-day evaluation period expires, the Management Gateway will no longer make connections. During or after the 45-day trial use license, you can switch to a full activation that uses a LANDesk Software account. If the trial-use license has expired, switching to a full-use license will reactivate the Management Gateway.

To activate a 45-day evaluation

1. From the Management Gateway console, click **Activation**.
2. Click **Activate now**.

3. Click **Start 45 day trial activation**.
4. Click **Activate**.

Manually activating

If the Management Gateway doesn't have direct Internet access (for example, if it has been set up between internal firewalls) you will need to manually activate using e-mail.

To manually activate a Management Gateway

1. From the Management Gateway console, click **Activation**.
2. Click **Install activation**.

You'll see the PGP-encoded text file (ldmg_activation.req) required for activation.

3. Click **Save activation request** to save the file.
4. Save the **ldmg_activation.req** file to your hard drive.
5. Attach the **ldmg_activation.req** file to an e-mail message and send it to **licensing@landesk.com**. The message subject and body don't matter.

LANDesk Software will process the message attachment and reply to the mail address from which you sent the message. The reply will include an attached authorization file.

Important: Disregard the instructions in the reply email (the instructions apply to LANDesk Management Suite and do not apply to the LANDesk Management Gateway). Instead, follow the steps below.

6. From the Management Gateway console, click **Activation**.
7. Click **Install activation**.
8. Click **Browse**, browse to the file you received from LANDesk, and click **Open**.
9. Click **Activate**.

It may take a few moments for activation to complete.

Phase 4: Configuring managed devices

After you have completed setup phases 1, 2, and 3, you must configure the managed devices to connect to the core through the LANDesk Management Gateway. There are three options for configuring managed devices:

- Manually configure each managed device to connect through the Management Gateway. This type of configuration enables LANDesk Management Suite and LANDesk Server Manager functionality through the Gateway.
- "Push" the configuration to mobile devices while they are attached to the local network. This is an easy way to configure mobile devices so they can connect through the Management Gateway after they are disconnected from the local network. This type of configuration enables LANDesk Management Suite and LANDesk Server Manager functionality through the Gateway without the necessity of manually configuring individual managed devices.
- Configure a managed device for on-demand remote control only.

To manually configure managed devices

1. From a command prompt on the managed device, enter **BrokerConfig.exe** (you can use the **-h** startup option to see a list of other valid startup options).
2. From the **Certificate request** tab, type a LANDesk console user name and password, then click **Send**.
3. Click **Test** to test the connection from the managed device to the Gateway.
4. If the test fails, check the information you entered and correct any mistakes, then click **Test** to make sure the connection works.
5. Click the **Gateway information** tab.
6. If the managed device accesses the Internet through a proxy, specify the Internet Explorer proxy settings.
7. Choose the best connection method to the LANDesk core.
8. Click **Update** or **Close**.

To "push" the configuration to a mobile device while it is connected to the network

1. In the **Manage scripts** window, click **Scripts | All other scripts**.
2. Click **Create Management Gateway client certificate**.
3. Click the **Schedule** button. This displays the **Scheduled tasks** window and adds the script to it, where it becomes a task.
4. In the **Network view**, select the devices you want to be task targets and drag them onto the task in the **Scheduled tasks** window.
5. In the **Scheduled tasks** window, click **Properties** from the task's shortcut menu.
6. On the **Schedule task** page, set the task start time and click **Save**.

To configure a device for on-demand remote control only

- Install the client software after you have completed setup phases 1, 2, and 3. The managed device will need to download and install the on-demand remote control agent prior to requesting remote control. See *Remote control* for more information.

Reference

Using the Management Gateway administrator console

Use the administrator console to configure the Management Gateway at setup and to change configuration settings after setup.

Network settings

Use **Network settings** to add, delete, or edit a network connection, specify or change a host name/domain, or edit name resolution settings.

To add a network connection

1. Click **Network settings**.
2. Click **Network connections**, then click **Add**.
3. Specify the address, netmask, and gateway.
4. Click **OK**.

To edit a network connection

1. Click **Network settings**.
2. Click **Network connections**.
3. Select the connection you want to edit, then click **Edit**.
4. Specify the address, netmask, and gateway.
5. Click **OK**.

To add or delete a network connection

1. Click **Network settings**.
2. Click **Network connections**.
3. Select the connection you want to delete.
4. Click **Del**.
5. Click **OK**.

