Intel® LANDesk® Server Manager 6

Administrator's Guide

Intel Corporation
5200 N. E. Elam Young Parkway
Hillsboro, Oregon 97124-6497

Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

“Year 2000 Capable”
An Intel product, when used in accordance with its associated documentation, is “Year 2000 Capable” when, upon installation, it accurately stores, displays, processes, provides, and/or receives date data from, into, and between the 20th and 21st centuries, including leap year calculations, provided that all other technology used in combination with said product properly exchanges date data with it.

part number 712901-002

Contents

1 Introduction to Intel® LANDesk® Server Manager

This chapter gives a brief introduction to Intel® LANDesk® Server Manager by answering the following questions:

- What is Server Manager?
- What are Server Manager’s hardware components?
- What are Server Manager’s software components?
- What is Server Manager “at-a-glance”?
- How do I use this guide?

What is Server Manager?

Server Manager combines hardware and software to help you manage your servers. Use Server Manager to:

- Monitor critical server functions.
- Receive alerts when server problems or events occur, such as low disk space, extreme voltage fluctuations, or a hung server.
- Set an automatic temperature-based shutdown to protect your servers from overheating.
- Maintain a history log of server data.
- Track trends using a printed history log.
- Diagnose server problems.
- Remote control servers over the network or phone lines.
- Power down or up servers remotely.
- Access a server even when power is lost or the network isn’t functioning.
- View a hung server screen.
- Access server POST codes and alerts that are stored in the Intel remote management card’s non-volatile RAM. This information is accessible even when power to the server is lost.

What are Server Manager’s hardware components?

Server Manager’s hardware components consist of the following:

- Intel remote management card (IRMC)
- Intelligent Power Module (IPM)

Intel remote management card

The Intel remote management card (IRMC) is a PCI card that monitors and controls a wide range of server hardware. Because the IRMC contains its own microprocessor, RAM, power cord and plug (with optional backup battery pack), network connector, and modem connector, it can continue to function as a separate hardware entity even if its host server is hung or has lost power. With the IRMC in a server, you can manage a hung server via modem when normal access channels are no longer available.

Intelligent Power Module

The Intelligent Power Module (IPM) is a separate power switch that enables the remote management card to control server power, turning the server on or off at your command or when the critical temperature threshold is exceeded.

What are Server Manager's software components?

Server Manager's software components consist of the following:

- Server Manager console software
- Server Manager agent software
- Alert Management System² (AMS²) software
- Desktop Management Interface (DMI) software

Server Manager console software

You can install the Server Manager console software on a centralized computer running Windows* 95 or Windows NT*. With console software, you can easily administer remote servers running the Server Manager agent software. The Server Manager console enables you to monitor and manage critical server parameters such as:

- Volume space used
- Number of server connections used
- CPU utilization

You can also create history files to keep a record of what happens to graphable parameters on your server during a specified time period. Use history files to see what happened on your server before a particular event, such as a server going down. From the Server Manager console, you can also configure alerts and remote control servers on your network.

Server Manager agent software

The Server Manager agent software runs on any NetWare* 3.12, 4.1, or 4.11 server or any Windows NT 3.51 or 4.0 server in your network environment. This agent monitors the server on which it's installed and provides information to the Server Manager console. The Server Manager agent also communicates with the IRMC to monitor and provide critical information about the server's health and hardware status.

Alert Management System²

The Alert Management System² (AMS²) is software that works with Server Manager to provide you with alerting capabilities. See chapter 4 for more information regarding the Alert Management System².

Desktop Management Interface (DMI)

Desktop Management Interface (DMI) is a standard, created and managed by the Desktop Management Task Force (DMTF), for managing computer system components. Examples of components are network adapters, motherboards, and software applications.

Components must provide a Management Information Format (MIF) file to be DMI compliant. MIF files are essentially text files that store data describing a component's manageable attributes. For example, the fan type or hard drive description are attributes that could be listed in a MIF file.

Ideally, DMI-compliant components also provide component instrumentation. With DMI instrumentation, you can read attribute values in real time. For example, if a DMI-compliant component, such as a motherboard, provides instrumentation to query the motherboard's voltage, you can use Server Manager to read the voltage information.

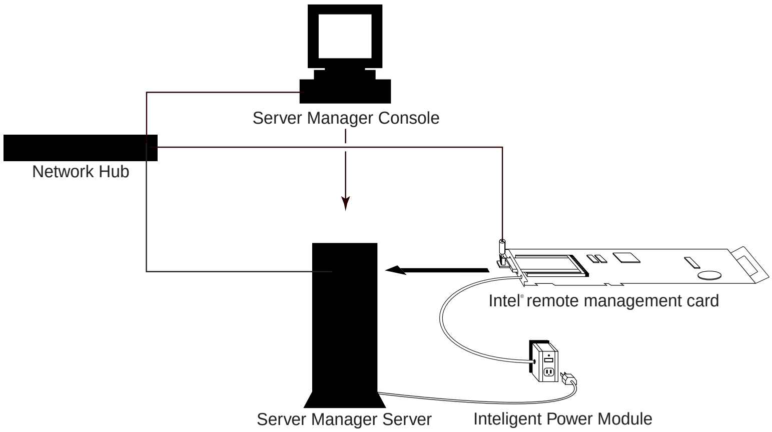
The Server Manager software component that monitors DMI instrumentation is the DMI Service Provider. It runs as a service (Win32sl) on Windows NT servers, and as an NLM (NWSL.NLM) on NetWare servers. See the Server Manager Tutorial for more information about using DMI in Server Manager.

For more information about DMI , DMTF, instrumentation, or MIF files, visit the following site on the World Wide Web:

http://www.dmtf.org.

Server Manager “at-a-glance”

Component	Definition
Server Manager console	The user interface.
Server Manager server	A managed server that has Server Manager agent software installed on it.
Intel remote management card	The hardware card installed on a server that enables the console to manage the server (optional).
Intelligent Power Module	A separate power switch that enables the remote management card to control server power.



How do I use this guide?

This guide is not meant to provide comprehensive documentation for the Server Manager product, but rather to help you quickly learn some of Server Manager's common features. Use this guide to help you understand how to:

- Navigate and use the Server Manager console
- Configure console security
- View and organize server information
- Create and use health groups
- Remote control servers
- Configure and use several different types of alerts
- Access the Intel remote management card
- Use Server Manager's SNMP Trap Receiver
- View DMI information from supported components

You can find more information in the Server Manager console's online help by clicking Help | Help Topics.

