LANDesk® Management Gateway

User's Guide

LANDesk®

An Avocent® Company

Copyright and trademark notice

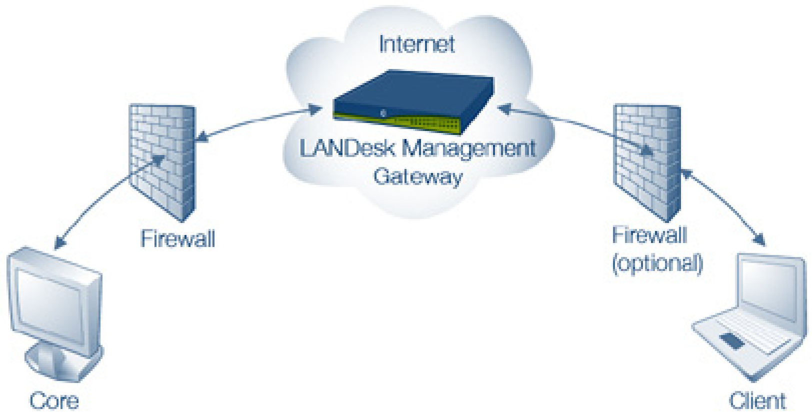
LANDesk and Avocent do not warrant that this document is error free and each retains the right to make changes to this document or related product specifications and descriptions at any time without notice. LANDesk and Avocent do not assume any obligation to update the information contained herein. This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

Table of Contents

Overview

What is the LANDesk® Management Gateway?

The LANDesk® Management Gateway appliance 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 open ports 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 2.6.20.4 kernel. It uses standard messaging, Web, and database services, and logs connection information (such as connection time, bytes transmitted, and identification information). Connections are initiated from inside the firewall and data is transmitted through the SSL protocol (port 443).

Using the LANDesk 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 appliance 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 LANDesk Management Gateway, you will need to configure managed devices with this in mind. Also note that managed devices connecting through the appliance can only connect with the core server.

How many connections can it handle?

The actual number of connections that a single LANDesk Management Gateway appliance 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 LANDesk 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 appliance 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 appliance'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.

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 LANDesk 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.

Configuring the core server and managed devices

LANDesk Management Gateway setup overview

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.

Setting up the LANDesk Management Gateway consists of three phases:

- Configure the LANDesk Management Gateway appliance by following the instructions on the *Quick Installation Guide* sheet included in the package.
- Configure the core server to use the LANDesk Management Gateway. This configuration must be done from the console on the core server.
- Configure managed devices to connect through the LANDesk Management Gateway.

Configuring the core server

You must configure the core server to connect through the LANDesk Management Gateway before you configure managed devices to use it.

Note: The Configure LANDesk Management 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 LANDesk Management Gateway configuration.

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

Starting and stopping the LANDesk Management Gateway service

You can start or stop the LANDesk Management Gateway service by checking or unchecking **Enable gateway**. This setting also determines whether or not the LANDesk Management Gateway service starts when the appliance is restarted.

You can also use the start, stop, and restart buttons to start or stop the service as you are testing connectivity.

Configuring managed devices

There are three options for configuring managed devices to connect to the core through the LANDesk Management Gateway:

- Manually configure each managed device to connect through the LANDesk Management Gateway. This type of configuration enables LANDesk Management Suite and LANDesk Server Manager functionality through the appliance.
- "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 LANDesk 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 appliance 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 LANDesk Management 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. 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

Logging in to the LANDesk Management Gateway Web console

Note: To manage certificates or make changes to the appliance 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 **https://*hostname*/gsb** where *hostname* is hostname of the LANDesk Management Gateway.
3. Enter the user name and password (the default user name is **admin** and the default password is also **admin**).
4. Click **OK**.

Status

The information shown on the Status page is real-time information that you can refresh by clicking the **Refresh** button on your browser. This information can be useful for determining peak times of daily LANDesk Management Gateway usage.

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 LANDesk Management Gateway console. Note that the LANDesk Management Gateway can "see" more than one core, but each core can only see a single LANDesk Management Gateway.

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 LANDesk Management Gateway Web console

1. Open the certificate you want to add in a text editor.
2. Copy the entire body of the certificate.
3. From the LANDesk 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 LANDesk 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 LANDesk Management Gateway Web console

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

This is a read-only list of blocked certificates. You can only add certificates to the blocked client certificates list from the console on the core server.

