Dell OpenManage™ IT Assistant

Version 8.0

User's Guide

www.dell.com | support.dell.com

Notes and Notices

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

June 2006

Contents

Introducing Dell OpenManage™ IT Assistant

Dell OpenManage IT Assistant provides a central point of access to monitor and manage systems on a local area network (LAN) or wide area network (WAN). By allowing an administrator a comprehensive view across the enterprise, IT Assistant can increase system uptime, automate repetitive tasks, and prevent interruption in critical business operations.

Simplifying System Administration

Using IT Assistant, you can:

- Identify the groups of systems that you want to manage remotely.
- Consolidate your view of all systems, giving you a central launch point for managing them.
- Create alert filters and actions that will automatically notify you when system uptime is affected.
- Create customized enterprise-wide reports that provide a detailed inventory of each system.
- Create customized tasks that allow you to coordinate configuration management across the entire enterprise, including software update, device control (shutdown/wake up), and command line execution.
- Measure the performance of systems on your network.

Identifying the Groups of Systems for Remote Management

IT Assistant performs discovery and status polling, allowing system administrators to identify systems and devices on a network by host name, IP address, or IP subnet range. During a status poll, IT Assistant queries the health, or *status*, of a system and its components. Information that is gathered during discovery and status polling is displayed in the management console and written to the IT Assistant database. The default database packaged with IT Assistant is the Microsoft® SQL Server 2005 Express. Users who require a more powerful database can use Microsoft SQL 2005 Server or SQL Server 2000.

Consolidating a View of All Your Systems

IT Assistant allows system administrators to take actions on managed systems from the management console. Using IT Assistant, you can create tasks that apply to a single system or each system in a group, create dynamic groups of systems to facilitate management, and conduct inventory on any system. In addition, IT Assistant provides a consolidated launch point for the following Dell systems management applications and devices: Dell OpenManage Server Administrator, Dell OpenManage Array Manager, Remote Access Console, Dell OpenManage Switch Administrator, Digital keyboard/video/mouse (KVM), printers, tapes, storage devices, and Intelligent Platform Management Interface (IPMI) devices.

Creating Alert Filters and Actions

You can use IT Assistant to create alert *filters* to isolate alerts that are of greatest interest to a system administrator. System administrators can then create corresponding alert *actions* that are triggered when the criteria used to define the alert filter are met. For example, IT Assistant can alert a system administrator when a server fan is in warning or critical state. By creating a filter with a corresponding e-mail action, the administrator is e-mailed if a fan reaches the defined status. The administrator can then act on the notification by using IT Assistant to shut down the system, if necessary, or launch Server Administrator to troubleshoot the problem.

Creating Customized Discovery and Inventory Reports

Using IT Assistant's report wizard, you can create customized reports for any device or group across the enterprise. These reports can contain device inventory information based on a broad selection of attributes. For example, you can create a report that lists details for each add-on card in all systems in a group, including bus speed and width, manufacturer, and slot length and/or number. IT Assistant also provides a collection of pre-formatted reports that gather common information from the enterprise.

Creating Tasks That Enable Configuration Management From a Central Console

IT Assistant also enables you to drive common configuration management tasks across the entire enterprise from a single console. By setting up simple tasks using IT Assistant's wizard-based user interface (UI), you can perform device control tasks (shut down/wake up), software updates, deploy agents, or run command line tasks on any systems in your managed group. IT Assistant allows you to load Dell Update Packages (DUP) and System Update Sets into a central repository, and run a compliance check against systems in the enterprise. The system administrator can then instruct IT Assistant to perform the updates immediately or according to a defined schedule.

NOTE: To perform a software update, the appropriate agent software must be installed on the target device. For more information on agents, see "Agents on the Systems That You Want to Monitor."

Measuring the Performance of Systems on Your Network

IT Assistant helps you to monitor the performance of a device or a group of devices with supported operating systems over a specified period of time. Performance is monitored with the help of a set of performance counters that you can configure to send alerts when the thresholds are crossed.