Installing Server Manager
For detailed instructions on installing Server Manager, see the *Intel LANDesk Server Manager 6 Installation Guide.*

2 Using the Server Manager console

The Intel LANDesk Server Manager console gives you complete control over servers that have the Server Manager agent software and Intel remote management card installed. Read this chapter for details on:

- Navigating the console
- Console security (handling server credentials)
- Organizing server information
- Viewing server information

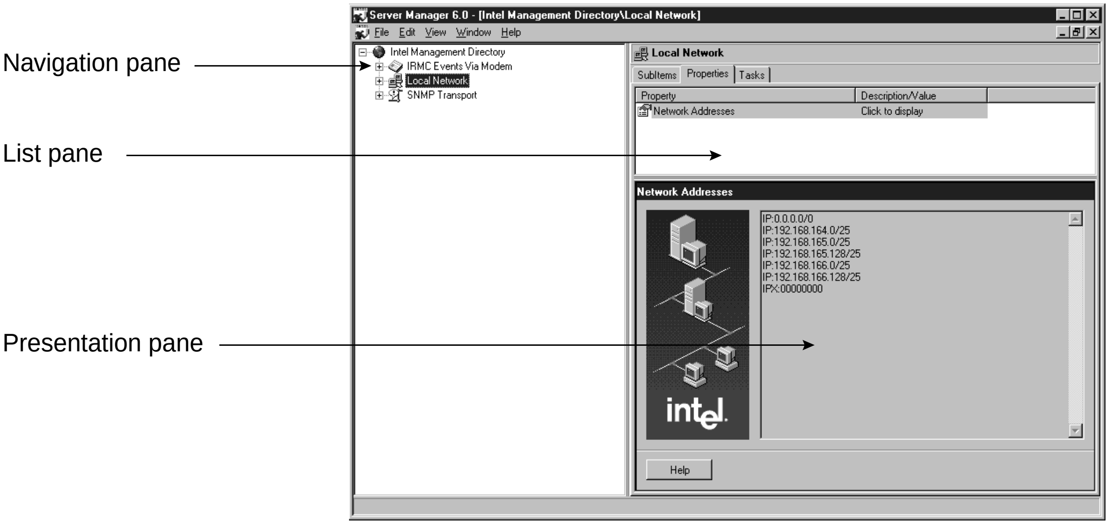
Navigating the console

Each time you run the Server Manager console, the Intel Management Directory displays as the root object in the console's navigation pane on the left.

To view other objects in the navigation pane, double-click the Intel Management Directory (or any other viewable object in the navigation pane) to expand it.

The console is divided into three main panes:

- The navigation pane
- The list pane
- The presentation pane



Property	Description/Value
Network Addresses	Click to display

```
IP:0.0.0.0/0
IP:192.168.164.0/25
IP:192.168.165.0/25
IP:192.168.165.128/25
IP:192.168.166.0/25
IP:192.168.166.128/25
IPX:00000000
```

Objects display in the navigation pane on the left. Attributes and information for the selected object appear in the list pane on the right. What appears in the presentation pane depends on what is selected or active in the list pane. What appears in the list pane depends on what is selected or active in the navigation pane.

Using the list pane's tabs

The tabs in the list pane present several actions you can take with respect to the object selected in the navigation pane. Depending on what's active in the navigation pane, all three tabs may or may not be available.

Tab	Description
Subitems tab	Displays subitems that exist for the active object in the navigation pane. You can view these same subitems in the navigation pane by double-clicking the item to expand the tree.
Properties tab	Displays the properties for the active object in the navigation pane. At times, you can edit these properties. The standard headings found under properties are: • Name (of the property) • Value (the number or text of the property)
Tasks tab	Contains step-by-step tasks or "wizards" that you can perform for the active object in the navigation pane. The standard headings found under the Tasks tab are: • Task Name • Description (of what the task does)

Console security (handling server credentials)

Each server running the Server Manager agent requires a username and password before you can access it in the Server Manager console. The default username and password are “root” and “calvin.” This default user can’t be removed, but you can change its password. For security, you should change the default user’s password on each server listed in the Server Manager tree as soon as you install Server Manager.

To change the username and password on a server

1. From the tree, double-click Intel Management Directory.
2. Double-click Local Network.
3. Double-click one of the network types.
4. Double-click the server whose username and password you want to change.
5. When prompted for the credentials, enter the current username and password for the server, such as “root” and “calvin.” The username and password are case sensitive.
6. After logging on to the server, click the Tasks tab.
7. Click the Configure Server Users task.
8. Add, edit, or delete user accounts for Server Manager users allowed to access this server.

   You can edit the default user account’s password, but you can’t delete it or change its access privileges.
9. Repeat this process for other servers on your network.
10. Test the user accounts by accessing each server using the new usernames and passwords.

Once you have entered a username and password during a Server Manager session, Server Manager temporarily stores the login and tries to use that username and password combination on all servers you access in the tree during that same session. This keeps you from being required to enter the same username and password for multiple servers.

Organizing server information

Server Manager recognizes both Windows NT and NetWare servers, and separates those servers into different network groups. The first time you expand a network group in Server Manager, it discovers the servers on that network or subnet running Server Manager. Depending on the size of your network, and how many Server Manager servers you have, the discovery may take a few minutes. You can continue working in Server Manager while it's discovering servers.

Depending on how many Server Manager servers you've got, it may be tedious to scroll through a long list of servers. Server Manager lets you organize your servers into different server groups. For example, you may want to group your servers based on:

- Geographic location
- Organization or department
- Server type (file or production)

Adding a network group

You can create a custom network group that works like the default Local Network group, and contains NetWare and Windows NT subitems. Use either IPX* or IP address ranges to specify the subnet discovery range.

To add a network group

1. From the tree, click Intel Management Directory.
2. From the Tasks tab, click Add a Network and complete the task.

For more information on completing tasks, click the Help button at the bottom of the presentation pane for the task.

Adding a server group

You can create server groups at Server Manager’s network level. For example, if you’re responsible for a subset of the total number of servers Server Manager discovers, you can put only those servers you manage into a group. This can be useful if you manage both NetWare and Windows NT servers and want to keep those servers under the same branch in the tree.

Server groups you create appear below the Local Network item but they aren’t filled with servers automatically. After you’ve created a group, you need to add servers to it.

To add a server group

1. From the tree, double-click Intel Management Directory and click Local Network.
2. From the Tasks tab, click Add a Device Group and complete the task.

With this task you are essentially naming an empty group. Once the group is created, you can then add servers to that group.

Adding servers to groups

Once you’ve created and named a group, you need to add servers to that group. You can either add Server Manager servers that are already listed elsewhere in the tree, or you can add new Server Manager servers.

To add servers to groups

1. From the tree, click the custom group name that you just created.
2. From the Tasks tab, click Add a Server/Workstation and complete the task.

Discovering servers on other networks

By default, Server Manager discovers manageable servers on your current network or subnet. If Server Manager isn’t displaying some servers that you know have Server Manager agent software, you need to point Server Manager to the network or subnet those servers are on so Server Manager can discover servers there too.

Use either IPX or IP address ranges to specify the network address.

To specify server networks to discover

1. From the tree, double-click Intel Management Directory and click Local Network.
2. From the Tasks tab, click Configure Network Group and complete the task.

Viewing server information

You can view several types of information about each server from the Server Manager console, including:

- Health
- Historical data
- Instrumentation
- Intel remote management card (see chapter 5 for more information)
- Snap-ins

Health

Health is a subitem of each server that appears in the navigation pane. When Health is expanded, health groups appear. Server Manager automatically creates ten sample health groups to get you started:

- Browser Group
- Data Map Hits %
- Logical Disk Group
- Memory Group
- Paging File Group
- Physical Disk Group
- Processor Group
- System Up Time
- Temperature Group
- Voltage Group

You can delete any of these health groups if you don't intend to use them, and create new groups based on your needs.

Health groups can't be renamed
Be careful in choosing the names for any new health groups you create because you can't rename a Health group once it's created. You can delete a group and create a new one using a new name, but if you've added sub-groups and parameters, this can involve several steps.

To create a new health group

1. From the tree, double-click Intel Management Directory.
2. Double-click Local Network.
3. Double-click one of the network types.
4. Double-click the server where you want to create a new health group and enter the username and password.
5. Click the Tasks tab.
6. Click Add a Parameter Group and complete the task.

To add a parameter to a health group

1. From the tree, double-click Intel Management Directory.
2. Double-click Local Network.
3. Double-click one of the network types.
4. Double-click the server containing the health group you want to add a parameter to. Enter the username and password if prompted.
5. Click the group you want to add a parameter to.
6. Click the Tasks tab.
7. Click Add a Parameter and complete the task.