Configuring the LANDesk Management Gateway service

You can change the following LANDesk Management Gateway service configuration settings:

- **Verbosity of log messages**: The amount of detail saved to the system log file.
- **64-bit encryption**: Whether 64-bit encryption is enabled or disabled.
- **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 LANDesk Management Gateway.
- **Additional host names**: A space-separated list of other host names or IPV4 dotted decimal addresses by which this appliance 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 LANDesk Management Gateway service configuration

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

Configuring system settings

Date and time settings

The options on the **Dave/time settings** tab let you change the date, time, and time zone settings used by the LANDesk Management Gateway.

To configure Date/time settings

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

Network settings

The options on the **Network settings** tab let you configure the network settings used by the LANDesk Management Gateway.

Use the **Device settings** to add or remove IP addresses for NIC 1 (Eth0) and NIC 2 (Eth1). Each NIC may be configured to have multiple addresses, allowing access to different networks. Use the **DNS settings** to specify the DNS server(s) that will be used by the LANDesk Management Gateway for name resolution (you can also specify DNS suffixes that you want to append to the search). Use the **Hostname settings** to configure the name and domain of the appliance itself.

To configure Network settings

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Network settings** tab.
3. Under **Device settings**, add IP address, netmask, and gateway for either NIC, then click **Add**, or click the **Delete** button associated with an address you want to remove.
4. Under **DNS settings**, add or delete DNS servers. You can also add and save any DNS suffixes that you want to append to the search.
5. Under **Hostname settings**, make any changes to the hostname and domain.
6. Click **Save**.

Updates

The options on the **Updates** tab let you download and apply software updates to the LANDesk Management Gateway.

To find and apply updates

1. From the LANDesk Management Gateway console, click **System**.

2. Click the **Updates** tab.
3. Click **Scan for updates** to check the LANDesk patch server for any available updates.
4. Select any desired updates from the **Available updates** list and click **Apply**.

Back up and restore

The options on the **Backup and restore** tab let you create and manage backup files of the LANDesk Management Gateway configuration. These files can be used to restore all configurable settings.

The LANDesk Management Gateway stores the 14 most recent backup files, deleting the oldest of the 14 files each time a new backup is created.

To back up the current configuration of the LANDesk Management Gateway

In addition to the LANDesk Management Gateway's automatic timed backups, you can create a backup file of the appliance's current configuration at any time.

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Back up and restore** tab.
3. Click **Back up now**.

To restore a configuration from the Backup files list

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Back up and restore** tab.
3. Click the **Restore** link for the backup file containing the system configuration you want to restore.

Important: When you restore a backup, the LANDesk Management Gateway password is reset to **admin**. After logging in, you should change the password to a strong password.

To export a backup file to another location

You can export (save) a backup file to another location, such as a thumb drive or the hard drive of a machine from which your are browsing to the appliance. This lets you save the backup configuration for later use or to configure another LANDesk Management Gateway appliance. Because the appliance stores only the 14 most recent backups, exporting can be used as a safeguard to ensure that important backup files are not deleted.

You cannot export files if you are connected directly to LANDesk Management Gateway. This functionality is only available if you are browsing to the appliance from another machine.

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Back up and restore** tab.
3. Click the **Export** link for the backup file you want save to another location.
4. Browse to the desired location and save the file.

Important: Do not rename the backup file or you will not be able to import it later.

To import a backup from another location

To restore a backup from another location, you must first import it to the **Backup files** list.

You cannot import files if you are connected directly to LANDesk Management Gateway. This functionality is only available if you are browsing to the appliance from another machine.

1. From the LANDesk Management Gateway console, click **System**.
1. Click the **Back up and restore** tab.
2. Click **Browse**.
3. Navigate to the backup file you want to import.
4. Click **Open**.
5. Click **Import** to add the file to backup list

You can now restore the backup configuration.

To change backup frequency

By default, the LANDesk Management Gateway creates weekly backup files. You can change the frequency to monthly. Remember that the appliance stores only the 14 most recent backups.

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Back up and restore** tab.
3. Select the desired **Backup frequency**.
4. Click **Save**.

Appliance

The options on the **Appliance** tab let you reboot or shutdown the LANDesk Management Gateway.