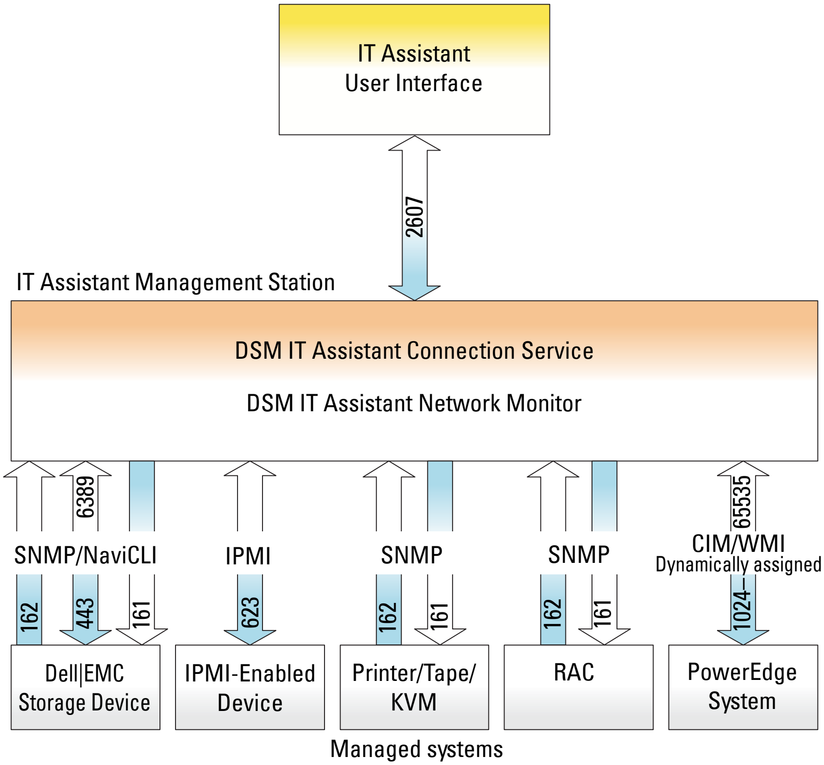
Understanding IT Assistant's Components

To understand the other sections of this document, you must understand the following components of IT Assistant:

- IT Assistant user interface (UI)
- IT Assistant Services Tier (Network Monitoring Service, Connection Service, and database)
- Managed system

The IT Assistant UI provides a graphical user view of the information gathered by the IT Assistant Services Tier. This information depicts the overall health and configuration details of each system in the managed group. Systems in the managed group that are being monitored by IT Assistant are referred to as *managed systems*; the system running the IT Assistant UI is generally called the *network management station*.

Figure 1-1. IT Assistant User Interface, Services System, and Managed System



NOTE: The numbers in Figure 1-1 are the port numbers used by IT Assistant to communicate with the managed systems.

NOTE: For more information on the ports used by IT Assistant, see the *Dell OpenManage Installation and Security User's Guide*.

User Interface

From the IT Assistant UI, you can perform a wide variety of configuration and management tasks, such as specifying systems to discover, creating alert filters and actions, and power-cycling systems.

The IT Assistant UI is based on Sun Microsystems' Java technology. Remote access is through either a Web browser (Internet Explorer, Mozilla, or Firefox) or a terminal service session.

IT Assistant Services

The IT Assistant Services Tier is installed as part of the standard installation. Technically, the Services Tier consists of the Network Monitoring Service, the Connection Service, and the database. In highly customized installations, some users may install their database on a separate system. If you are configuring the simple network management protocol (SNMP) agent on a managed system, trap destinations for the SNMP service must point to the host name or IP address of the system where IT Assistant is installed.

Terminology: Managed System and IT Assistant System

For the purposes of IT Assistant, a *managed system* is a system that has supported instrumentation or agents installed that allow the system to be discovered and polled for status. IT Assistant simplifies system administration of many managed systems by allowing an administrator to monitor them from one management console. For more information on agents, see "Agents on the Systems That You Want to Monitor."

In this guide, the terms *IT Assistant system* or *network management station* are used to identify the system on which the IT Assistant software is installed.

Integrated Features

Native Install

The Dell OpenManage systems management software products are installed using the install process native to the operating system.

User Interface Design and Online Help

IT Assistant user interface (UI) includes wizard-based dialogs for performing many standard tasks. IT Assistant version 8.0 menu bar contains new menu options for the new features. Take some time to familiarize yourself with the new layout.

Comprehensive online help is available, both from the **Help** link at the top right of the IT Assistant window and from context-specific **Help** buttons within individual dialogs and wizards.

The UI is exclusively Web based, uses Sun Microsystems' Java technology, and also supports Linux systems.

DMI Support

IT Assistant no longer supports the Desktop Management Interface (DMI) protocol. As a result, systems running DMI using Dell OpenManage Server Agent 4.5.1 (and earlier) and Dell OpenManage Client Instrumentation 6.0 (and earlier) will not be discovered by IT Assistant.

Topology View

In the UI, you can select **Views→Topology** to see a graphical presentation of the devices in your network. When you double-click the icon for the group you want to view, you move down through the hierarchy. In addition, you can display detailed device information by moving the cursor over each icon. You can also perform tasks on the devices in this view, such as application launch, refresh inventory and status, and troubleshooting.

Dynamic Groups

You can create dynamic groups of devices to help you manage and monitor them more effectively. For more information, see the Group Configuration topic in the *Dell OpenManage IT Assistant Online Help*.