Configuring a health parameter's thresholds

You can configure upper and lower thresholds for any health parameter. If a threshold is exceeded, it triggers an AMS² alert action for the health group if you configured the action to occur. For more information on alerts, see chapter 4. By default, thresholds are disabled for each parameter you add to a health group.

There are three possible thresholds you can set for each health parameter:

- Informational
- Warning
- Critical

Depending on the parameter you want to monitor, it's generally a good idea to configure all three thresholds for each parameter and not just one or two. Configuring all the thresholds ensures that you will be alerted regardless of the threshold level exceeded.

To configure parameter thresholds

1. From the tree, click the health parameter whose thresholds you want to configure.
2. From the Tasks tab, click Configure Thresholds and complete the task.

For more information on completing tasks, click the Help button at the bottom of the presentation pane for the task.

Viewing server health from the navigation pane

When a parameter threshold is exceeded, an icon appears in the tree representing the change in server health:

ℹ means that an information-level threshold was exceeded.

⚠ means that a warning-level threshold was exceeded.

❗ means that a critical-level threshold was exceeded.

Server Manager propagates the most critical health status of any *parameter* in a group to determine that *group's* health status. For example, if the Logical Disk Group's % Free Space exceeds a warning threshold, the entire Logical Disk Group will indicate a warning status.

Likewise, Server Manager propagates the most critical health status of any *group* to determine that *server's* health status. For example, if one health group has a status of Information, and one group has a status of Warning, the server health indicates a Warning status.

Health groups and alerting

Server Manager alerts are configured for an entire health group—you can't configure unique alerts for individual parameters. To configure an alert for a specific parameter, you must first add that parameter to a health group, even if it's the only parameter in that group.

Parameters within health groups can have thresholds that trigger alert AMS² actions at the group level. All parameters within that group share the alert action you configure on the group. If you need to configure different alert types for certain parameters, simply place them in different health groups.

Before configuring a unique alert action for parameters within a specific group, consider configuring AMS² alert actions based on severity instead. For example, you can group all critical parameters together, or group all parameters with the same alert action together. For more information on alerts, see chapter 4.

Historical data

Historical data includes two types of historical data:

- Server Alert Log
- History Log

Server Alert Log

All alerts generated on a server are stored in that server’s Alert Log. The Server Alert Log is a subitem of Historical Data for any server in the Intel Management Directory tree.

A list of alerts appears in the Alert Log with the following information:

- Alert Name
- Source
- Computer
- Date
- Time
- Severity

In addition to the basic information the Alert Log dialog displays, you can access more detailed information about each alert in the Alert Information dialog.

To access the Alert Information dialog

1. From the tree, click the server whose log you want to view.
2. Double-click Historical Data.
3. Double-click Server Alert Log.
4. Double-click the Alert Log item you want to view.

You can configure the Alert Log to display only those alerts that match conditions you specify.

To filter the Server Alert Log

1. From the tree, click the server whose log you want to view.
2. Double-click Historical Data.
3. Double-click Server Alert Log.
4. Right-click the Server Alert Log and click Properties.
5. Specify any filtering rules for the Alert Log and click OK.

Each server stores its own copy of the Alert Log locally. When you select a server and view its Alert Log, you're actually retrieving a copy of that server's Alert Log to your local console. Therefore, if that server isn't displayed or available, you won't be able to retrieve its Alert Log for viewing.

If you configure a threshold for certain events without configuring AMS^2 alert actions, the Alert Log still records that the threshold was exceeded. See chapter 4, “Configuring Alert Actions” for more information on alerts.

History log

One of Server Manager’s most powerful features is its ability to record the histories of graphable parameters. Histories provide access to past information about parameter values that you can use for diagnostics and baselining. Baselining gives you a measure for comparing current performance against normal performance.

After installation, Server Manager automatically starts a 24-hour rolling history for several default parameters, such as Percent Processor Time and Free Disk Space. Histories are automatically stored in a server’s History Log.

To view a history

1. From the tree, click the server whose history you want to view.
2. Double-click Historical Data.
3. Double-click History Log.
4. Click the history you want to view.
5. In the list pane, click the History Graph for either actual data or averaged daily data.

To start a history for a Server Manager 2.x server

1. In the Intel Management Directory tree, double-click a 2.x server.
2. Double-click Tools.
3. Select the parameter you want to start a history for.
4. Click the Tasks tab.
5. Click Histories for SM 2.x and complete the Start/Stop Histories for Server Manager 2.x Servers task.

If a parameter history is currently running, stop the current history first. Otherwise, Server Manager assumes that the history is a rolling history or “continuing” history. For Server Manager to save a history file, the file must have a beginning and an end. Histories are automatically saved when you stop them. To delete a history, right-click the history and click Delete.

Instrumentation

Instrumentation contains various sources of real-time information about a server. These sources include DMI, Intel remote management card (IRMC), and NT Performance Monitor. Double-clicking these objects displays the server information from these sources.

Desktop Management Interface (DMI) is a standard for managing computer system components such as network adapters and motherboards. DMI instrumentation enables you to read a component's attribute values in real time. For example, if a DMI-compliant component, such as a motherboard, provides instrumentation to query the motherboard's voltage, you can use Server Manager to read the voltage information.

If your computer does not include any DMI instrumentation, Intel DMI Proxy and Win32 DMI Service Provider are the only groups included under DMI. (This information is not particularly useful in server management.)

Snap-ins

Snap-ins doesn't include any subitems unless you installed a Server Manager snap-in during installation, such as Intel LANDesk Client Manager console or APC PowerXtend* DMI software. (The APC software is found in the Plug_ins directory on the Server Manager CD.)

3 Managing servers with remote control

One of Intel LANDesk Server Manager’s most powerful features is its ability to remote control servers that have the Server Manager agents installed.

Read this chapter for details on:

- Remote controlling servers
- Using the Remote Control window
- Rebooting and controlling remote server power

Remote controlling servers

You can remotely monitor and control any Windows NT or NetWare server that the Server Manager console displays in its navigation pane.

Remote controlling a Windows NT server from Windows 95
Windows 95 consoles can remote control Windows NT servers only if both the console and the agent software is Server Manager 3.0 or greater.

When you remote control a server, Server Manager first attempts to connect you to that server by accessing the server’s agent software. If this fails (because the server is hung or in the process of booting), Server Manager attempts to connect to that server’s Intel remote management card 2 (IRMC 2) via the network. If this fails (because the network is unavailable), Server Manager attempts to connect to that server’s IRMC 2 via modem.

Regardless of the method used to remote control a server, the steps are the same.

To remotely connect to a server

1. From the console's navigation pane, click a remote server.
2. If prompted, enter your username and password to access the server. (The default username is "root." The default password is "calvin.")
3. Click the Tasks tab.
4. Click Remote Control Connection and complete the task.

Remote controlling servers with an IRMC 1 (ISA card)
If you attempt to remote control a server with a legacy IRMC 1 (ISA card), you may be prompted to indicate which method you want to use to remote control the server—either in-band (via network) or out-of-band (via modem).

To connect to the Intel remote management card (IRMC) via modem, your console computer must be equipped with a modem. You must also configure the IRMC's modem to communicate with your console computer's modem.

Remote control security for Windows NT

Before you can remote control a server, you first must provide the proper credentials to access that server. (For more information, see "Console security (handling server credentials)" in chapter 2). On Windows NT servers, even if several authorized administrator accounts can access a server in the tree, you can restrict remote control access to only certain users.