To specify or change host name/domain

1. Click **Network settings**.
2. Click **Host name/domain**.
3. Specify host name and domain.

4. Click **OK**.

To edit name resolution settings

1. Click **Network settings**.
2. Click **DNS settings**.
3. Select a DNS server from the list, or specify an IP address and click **Add** to add a DNS server to the list (you can also delete the selected DNS server from the list by clicking **Del**).
4. Add anything you want to append to the search.
5. Click **OK**.

Gateway control

Use **Gateway control** to start or stop the Gateway or firewall service.

To start or stop the Gateway service or firewall service

1. Click **Gateway control**.
2. Click the **Start** or **Stop** button for the service you want to start or stop.

User accounts

Use **User accounts** to reset passwords or remove lockouts for Management Gateway users.

To reset a password

1. Click **User accounts**.
2. Select the account for which you want to reset the password.
3. Click **Reset password**.
4. Specify the new password.
5. Click **OK**.

To remove all lockouts

1. Click **User accounts**.
2. Click **Remove all lockouts**.

Logging in to the Management Gateway Web console

Note: To manage certificates or make changes to the Gateway configuration, you must log in as admin.

To log in to the LANDesk Management Gateway

1. Open a browser.
2. In the Address field, enter **http://hostname** where *hostname* is hostname of the LANDesk Management Gateway.
3. Click **Management Gateway console**.
4. Enter the user name and password.
5. Click **OK**.

Managing core certificates

The easiest way to add a core certificate to the LANDesk Management Gateway is to post it from the console on the core server. You can also manually add a core certificate by copying its contents and pasting them to the Management Gateway console.

To post a certificate from the console on the core server

1. From the console on the core server, click **Configuration | LANDesk Management Gateway**.
2. Click the **Certificates** tab.
3. Click **Post to Gateway**.

After you have successfully posted the certificate, it will appear as a link beneath the **Post to Gateway** button.

To manually add a certificate using the Management Gateway Web console

1. Open the certificate you want to add in text editor.
2. Copy the entire body of the certificate.
3. From the Management Gateway console, click **Manage core certificates**.
4. Click **Add certificate**.
5. Paste the copied certificate text into the text box.
6. Click **Save**.

To remove a certificate

- From the Management Gateway Web console, click the **Remove** link associated with the certificate you want to remove.

Managing client certificates

From the console on the core server, an administrator can block or delete computers from the list of managed devices which have been granted certificates to connect through the LANDesk Management Gateway. Blocked computers remain in the list and can be unblocked later,

You can view the list of blocked certificates from the LANDesk Management Gateway.

To block or delete client computers

1. From the console on the core server, click **Configuration | LANDesk Management Gateway**.
2. Click the **Certificates** tab.
3. Click **Manage client certificates**.
4. Select the computer(s) you would like to block or delete.
5. Click **Block selection** or **Delete selection**.
6. Click **OK**.

To unblock a client computer

1. From the console on the core server, click **Configuration | LANDesk Management Gateway**.
2. Click the **Certificates** tab.
3. Click **Manage client certificates**.
4. Uncheck the **Block** checkbox for the computer to which you want to restore access.
5. Click **OK**.

To view a list of blocked client certificates from the Management Gateway Web console

- From the LANDesk Management Gateway Web console, click **Blocked client certificates**.

Configuring the Gateway service

You can change the following Gateway service configuration settings:

- **Verbosity of log messages:** The amount of detail saved to the system log file.
- **Lockout attempts:** The number of times a login attempt can fail before the user is locked out of the system.
- **Lockout time:** The number of minutes a user is locked out of the system after unsuccessfully attempting to log in.
- **Session timeout:** The number of minutes before an inactive session is disconnected.
- **Maximum connections:** The maximum number of concurrent connections allowed by the Management Gateway.
- **Additional host names:** A space-separated list of other host names or IPV4 dotted decimal addresses by which this Gateway may be referenced (for example, if the LANDesk Management Gateway is located in a DMZ and uses a different DNS name for access via the Internet than it does for access from within the network).

To change the Gateway service configuration

1. From the Management Gateway console, click **Gateway service**.
2. Make any desired changes to the configuration settings.
3. Click **Save**.

Configuring system settings

You can change the date, time, and time zone settings used by the LANDesk Management Gateway.