To reboot or shut down the LANDesk Management Gateway

1. From the LANDesk Management Gateway console, click **System**.
2. Click the **Appliance** tab.
3. Click **Reboot** or **shutdown**.

Configuring security settings

Firewall settings

Firewall settings let you block specific addresses and address ranges from connecting to the LANDesk Management Gateway. You can also create and manage a "white list" of specific addresses and address ranges which are allowed to connect to the LANDesk Management Gateway. Make sure that any addresses added to the Allowed address list are completely trusted. An address cannot exist in both the Blocked and Allowed address lists at the same time.

To enable or disable the Blocked addresses and Allowed addresses lists

1. From the LANDesk Management Gateway console, click **Security**.
2. Under **Firewall settings**, click **Enable** or **Disable**.

To add an address to the Blocked addresses or Allowed addresses list

1. From the LANDesk Management Gateway console, click **Security**.
2. Under **Firewall settings**, type the address in the appropriate **Add** field, then click **Add**. 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 or Allowed addresses list

1. From the LANDesk Management Gateway console, click **Security**.
2. In the appropriate list under **Firewall settings**, highlight the address you want to remove, then click **Remove.**
3. Click **Save**.

Trusted services settings

Trusted services settings let you specify which services are allowed for each network device. For example, if your LANDesk Management Gateway is configured with an inward facing NIC and an outward facing NIC, you will probably want to require more security on the outward facing NIC.

To specify trusted services for network devices

1. From the LANDesk Management Gateway console, click **Security**.
2. Under **Trusted services**, select the network device for which you want to specify trusted services.
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 the LANDesk Management Gateway.
- **Non-administrator**. A non-administrator can remote control other devices.

Notes:

- You must use strong passwords which are at least eight characters long and include at least one lowercase letter, one uppercase letter, one number, and one symbol.
- 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. From the LANDesk Management Gateway console, 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. From the LANDesk Management Gateway console, 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. From the LANDesk Management Gateway console, 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. From the LANDesk Management Gateway console, click **Users**.
2. Select 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 LANDesk 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.
- **LANDesk Management Gateway connection table:** Shows all current connections to the appliance. This report is included as a diagnostic tool in the event that you ever require technical support.
- **Gateway service status:** Shows statistics about the LANDesk Management Gateway service.
- **System test:** Runs a series of test scripts that can be used to troubleshoot appliance configuration.

To view a report

1. From the LANDesk 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 appliance 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 LANDesk 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 appliance (see *Configuring managed devices*), 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 User's 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 LANDesk 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 appliance 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 2.6.20.4. This version is open source and contains no proprietary components.

Can the Linux version be patched or upgraded?

No. The LANDesk Management Gateway appliance should not be modified. LANDesk will make available any recommended bug fixes or upgrades.

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 LANDesk Management Gateway to the core.
- If you specify a user name and password, clicking **Test** tests the connection through the LANDesk 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 LANDesk Management Gateway service (click **Configuration | LANDesk 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 **ProgamFiles\LANDesk\ManagementSuite\brokerreq** to see if a **.csr** file has been created.

If a .crs 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 LANDesk Management 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 LANDesk Management 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 LANDesk 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 LANDesk Management Gateway address.

1. From a command prompt on the managed device, enter **BrokerConfig.exe**.
2. Click the **Gateway information** tab.
3. Specify the LANDesk Management 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 LANDesk 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 LANDesk Management Gateway, and the "Test settings" button returns a "Settings test successful" response, but managed devices are unable to connect to the core though the LANDesk Management Gateway.

This can occur if the core is configured to connect to the LANDesk Management Gateway through a proxy, but you did not specify proxy settings from the **LANDesk 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 **LANDesk Management Gateway configuration** dialog will use those settings and will succeed, but the LANDesk Management Gateway service will not use them and will fail to connect. The BrokerService.log file may state that the LANDesk Management Gateway service was unable to connect to the LANDesk 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 | LANDesk 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 LANDesk Management 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 LANDesk Management Gateway Web interface, you can remove the lockout from the LANDesk Management Gateway administrator console.

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

A CRT monitor connected directly to the LANDesk Management Gateway does not display correctly.

If you encounter display problems when connected directly to the appliance, you may need to reset the screen resolution setting on the LANDesk Management Gateway.