Server Manager's Windows NT remote control viewer uses a security system that is based on Windows NT users and groups—the same users and groups that you see in the Windows NT Server's User Manager for Domains (or Windows NT Workstation's User Manager). When you install the Server Manager agent on each server, you specify a Windows NT group that is authorized to remote control that server. Setup defaults to the "administrators" group. The group name you specify (such as "administrators") is entered into the following registry key on that server during Server Manager installation:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\WUSER32\
PermittedViewers
```

After installing Server Manager on a server, you must access User Manager for Domains to add or remove users who are authorized to remote control that server.

To add or remove remote control users

1. At the server you want to modify remote control access to: From the Windows NT Start menu, click Programs | Administrative Tools | User Manager for Domains.
2. Double-click the User Manager group you want to modify (such as Administrators).
3. Use the Add and Remove buttons to add or remove users from the group.
4. When finished, click OK.

To change the group name, you must edit the Windows registry
If you want to change the name of the Windows NT users group you entered during installation (for example, from “Administrators” to “RCUsers”), you need to edit the server’s registry key HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\WUSER32\PermittedViewers.

When you start a session, the remote control viewer first tries the username and password you used to log onto your Windows NT domain. If the server you’re viewing is a member of the same domain, and your username is a member of a group with permitted viewer rights, remote control proceeds immediately.

If the username and password you used to log onto your Windows NT domain isn’t recognized as a permitted viewer, the credentials dialog appears.

In the credentials dialog, you need to enter a username and password for an account that is a member of a permitted viewers group. In the Domain field, type the domain name that contains the authorized remote control user account, or leave it blank if the user account is on the server you’re attempting to remote control.

Domain accounts and local computer accounts
Remote control can use Windows NT user accounts on the domain level and the local computer level. When adding user accounts to permitted viewer groups, you need to remember if the user accounts came from domains or from a local computer account. This affects what you type in the credentials dialog’s Domain field.

Remote control security for NetWare

Server Manager does not provide any additional remote control security to NetWare servers. Any administrator account that can access a NetWare server can also remote control it.

Using the Remote Control window

The Remote Control window functions like any other window. You can minimize it and work in other applications on your computer. The Remote Control window has a yellow and black moving border that distinguishes it from a standard window.

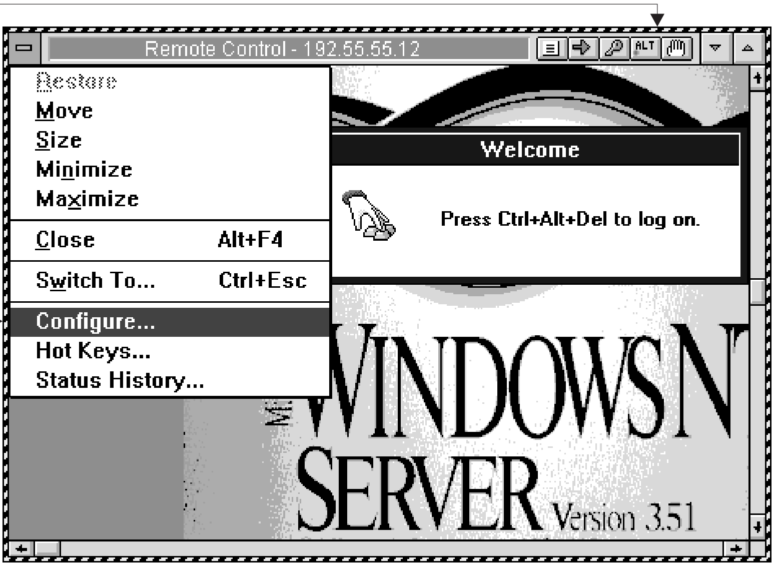
The Remote Control window automatically handles different source and destination screen resolutions and color depths and also has control options and hot keys to handle the following:

- Window performance
- Keyboard commands
- Viewing controls
- Navigation

Access the control menu of the Remote Control window to set these options, as shown in the following graphic.

Click one of the title bar buttons to adjust how the Remote Control window works.

Click the control menu and choose Configure to adjust the Remote Control window.



Close down remote control sessions before exiting
Exit the Server Manager console only after you've ended all remote control sessions.

Remotely rebooting and controlling server power

From the console, you can request that the IRMC perform a warm reboot of the server. If the server supports it and the Intelligent Power Module (IPM) is attached, you can also perform a hard reset, power up, or power down.

When you remotely power down a server, the IRMC may or may not continue operating on its backup power. If the server operating system is shut down normally before the server loses power, the IRMC interprets this as a normal situation and turns itself off when the server is turned off. If the server operating system isn’t shut down normally and the server loses power, the IRMC considers this an unusual situation and continues operating on backup power.

If you connect to the IRMC via modem and turn off the server via remote control, the IRMC stays active on backup power.

Check NLMs and services before powering down a server
If the Server Manager NLMs or Windows NT services are not loaded and you choose to reset or power down a server, the result is an immediate shutdown. This can result in lost data, since system buffers aren’t flushed properly.

Remote control limitations

If you attempt to remote control a server that uses a different keyboard mapping than the Server Manager keyboard, you may experience some problems when typing.

On a server that has an AGP video card and the IRMC 2 installed, you will experience these limitations:

- Depending on the system BIOS, you may not be able to remote control the server until after the software agent has loaded. This means you may not be able to see the server’s boot sequence via remote control.
- On a NetWare server running only IPX (without IP), you may not be able to remote control the server.

To enable remote control for these situations, use a PCI video card.

4 Configuring alert actions

Intel LANDesk Server Manager uses a software tool called Alert Management System² (AMS²) to alert you about server activity.

Read this chapter for details on:

- What is AMS²?
- How alerting works in Server Manager
- Configuring AMS² alert actions
- Viewing the Server Alert Log

What is AMS^2?

The Alert Management System^2 (AMS^2) is an Intel technology used by several LANDesk products. You configure AMS^2 to send different types of alerts when certain events occur with computers and servers on the network. These alert types include:

- Displaying a message box
- Sending a page
- Sending Internet mail
- Running a program
- Sending a network broadcast
- Sending an SNMP trap
- Writing to the Windows NT Event Log
- Loading a NetWare NLM
- Sending an Intel remote managment card (IRMC) page

For example, you can configure Server Manager to page you if a temperature threshold is exceeded on a server. If a threshold is crossed, AMS^2 responds by attempting to send a pager message you configure. Regardless of the AMS^2 alert action, the event is logged in the Alert Log.

How alerting works in Server Manager

You can configure alerts for parameter groups only, not individual parameters. When a parameter in a certain health group exceeds a threshold, an alert that you've configured for that group is triggered. For example, if a warning threshold you set for a parameter in the Memory Group is exceeded, the Memory Group sends the warning alert that you configured.

When you configure alert actions, select the group containing the parameter you want to alert on. The Configure Event Actions task is only available when you've selected Health or a health group, or one of the IRMC 2 alerting groups.

When you create an AMS² alert event for a parameter group, AMS² displays a folder called Data Groups that contains two alert objects. The *group* object object contains primary alert actions that will run whenever this alert event is triggered; the *default alert* object contains backup alert actions that only run if none of the primary actions successfully run. Expand these objects to see the alerts actions currently defined for them.

Working with alertable parameters

There are two alertable parameter types in Server Manager:

1. Graphable parameters that have three independently configurable thresholds: informational, warning, and critical.
2. Event-only parameters that track NetWare operating system events only, such as an NLM loading.

When these parameters exceed the thresholds you set, Server Manager sends an alert to AMS², which executes any alert actions you've configured, such as sending a page or executing a program.

When you configure alert conditions on a parameter, such as configuring a threshold, those alert conditions are global for all Server Manager consoles. Any console you go to will show the same alert conditions for the parameter you select.

Configuring AMS² alert actions

Each AMS² alert action configuration task is explained in this chapter. Because much of the detail is common to all tasks, here are some things to consider:

- When you select an alert action to configure, Server Manager looks on the network to find all of the computers running AMS² that can execute this alert action. This process takes several seconds, especially the first time it occurs.
- In the Select Action Severity dialog, the OK alert is included so Server Manager can alert you when the conditions triggering another alert correct themselves. For example, if you receive a warning alert indicating low disk space on a server, and the problem corrects itself, Server Manager sends you an OK alert (if this option was selected).
- For alert actions that generate messages (such as Message Box, Broadcast, Pager, and Internet Mail) the message is composed of text and alert parameters. (The Alert Parameters list usually includes host name, date, time, severity, alert name, and alert value. This list may vary, however, depending on the selected alert.)
- You can enter about 500 characters of message text in each alert action’s Message dialog (including parameters). The Message dialog contains two list boxes. The Message box contains the text of the message you want to send. The Alert Parameters list contains any parameters you want included as message text. (Alert parameters are delimited by the “<>” characters when you insert them into the message text.) To quickly create a message, click the Default button to use default message information for an alert action.
- When an alert occurs, each parameter placeholder you add to the Message box is replaced in the alert message with corresponding alert information.
- You can test alert actions you configure to make sure they work as expected. To do so, select the configured alert action and click the Test Alert Action button.
- Once you’ve configured an alert action, the action appears in the Configure Event Actions dialog under the parameter you configured the action for.

Configuring the Message Box alert action

The Message Box alert action displays a message box on the computer you specify. You can select whether the message box sounds a beep when it appears and whether the message box remains on top until cleared.

To configure a Message Box alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Message Box.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the Message Box dialog, specify the display options and click Next.
10. In the Message dialog, enter the action name. Then, type message text in the Message box and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.
11. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Send Page and Send IRMC Page alert actions

The Send Page and Send IRMC Page alert actions send a pager message to the pager number you specify. The Send Page alert originates a pager alert from the server and sends it over the network. The Send IRMC Page originates the alert at the IRMC 2 and sends it over the IRMC 2’s modem. They perform essentially the same function but use a different channel in case one channel is unavailable. You can configure the pager alert using the more reliable method in your particular network environment, or both methods if you want increase fault tolerance for pager alerts.

Any computer you configure a pager action on needs to have a modem. You should test Pager alert actions to make sure they work as expected.

Configuring a pager alert action requires two major tasks:

1. Configuring a modem for AMS².
2. Configuring the Send Page or Send IRMC Page alert action.

To configure a modem for AMS²