To change the Gateway date and time settings

1. From the Management Gateway console, click **System settings**.
2. Make any desired changes to the system date and time settings.
3. Click **Save**.

Configuring firewall settings

Firewall settings allow you to block specific addresses or address ranges from connecting to the LANDesk Management Gateway.

To enable or disable the Blocked addresses list

1. From the Management Gateway console, click **Firewall**.
2. Click **Enable** or **Disable**.

To add an address to the Blocked addresses list

1. From the Management Gateway console, click **Firewall**.
2. Type the address on its own line in the blocked addresses list. In addition to standard IP addresses, you can use standard "slash notation" to denote address ranges.
3. Click **Save**.

To remove an address from the Blocked addresses list

1. From the Management Gateway console, click **Firewall**.
2. Delete the address from the blocked addresses list.
3. Click **Save**.

Managing users

You can add, edit, and remove users. The two types of users are:

- **Administrator.** An administrator can remote control other devices, can add other users, and can change settings on Management Gateway.
- **Non-administrator.** A non-administrator can remote control other devices.

Notes:

- You must use strong passwords.
- You can control access for support operators using the Organization field. When a managed device uses the on-demand remote control agent to request remote control support, it must specify the organization to which it belongs. That managed device will only appear in the list of operators who are members of that organization. You can place an asterisk (*) in the Organization field to allow a user to see all managed devices which request remote control support.

To add a new user

1. Click **Users**.
2. Click **Add**.
3. Type the information for the user you want to add.
4. Check **Admin privileges** if you would like the user to have administrator rights.
5. Click **Save**.

To edit a user

1. Click **Users**.
2. Click the **Edit** link associate with the user you want to edit.
3. Edit the user information you want to change.
4. Click **Save**.

To set or change a user's password

1. Click **Users**.
2. Click the **Set Password** link associated with the user whose password you want to change.
3. Type and confirm the password you want to set.
4. Click **Save**.

Note: Passwords for the default **Admin** and **Service** accounts can only be changed from the administrator console.

To remove a user

1. Click **Users**.

2. Check the user(s) you want to remove.
3. Click **Remove**.

Configuring e-mail settings

You can specify an e-mail address and SMTP relay host to which the LANDesk Management Gateway will send periodic reports.

To set e-mail settings

1. From the Management Gateway console, click **E-mail**.
2. Specify the administrator e-mail address.
3. Specify an SMTP relay host if required.
4. Click **Test** to send a test e-mail to the specified address.
5. Click **Save**.

Viewing reports

The LANDesk Management Gateway provides the following reports:

- **System logs:** Show connection information (connection time, bytes transmitted, identification information, etc.). Entries are deleted from the log after 90 days.
- **File system report:** Shows changes to the file system, and can be used to detect intrusion.
- **Gateway connection table:** Shows all current connections to the LANDesk Management Gateway. This report is included as a diagnostic tool in the event that you ever require technical support.
- **Gateway service status:** Shows statistics about the Gateway service.

To view a report

1. From the Management Gateway console, click **Reports**.
2. Click the report you would like to view.

Software distribution and patch management

When using the LANDesk Management Gateway in conjunction with LANDesk Management Suite or LANDesk Server Manager, communication through the Management Gateway must *always* be initiated by the managed device. In other words, managed devices can send data to the core and can request data from the core, but the core cannot "push" unrequested data to managed devices. Because managed devices connecting through the Management Gateway can only connect with the core server, both software distribution packages and patches must come through policy-based delivery methods from a Web share located on the core. See *Setting up the delivery server* under *Using software distribution* in the *LANDesk Management Suite user's guide* for information on setting up a Web server for software distribution.

Remote control

Before a managed device can request remote control through the LANDesk Management Gateway, it must either be configured to connect through the Management Gateway (see *Phase 3: Configuring clients*), or it must download and install the on-demand Remote control agent.

After the connection is established, remote control functionality through the LANDesk Management Gateway is identical to LANDesk Management Suite remote control. For details on remote control functionality, see the *Remote control* chapter in the *LANDesk Management Suite Users Guide*.

To create a remote control agent for on-demand download and installation

1. From the console on the core server, click **Configuration | LANDesk Management Gateway**.
2. Click the **Certificates** tab.
3. Click **Create**.
4. Specify the organization name.
5. Select the remote control features you want to allow.
6. Click **Save**.
7. Specify the location to which you want the remote control agent to be saved.
8. Click **Save**.

After creating the remote control agent, you can distribute it on CD or post it to an accessible location for download by managed devices.

To request remote control through the Management Gateway from a managed device

1. From the Start menu, click **LANDesk Gateway access**.
2. Specify user name, password, and organization.
3. Click **OK**.

To start a remote control session from the LANDesk console

1. In the **Device list**, right-click the managed device that has requested remote control.
2. Select **Management Gateway remote control**.

Appendices

Appendix 1: Frequently asked questions (FAQ)

What ports are used for the LANDesk Management Gateway?

The LANDesk Management Gateway uses port 443 for secure SSL over HTTPS. Port 80 is also open, and port 22 can be used to manage the Gateway via SSH v2.

Why am I prompted for a proxy address when no proxy is required for my connection?

If the managed device cannot communicate with the LANDesk Management Gateway, it checks for a proxy and prompts for a proxy address. If you do not use a proxy server, this message may be misleading. It is actually indicative of a connection problem between the managed device and the LANDesk Management Server. See *Troubleshooting* for information on how to diagnose and resolve the problem.

What version of Linux does the LANDesk Management Gateway use?

The LANDesk Management Gateway uses LDLinux which uses kernel 2.6.12. This version is open source and contains no proprietary components.

Can the Linux version be patched or upgraded?

No. Aside from the fact that it resides on a computer you select, the LANDesk Management Gateway functions very much like an appliance, and should not be modified. LANDesk will make available any recommended bug fixes or upgrades.

Is it okay to install other packages on the Global Support LANDesk Management Gateway?

The installation of other packages is not supported.

How do I configure the SQL database on the LANDesk Management Gateway?

The SQL database on the LANDesk Management Gateway is automatically configured during setup and does not require or allow further configuration.

Can the LANDesk Management Gateway be reconfigured?

Configuration changes can be made through the LANDesk Management Gateway interface. No other reconfiguration is possible.

Who has access to the LANDesk Management Gateway?

Two local accounts are installed by default:

- **Admin:** This account has rights to add or remove local user accounts, and to make configuration changes to the LANDesk Management Gateway.
- **Service:** This account is similar to admin, and is used to make core service connections.

You can create additional accounts to give access to other users.

Which parts of the boot menu are configurable?

The boot menu is not configurable.

Appendix 2: Troubleshooting

Connectivity problems

Most LANDesk Management Gateway issues are connectivity problems caused by invalid IP addresses or DNS entries. You can test the connection through the LANDesk Management Gateway from both the core and managed device. This allows you to pinpoint the connectivity failure so you can correct the problem.

How can I test the connection from core to managed device?

1. From the console on the core server, click **Configuration | LANDesk Management Gateway**.
2. Click **Test settings**.

How can I test the connection from managed device to core?

1. From a command prompt on the managed device, enter **BrokerConfig.exe**.
2. Click **Test**.

Notes:

- If you do not specify a user name and password, clicking **Test** checks for a valid certificate and tests the connection through the Management Gateway to the core.
- If you specify a user name and password, clicking **Test** tests the connection through the Management Gateway without checking for a valid certificate.

Troubleshooting connectivity problems.

In some cases, policy issues may prevent the CGI process from starting, which prevents communication between the managed device and the core.

To check for CGI problems

1. From the core server, stop the Gateway service (click **Configuration | Management Gateway**, then click the stop button at the bottom of the dialog).
2. From a managed device, request a certificate (from a command prompt on a managed device, enter **BrokerConfig.exe**, then, from the **Certificate request** tab, type a LANDesk console user name and password, then click **Send**).
3. On the core server, check the **ProgramFiles\LANDesk\ManagementSuite\brokerreq** to see if a **.csr** file has been created.

If a **.csr** file was created, the connectivity problem is not caused by a CGI problem. If file was not created, you will need to edit two policies to enable the CGI process to start.

4. From the Windows Control Panel, click **Administrative Tools**, then click **Local Security Policy**. Edit **Adjust memory quotas for a process** and **Replace process level token** to make sure they contain the user **IUSR_servername**.
5. Restart the Gateway service

For more information, see *CGI process will not start in Microsoft Internet Information Service (IIS) Manager* help.

A managed device is unable to connect using its current certificate.