1. From Windows Explorer, double-click MODEMCFG.EXE. On Windows NT computers, this utility is in the WINNT\SYSTEM32\AMS_ii directory. On Windows 95 computers, it’s in the WINDOWS\SYSTEM\AMS_ii directory.
2. Click the COM port the modem uses in the Com Port drop-down list.
3. Click the correct modem type in the Modem Type drop-down list.
4. Click OK to save these settings.

To configure the Send Page or Send IRMC Page alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Click Send Page or Send IRMC Page, then click Next.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. Enter your pager access telephone number, pager I.D. number, password, and paging service name. If your paging service is in the Service drop-down list, these parameters are configured automatically when you select the service.
10. Click Settings to ensure that your paging service settings are configured properly. Click OK and Next.
11. In the Message dialog, enter an action name. Then, type message text in the Message box and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.

    The Pager alert action supports both alphanumeric and numeric-only pagers (numeric-only pagers are often called beepers).

    If you’re paging an alphanumeric pager, the message can include any text you type and information from the alert that generated the message. This message shouldn’t exceed the maximum number of characters your paging service supports; otherwise, you could get a truncated message.

    If you’re paging a numeric-only pager, you can only send numbers. Server Manager has an assigned list of numbers for each problem or event that generates an alert action. For the complete list of numbers and their assigned actions, see HOBLOCAL.TXT in the WINNT\SYSTEM32\DRIVERS directory.
12. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Send Internet Mail alert action

The Send Internet Mail alert action sends an Internet mail message to the user you specify. When using the Send Internet Mail alert action, you need to also specify the SMTP Internet mail server that the alert action will send the message through. If you specify the mail server by name, you need to have a DNS server configured so that the Send Internet Mail alert action can resolve the server's IP address. If you don't have a DNS server, you can enter the mail server's IP address directly.

This alert action only works if you have access to an SMTP Internet mail server at your site.

To configure the Send Internet Mail alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Send Internet Mail.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. Enter names in the Internet Address, Sender Name, Subject, and Mail Server fields, then click Next.
10. In the Message dialog, enter an action name. Then, type message text in the Message box and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.
11. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Run Program alert action

The Run Program alert action runs a program on the computer you select. You must complete two fields in the Run Program dialog.

The Command Line field should contain the full path to the program you want to run and any command line options for that program. If you're running the program on a remote computer, the path you enter needs to be the path to the program from that computer. You can click the Browse button to browse for the program.

If you're running a Windows program, you can select whether that program runs in a normal or minimized state. This option has no effect on DOS* programs.

To configure the Run Program alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Run Program.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the Program field, enter a full path and filename. Click the Browse button if you need to browse the directory to locate the executable file. In the Command Line field, you can enter any command line options you want the program to use.
10. Select a Window state, either normal or minimized.
11. Click Finish.

Configuring the Broadcast alert action

The Broadcast alert action sends a network broadcast message to every computer that has a drive mapped to the action computer.

Configuring broadcasts from a Windows 95 console
To enable broadcasts from Windows 95 consoles, you must have the WINPOPUP.EXE utility loaded when the alert action occurs. WINPOPUP.EXE is usually located in the WINDOWS directory.

To configure the Broadcast alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Broadcast.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the Message dialog, enter the action name. Then, type message text in the Message box and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.
10. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Send SNMP Trap alert action

AMS² can generate an SNMP trap when an alert happens. The Send SNMP Trap alert action sends an SNMP trap to the SNMP consoles you specify, including Server Manager consoles. These alerts can also be sent to other SNMP consoles, such as HP OpenView* NNM, Tivoli* NetView, and CA Unicenter* TNG. For more information about integrating Server Manager with these SNMP consoles, visit this web site: http://www.intel.com/network/aims.

You can use Server Manager to view SNMP traps
If you don't have an SNMP management console, you can still view traps with Server Manager's Trap Receiver.

You must specify the address (either IP or IPX) of the computers that you want SNMP traps sent to. The following sections describe how to configure trap destinations for the operating systems Server Manager supports.

To configure trap destinations for Windows NT 4.0 servers

1. From the Windows NT server's Control Panel, double-click the Network icon.
2. Click the Services tab.
3. Select the SNMP Service item, then click Properties.
4. Click the Traps tab.
5. In the Community Name drop-down list, select “public.” If there is no public entry in the list, type it in, then click Add.
6. Once you've selected the “public” community name, click Add below the Trap Destinations list.
7. Enter the addresses of the computers you want traps sent to, then click Add.
8. Click OK, then Close.

To configure trap destinations for NetWare 4.x servers

1. From the NetWare server, type:

   ```
   load install
   ```

2. Click Product Options.
3. Click Configure Network Protocols.
4. Click Protocols.
5. Click TCP/IP. Ensure that TCP/IP is enabled.
6. Click SNMP Manager Table.
7. Enter the addresses of the computers you want traps sent to, then click Add.

NetWare 3.12 and 4.x traps function only if IP is running
Additional files may be required from NetWare for SNMP to function properly.

To configure the Send SNMP Trap alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click SNMP Trap.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the Message dialog, enter the action name. Then, type message text in the Message box to display in the SNMP trap and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.
10. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Write to Event Log alert action

The Write to Event Log alert action creates an entry in the Windows NT Event Log's Application Log. This entry is logged on the computer where the alert came from. This alert action is available only on Windows NT servers.

To configure the Write to Event Log alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Write to Event Log.
7. In the Select Action Computer dialog, select a computer to execute the action, then click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the Message dialog, enter an action name. Then, type message text in the Message box and move the available parameters you want from the Alert Parameters list to the Message box. Or, click Default to use the default message information for this alert action.
10. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Configuring the Load an NLM alert action

The Load an NLM alert action loads a NetWare Loadable Module (NLM) on a selected NetWare server when the AMS² alert occurs. You must configure this alert to determine which NLM is loaded, and the server it loads onto. This alert action is similar to the Run Program alert action for a Windows NT computer.

To configure the Load an NLM alert action

1. Select the parameter group that you want to generate an alert on.
2. Click the Tasks tab.
3. Click the Configure Event Actions task.
4. Click Configure AMS2 Alerts and click Next.
5. From the Configure Event Actions dialog, double-click any group.
6. Double-click Load NLM.
7. In the Select Action Computer dialog, select the computer where you want the NLM to load, and click Next.
8. In the Select Action Severity dialog, select the severity levels you want to trigger the alert action, such as Information, OK, Non-critical, or Critical. Click Next.
9. In the NLM field, enter the path and NLM to load. (NetWare servers usually store NLMs in the SYS:SYSTEM directory.) For example, use the system path such as SYS:SYSTEM\TEST.NLM. Don’t use drive letter mappings from your computer such as T:\SYSTEM\TEST.NLM because the server doesn’t use these drive letters on its own hard disk.
10. In the Command Line field, enter any command line options you want the NLM to use.
11. Click Finish. The action name appears in the Configure Event Actions dialog beside this action.

Viewing the Server Alert Log

You can use Server Manager's AMS² Server Alert Log to view a list of all alerts generated by servers running Server Manager. You can configure the Alert Log to:

- Display only those alerts that match conditions you specify
- Display a specified number of entries

The list of alerts appears in the Alert Log dialog with this information about each alert:

- Alert name
- Source
- Computer
- Date
- Time
- Severity

To view the Alert Log

1. From the tree, double-click the server whose Alert Log you want to view.
2. Double-click Historical Data.
3. Click Server Alert Log.

In addition to the basic information the Alert Log dialog displays, you can access more detailed information about each alert in the Alert Information dialog.

Viewing detailed alert information

Detailed alert information appears in the Alert Information dialog and includes alert parameters, their values, and the action status of each alert.

The Alert Information dialog also displays this information:

Action status	Description
Action Type	The type of action generated by the alert, such as Message Box, Pager, Internet Mail, Execute Program, or Broadcast.
Action Name	A name given to the specific action.
Computer	The name of the computer that the alert was configured for.
Status	The status of the alert. The Status field can include pending, processing action, error, completed successfully, and failed to complete.

To view detailed alert information

1. From the Server Alert Log, double-click the alert you want to display detailed information for.
2. When you finish viewing the alert information, click Close.

Filtering the Alert Log display list

You can configure the Alert Log to display only those alerts that match specified criteria. You can filter which alerts display according to these parameters:

Filter	Description
Computer	Displays alerts from a specific computer.
Source	Displays alerts from the same type of alert source (such as Windows NT Performance Monitor) on one or more computers.
Alert	Displays all alerts with a specific alert name.
Maximum Entries	The maximum number of entries the Alert Log holds before deleting the oldest entries.
Severity	Displays only alerts matching the severity levels you select. In Server Manager, you can specify these severity levels: information, warning (non-critical), and critical.

To specify which alerts appear in the Alert Log

1. Right-click in the Alert Log, then click Options.
2. Select the filters you want to apply to the Alert Log list.
3. Click OK.

To specify the number of entries in the Alert Log

1. Right-click in the Alert Log, then click Properties.
2. Specify the number of log entries you want the log to hold.
3. Click OK.

Number of entries can be configured
You can independently configure the number of entries an Alert Log holds on each server.

Deleting Alert Log entries

You can delete entries in the Alert Log either individually or as a group.

To delete a single log entry

- Select the log entry you want to delete, right-click in the Alert Log, then click Delete | Selected Entries.