The device ID of a managed device is stored in the certificate it uses for authentication. If the device ID of a managed device changes, that managed device must request a new certificate before it can connect through the Gateway to the core.

1. From a command prompt on the managed device, enter **BrokerConfig.exe**.
2. From the **Certificate request** tab, type a LANDesk console user name and password, then click **Send**.

A managed device receives the error "Connection not configured for Management Gateway access".

If the managed device was set up prior to setting up the core server, you will need to configure it with the Management Gateway address.

1. From a command prompt on the managed device, enter **BrokerConfig.exe**.
2. Click the **Gateway information** tab.
3. Specify the Gateway IP address.
4. Click **Update**.

A managed device is unable to access the LANDesk software distribution portal.

This can occur if Internet Explorer settings were not set up correctly for use with the Management Gateway. Simply change the managed device's Internet Explorer settings to allow local addresses to bypass the proxy.

The core is able to post a certificate to the Management Gateway, and the "Test settings" button returns a "Settings test successful" response, but managed devices are unable to connect to the core through the Management Gateway.

This can occur if the core is configured to connect to the Management Gateway through a proxy, but you did not specify proxy settings from the **Management Gateway configuration** dialog. If you have specified proxy settings for Microsoft Internet Explorer, the **Test settings** button and the **Post to Gateway** button in the **Management Gateway configuration** dialog will use those settings and will succeed, but the Management Gateway service will not use them and will fail to connect. The BrokerService.log file may state that the Gateway service was unable to connect to the Management Gateway IP address or that the configuration was not found.

If you encounter this problem,

1. From the console on the core server, click **Configuration | Management Gateway**.
2. On the **Gateway information** tab, check **Use proxy** and specify the same proxy settings that you have specified for Internet Explorer.
3. Click **Test settings** to test the core server connection to the Gateway.
4. If the test fails, check the information you entered and correct any mistakes, then click **Test settings** to make sure the connection works.
5. Click **OK**.

Other problems

The Admin account is locked out.

In the event that the admin account is locked out of the Gateway Web interface, you can remove the lockout from the Gateway administrator console.

1. Log in to the Administrator console.
2. Click **User accounts**.
3. Click **Remove all lockouts**.

Appendix 3: Supported NICs and controllers

Check the LANDesk Knowledge Base at <http://kb.landesk.com> for updates to this list.

Supported NICs

- Broadcom 440x10/100
- Intel ® Pro/100
- VIA Rhine II
- VIA - Rhine II Fast Ethernet Adapter
- 3Com 3C905BTX
- Intel Pro 1000 MT
- Broadcom NetXtreme Gigabit Ethernet
- Intel Pro 1000
- DUAL intel pro 1000 - 10.16.238 subnet
- Intel Pro/1000XT
- Realtech RTL 8139
- Intel 82544GC 10/100
- DUAL Intel PRO/1000 MT Dual Port NIC
- Intel PRO/1000 CT
- Intel 82547 Gigabit
- Intel 6300 ESB
- Intel 82559
- Intel 8355x-based Enet 10/100
- Intel Pro 1000 VE
- Intel 82545 EM Gigabit Eth. Controller (Copper) (Rev 01)

Note: The Marvel Yukon NIC family is also supported where drivers are available.

Supported controllers

IDE

IDE controllers are supported.

SATA

The following controllers have been tested:

- Silicon Image Sil 3112 SATALink Controller
- Intel 6300ESB SATA Storage controller

- Dual 3M-ST340014A
- Computer Corporation Smart Array 5i/532 (rev01)
- SATA Controller - On-board Intel 82801DB Ultra ATA

SCSI

The following controllers have been tested:

- Maxtor SCSI ultra 320
- Adaptec AIC-7902 U320
- LSI Controller Single channel integrated LSI 1020 Ultra320 SCSI controller
- 2 Imbedded Adaptec AIC-7902 Based Ultra320
- 2 MegaRAID SCSI-320-2 RAID Controllers
- Adaptec AIC-7892 Ultra160 PCI SCSI Card
- Adaptec AIC 2110 S

RAID

The following controllers have been tested:

- LSI Controller Single channel integrated LSI 1020 Ultra320 SCSI controller (Hardware Raid)
- Computer Corporation Smart Array 5i/532 (rev01) (Hardware Raid)
- 2 MegaRAID SCSI-320-2 RAID Controllers (Hardware Raid)