To delete multiple log entries

1 While pressing the Ctrl key, select the log entries you want to delete.

2 Right-click in the Alert Log, then click Delete | Selected Entries.

To delete all visible log entries

1 Adjust the log filters so only the entries you want to delete are visible.

2 Right-click in the Alert Log, then click Delete | Filtered Entries.

Copying Alert Log contents to the clipboard

You can copy Alert Log entries and their parameters to the Windows NT or Windows 95 clipboard, where you can then paste them to another application for printing or data analysis.

Only parameters visible in the log are copied. If you want to limit the number of entries the Alert Log copies to the clipboard, apply filters to limit the number of visible log entries.

To copy Alert Log contents to the clipboard

1 Adjust the log filters so that only the entries you want to copy are visible.

2 Right-click in the Alert Log, then click Copy.

5 Using the Intel remote management card

You can monitor your servers at all times with the Intel remote management card (IRMC).

For instructions on how to install the IRMC to a server, see the *Intel LANDesk Server Manager 6 Installation Guide*. Software-only versions of Server Manager don’t include the IRMC.

Read this chapter for details on:

- What is the Intel remote management card?
- Communicating through the Intel remote management card 2
- Configuring the Intel remote management card 2

What is the Intel remote management card?

The Intel remote management card (IRMC) is a computer on a card that extends your ability to manage servers. The IRMC provides additional parameters on which to view, graph, and configure events. It also provides dial-up communication so you can:

- Monitor the server's temperature and voltages
- View the server's most recent POST codes
- View the server's state table so you can review the most recent values for a number of critical server parameters
- Remote control the server by redirecting its screen to the Server Manager console
- Receive alerts from the IRMC about its host server

Server Manager supports two different versions of the IRMC—the IRMC 1, an ISA-based card shipped with Server Manager 3.0 or older, and the IRMC 2, a PCI-based card that ships with Server Manager 6.0.

This chapter describes how to work with the new IRMC 2. For information about the older IRMC 1, see the documentation that shipped with that card.

Communicating through the Intel remote management card 2

The Server Manager console can communicate with the IRMC 2 in one of two ways:

- If the network is functional, all communication is routed through the network.
- If the network isn't functional, the IRMC 2 can use its modem to communicate with a remote access server (RAS) that has network access to the console.

The diagram shows these two ways of communicating with the IRMC 2.

The IRMC 2 can use a RAS session to deliver alerts if the network goes down. An Alert Notification Phonebook lets you create definitions for multiple RAS servers, and choose what order the IRMC 2 calls those servers to establish a RAS session and deliver alerts.

You can also establish a RAS session from the Server Manager console to an IRMC 2 to perform all of the same functions that can be done over the network.

Configuring the modem

Settings for the IRMC 2’s modem are stored on the IRMC 2 itself. You need to enter the IRMC 2 modem’s phone number, speed, and communications strings to ensure proper communication to or from the IRMC 2.

To configure the IRMC 2 modem

1. In the Intel Management Directory tree, double-click a server.
2. Double-click Intel remote management card 2.
3. Click Modem.
4. Click the Tasks tab, click Configure the IRMC 2 Modem, and complete the task.

Once the modem is set up, the IRMC 2 can use it to dial out to a remote access server and deliver alerts if the network is down. The Server Manager console can also dial in to the IRMC 2’s modem through a RAS session for remote management.

Configuring the Alert Notification Phonebook

If the IRMC 2 can’t deliver alerts over the network, it uses its modem to initiate a connection with a remote access server that can handle the alert.

The Alert Notification Phonebook contains a list of RAS entries. Each entry contains the phone number and authentication information for a single remote access server. You can order the RAS entries to create a prioritized list. The IRMC 2 starts at the top of the list and attempts to deliver alerts to each remote access server until it succeeds.

To add a RAS entry to the Alert Notification Phonebook

1. In the Intel Management Directory tree, double-click a server.
2. Double-click Intel remote management card 2.
3. Click Alert Notification Phonebook.
4. Click the Tasks tab, then click Configure the IRMC 2 Alert Notification Phone Book.
5. Click Add Entries, then click Next.
6. Complete the task.

To edit a RAS entry to the Alert Notification Phonebook

1. In the Intel Management Directory tree, double-click a server.
2. Double-click Intel remote management card 2.
3. Click Alert Notification Phonebook.
4. Click the Tasks tab, then click Configure the IRMC 2 Alert Notification Phone Book.
5. Click Edit an Entry, then click Next.
6. Complete the task.

To reorder entries in the Alert Notification Phonebook

1. In the Intel Management Directory tree, double-click a server.
2. Double-click Intel remote management card 2.
3. Click Alert Notification Phonebook.
4. Click the Tasks tab, then click Configure the IRMC 2 Alert Notification Phone Book.
5. Click Change the Order of the Entries, then click Next.
6. Complete the task.

Configuring the Intel remote management card 2

You need to configure the IRMC 2 to communicate with Server Manager, both by network and by modem. You also need to configure any optional hardware sensors or options you’ve added.

Use the Configure the IRMC 2 task to complete this initial configuration process:

- **Configure the IRMC 2 Modem**—sets up the modem on the IRMC 2. This is described in more detail earlier in the chapter.
- **Configure the IRMC 2 Alert Notification Phone Book**—adds a single entry to the phonebook.
- **Configure the IRMC 2 IP Address**—lets you get an IP address for the IRMC 2 from DHCP, or lets you enter static a static IP address.
- **Configure IRMC 2 Instrumentation**—configures the IRMC 2 to monitor onboard and optional external sensors.

You can run these tasks separately, or you can perform them all at once using the Configure IRMC 2 task.

To configure the IRMC 2

1. In the Intel Management Directory tree, double-click a server.
2. Double-click Intel remote management card 2.
3. Click the Tasks tab.
4. Click Configure IRMC 2.
5. Choose the configuration tasks you want to perform, then click Next.
6. Complete the task.

6 Working with SNMP

Intel LANDesk Server Manager uses the SNMP Trap Receiver to manage SNMP traps generated by SNMP-compliant components you specify. You can then configure AMS^2 alert actions that respond to traps.

Server Manager also enables you to manage APC* UPS devices with PowerNet* SNMP adapters installed. With supported UPSs, Server Manager displays information about UPS voltage supplies and battery life, and enables you to remotely control power to servers connected to the UPS.

Read this chapter for details on:

- Understanding SNMP
- Viewing the SNMP Trap Log
- Generating AMS^2 alerts when an SNMP trap is received
- Managing APC UPS devices

Understanding SNMP

Simple Network Management Protocol (SNMP) is a message-based protocol proposed as an Internet standard for systems management in 1990. SNMP uses “traps” (notifications) to report exception conditions such as component failures and threshold violations.

SNMP has become widely used as a network management protocol for a variety of components such as routers, hubs, UPSs, network and disk controller cards, as well as servers themselves. SNMP is a valuable tool for network administrators, because each component on the network can automatically communicate small problems to a central console. You can use this information to troubleshoot and resolve developing problems before they cause system errors or even network failure.

The SNMP tools are available under the SNMP Transport item in the Intel Management Directory tree. When you double-click the SNMP Transport icon, the SNMP Trap Receiver and UPS icons appear.

SNMP shows up in the tree even if it’s not installed
If SNMP was not installed on your console computer when you ran the Server Manager Console Setup, the Setup program should have prompted you to install SNMP before continuing.

If you ignored the message and installed the Server Manager console without SNMP, the SNMP Transport icon still appears in the tree but isn’t functional. If you install SNMP on a Windows NT server after installing Server Manager, you must reinstall the Server Manager agents for SNMP to work properly.

Viewing the SNMP Trap Log

Server Manager’s Trap Receiver intercepts all SNMP traps (as defined in the initialization file, SNMPMON.INI) sent to the console and displays them in the SNMP Trap Log. The SNMP Trap Log window displays all SNMP traps that have been received since the last Server Manager session. When a trap arrives, the SNMP Trap Log window looks up the enterprise number in the trap message, and then scans the list of traps defined for that enterprise. If the enterprise isn’t found, no action occurs. If the enterprise is present but the specific trap number is not found, the Trap Receiver signals the alert at the default level for the enterprise. The alert default level is set in the SNMPMON.INI file.

The Trap Log window lists, in sequential order, the traps received from all active enterprises, even if the window wasn’t open when the trap arrived.

The Trap Log window consists of two main areas, an upper and a bottom area:

- The upper area displays the list of traps with an icon to indicate trap severity: failure, warning, or informational.
- The bottom area displays a description of the trap selected in the upper area.

Trap Receiver logs aren’t permanent
The Trap Receiver only receives traps when you have Server Manager running; once you close Server Manager, any traps you received are gone.

To view the SNMP Trap Log

1. From the tree, double-click the SNMP Transport item and click the SNMP Trap Receiver item.
2. From the Properties tab, click Traps Received. The Trap Receiver appears in the lower pane.

Column	Trap Log description
Server	Server that generated the alert. This is either a text name (if the Windows NT DNS can resolve the IP address) or an IP address.
Trap Name	A brief name identifying the trap received.
Owner	Owner name of the enterprise or the enterprise number as configured in the SNMPMON.INI. If the Trap Receiver can’t determine the owner name, the field reads “Unknown.”
Received	Date and time at which the alert occurred (displayed in short-form International Date & Time settings. For example, 06/07/96).
Description	Enterprise Alert description as read from the SNMPMON.INI file. If the Trap Receiver can’t determine the description of the alert, the field reads “Unknown.”

Displaying SNMP traps from other vendors

The SNMPMON.INI file contains the information needed to interpret SNMP traps and alerts and display them in the Server Manager console’s SNMP Trap Receiver. This file controls which traps the Trap Receiver recognizes, and initially includes support for APC UPS devices. You can receive alerts from these devices without making additional modifications to the SNMPMON.INI file. To enable alerting for other SNMP-compliant alerting devices, you must add the device’s enterprise and alert numbers to the SNMPMON.INI file.

The SNMPMON.INI file consists of three major sections:

- Enterprises
- Enterprise Traps
- Enterprise Alerts

Enterprises

The [Enterprises] section is a list of all vendors for which Server Manager monitors traps. The key for each entry is the Internet Assigned Numbers Authority (IANA) number for that manufacturer.

The value of the key contains the text name of the enterprise number and the default alert level for the enterprise. The valid values for the alert level are info, normal, warning, and failed (entry is not case sensitive). For example:

```
[Enterprises]
318=APC,Info
```

To add enterprises and specific alerts to the SNMPMON.INI file, consult your vendor to obtain the vendor’s IANA number and a list of trap numbers generated by the vendor’s SNMP agent, along with descriptions and alert levels. You should add an entry for each additional vendor to the [Enterprises] section as follows:

```
<IANA number>=<Vendor>,<Default Alert Level>
```

Enterprise Traps

The [Enterprise Traps] section is a list of specific traps for that enterprise. If a list of specific traps is not provided, a default trap is entered in the Trap Log. You can still configure actions on the default traps. When an SNMP trap arrives, the trap receiver looks up the enterprise number (such as 318 for APC) in the trap message, and then scans the list of specific traps for that enterprise. See the example below.

```
[APC]
1=None,Failure,Communications Lost
2=None,Failure,Overload
3=None,Failure,Diagnostics Failed
```

If the trap number is found, the Trap Receiver generates an alert with the specified alert level and text. The text to the right of the equal sign indicates a related alert. If the trap number is not found, the alert is signaled at the default level for the enterprise. If the enterprise is not found, no alert action occurs.

Enterprise Alerts

If you have a listing of specific alert numbers, you should then add an [Enterprise Alerts] section to the file. Add the [Enterprise Alerts] section to the SNMPMON.INI file in the following format:

```
[<Vendor>]
<Alert Number>=<Related Alert>,<Alert Level>,<Alert
Text>
```

The related alert value is required. Always set the related alert value to "None" when adding custom alert numbers. For example, to add a section for vendor XYZ, with 675 as the alert number, make the following entries to the SNMPMON.INI file:

```
[XYZ]
675=None,Warning,XYZ Unit Needs Attention
```

To edit the SNMPMON.INI file

1. In the WINNT directory, open the SNMPMON.INI file into any text editor, such as Notepad*.
2. Make any needed changes to the file.
3. Save and close the file.

Generating AMS² alerts when an SNMP trap is received

The SNMP Trap Receiver enables you to easily integrate SNMP trap-generating devices into Server Manager's Alert Management System² (AMS²). You can configure a particular alert action to occur when the Trap Receiver receives a trap. For example, you could configure the Trap Receiver to send you a pager notification when it receives a trap indicating that an APC UPS battery needs to be replaced.

This automation frees you to concentrate on more important matters, while still allowing complete control over your entire network.

For more information, see chapter 4, "Configuring Alert Actions."

Configuring servers to send SNMP traps

When a server sends a notification to the Server Manager console, it also has the ability to send an SNMP trap to specified destinations. This is beneficial if you want Server Manager notifications from every server on a large enterprise network to be sent to a single SNMP management console (which may or may not reside on the immediate network).

Configuring a server to send an SNMP trap requires several steps. In general, you'll need to:

- Install and configure SNMP, which includes specifying a destination for the SNMP traps. This destination can be either an IP address or a server name.
- Start SNMP and the SNMP trap service.

Installing and configuring SNMP on your NetWare servers depends heavily on your individual server and network configuration. See your NetWare documentation for more information.

To install and configure SNMP on Windows NT servers

1. From the Windows NT server's Control Panel, double-click Network.
2. Click the Services tab.
3. Click Add.
4. Double-click SNMP Service.
5. Specify a location for the Windows NT install files and click Continue.
6. At the Microsoft SNMP Properties dialog, click the Traps tab.
7. In the Community Name box, type a name for the SNMP community, such as Public.
8. Click Add.
9. Below the Trap Destinations box, click Add.
10. Type the computer name or IP address of your network's SNMP management console (where you want the traps sent).
11. Click Add.
12. Click OK.
13. Click Close.
14. When prompted, click Yes to restart your computer.

To start the SNMP services under Windows NT

1. From the Windows NT server's Control Panel, double-click Services.
2. If it's not already started, click SNMP and click Start.
3. If it's not already started, click SNMP Trap Service and click Start.
4. Click Close.

Managing APC UPS devices

Server Manager supports APC UPS devices (with PowerNet SNMP adapters installed) connected to monitored servers. If you installed the APC PowerXtend* snap-in software during installation (using the Have Disk button), you can open APC PowerXtend from the Server Manager console.

PowerXtend works in conjunction with Desktop Management Interface (DMI) to:

- Monitor UPS status and power quality.
- Configure UPS parameters.
- Control UPS and server operations.
- Test UPS operations.

To run the APC PowerXtend software

1. In the Intel Management Directory tree, double-click the server that's connected to the APC UPS device you want to control.
2. Double-click Tools.
3. Click APC Power.
4. Click the Tasks tab.
5. Click Launch Applet.
6. Click Apply to open APC PowerXtend.

APC PowerXtend opens as a separate application independent from Server Manager. You can't manage or close it from the Server Manager console. APC PowerXtend provides its own online documentation. Adobe Acrobat* versions of the APC documentation are stored on the Server Manager CD-ROM in the plug_ins/APC directory.

G Glossary

Alert Management System^2 (AMS^2)

A notification system that alerts the network administrator or other servers when server parameter thresholds are reached or exceeded. Alerts can be sent in several ways; some examples are a page sent to the network administrator, a broadcast message over the network, or Internet mail.

Arbiter

The Arbiter is software that acts a “traffic officer” directing traffic and giving access to the COM ports on the Server Manager console.

authentication

The process of providing a valid username and password to gain access through the Server Manager console to information and services on servers installed with the Server Manager agents.

Health

A collection of user-specified parameters that provide the overall status of the server.

HOBBSRV.HDW

A legacy file found only with the IRMC 1 that enables you to configure the remote management card parameters.

HOBLOCAL.TXT

A legacy file found only with the IRMC 1 that contains localization-configurable parameters for the remote management card.

Intel remote management card (IRMC)

Server Manager’s hardware card that’s installed directly on servers with Server Manager agents. There are two versions of the card, the IRMC 1 is an ISA-based card; the IRMC 2 is a PCI-based card.

ping

Ping is a basic TCP/IP program that lets you verify that a particular IP address exists and can accept requests. “Pinging” is the act of using the ping utility or command to ensure that a computer (or group of computers) is properly connected to the network or Internet.

remote control

Controlling or operating one computer from another computer’s console. Using the Server Manager console, you can view the remote server’s screen display and operate the server as if you were seated in front of it.

Server Manager console

The user interface that the network administrator uses to monitor the status of servers. The console is connected to servers either through the network or through a modem connection. From the console, the network administrator can manage any server that has the Server Manager agents installed.

severity

The degree of seriousness assigned to an event. The user assigns one of three possible severities to all alert conditions. The three severities used in Server Manager (from lowest to highest severity) are: Informational, Warning, and Critical.

TAP

Telocator Alphanumeric input Protocol. TAP is an industry standard protocol for sending page requests from automated equipment, computers, and other data-entry devices to radio paging systems.

TAPI

Telephony Application Programming Interface. An API for connecting a Windows computer to telephone services. TAPI is the result of joint development by Microsoft and Intel. The standard supports connections by individual computers as well as LAN connections serving many computers. Within each connection type, TAPI defines standards for simple call control and for manipulating call content.

UPS

Uninterruptible Power Supply. A power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data in RAM and shut down the computer gracefully.

watchdog

A hardware timer used to automatically reboot a server after a system crash. This timer can be set to any value from 2 to 255 minutes. When enabled, this register continuously decrements until it reaches zero. If the count reaches zero, the hardware reboots the computer. In order to stop the count from reaching zero, the LANDesk software contains a heartbeat function that periodically resets the timer value to its initial value.

I Index