NOTE: You can re-use the device selection queries created in one module of IT Assistant in other modules as well. For example, a query created from the search-devices module will also be available when you are creating or editing a report, an alert filter, or a task.

Application Launch

IT Assistant provides a consolidated launch point for the following Dell systems management applications: Server Administrator, Array Manager, Remote Access Console, Dell OpenManage Switch Administrator, Digital keyboard/video/mouse (KVM), printers, tapes, storage devices, and Intelligent Platform Management Interface (IPMI) devices. For more information, see the Application Launch topic in the *IT Assistant Online Help*.

NOTE: Network Address Translation (NAT) is not a supported configuration on IT Assistant. Therefore, application launch does not work in conjunction with NAT, even though IT Assistant successfully discovers the managed systems. You should use IT Assistant to connect only to the IP address with which a system was discovered. Other IP addresses available on the system may not be accessible to IT Assistant. In many implementations, such as a server farm or load balancer implementation, the system will be behind a NAT. In such environments, IT Assistant will fail to connect to Server Administrator running on those systems.

Reporting

IT Assistant offers a customizable reporting feature that gathers data from the SQL Server database. Report results are based on the data gathered in the last discovery and/or inventory cycle.

The report interface wizard is designed to allow you to select actual fields in the IT Assistant database. You can create a report containing information such as:

- Details of the hardware devices being managed by IT Assistant, including systems, switches, and storage devices
- BIOS, firmware, and driver versions
- Field Replaceable Units (FRU) data
- Other asset or Cost Of Ownership details

You can also specify the output format, such as HTML, XML, or comma-separated values (CSV). CSV is normally used in a spreadsheet tool, such as Microsoft Excel®. IT Assistant saves the report definitions for later use and retrieval.

To use the IT Assistant report wizard, select **Views→Reports**. A full description of the capabilities and steps for using the report wizard is available in the *IT Assistant Online Help*.

Software Updates

IT Assistant allows you to load Dell Update Packages and System Update Sets into a central repository, then compare the packages to the versions of the software currently running on your enterprise systems. You can then decide whether to update systems that are not in compliance, either immediately or according to a schedule you define.

You can also customize the view of the package information by operating system, system type, component name, and software type.

To use the software update feature, select **Manage→Software Updates**. For more information, see the Software Update topic in the *IT Assistant Online Help*.

Manage Tasks

IT Assistant provides an updated task management functionality that allows you to set up and remotely run certain tasks on all systems in your enterprise, including device control (shutdown and wake up), software update, software deployment, and command line execution.

To use the task management functionality, select **Manage→Tasks**. For more information, see the Task topic in the *IT Assistant Online Help*.

Troubleshooting Tool

A graphical troubleshooting tool is available at **Tools→Troubleshooting Tool** to diagnose and resolve discovery and configuration problems, including SNMP and Common Information Model (CIM) related issues. You can also use the tool to test device and e-mail connectivity.

For more information, see the *IT Assistant Online Help*.

User Authentication

For previous users of IT Assistant, IT Assistant now uses operating system or domain-based authentication; the IT Assistant 6.*x* read/write password is no longer used. For information on the Microsoft Active Directory® schema and how to configure it for use with IT Assistant, including how to install the required snap-in, see the *Dell OpenManage Installation and Security User's Guide*.

Enhanced Inventory Cycle

IT Assistant collects inventory information, such as software and firmware versions, as well as device-related information about memory, processor, power supply, PCI cards and embedded devices, and storage. For details about the inventory information that IT Assistant collects and stores in its database, see "Add Report — Using the IT Assistant Reporting System" in the online help. For configuring inventory settings, see "Inventory Poll Settings — Configuring IT Assistant to Perform Inventory" in the online help.

Single Sign-On

Single Sign-On on Windows systems is supported. Use Single Sign-On to bypass the login page and directly access IT Assistant by clicking the **IT Assistant** icon on your desktop. The desktop icon queries the registry to see if the **Automatic Logon with current username and password** option is enabled in Internet Explorer. If this option is enabled, then Single Sign-On is executed; otherwise, the normal login page will be displayed. For more information on how to set these options, see "Single Sign-On."

User Preferences

User Preferences are independent of user privileges. You can use this feature to customize your view of the device groups. You can access this feature from **Tools→User Preferences**. For more information on how to use this feature, see "User Preferences — Customizing the IT Assistant User Interface" in the online help.

For information about the new features in IT Assistant version 8.0, see "What's New for Dell OpenManage™ IT Assistant Version 8.0?"

Other Information You May Need

This *User's Guide* is intended to present a high-level view of IT Assistant. Not all features and capabilities are shown in this document. However, each feature is fully explained in the online help available from the IT Assistant UI.

Additionally, the following resources are available on either the Dell Support website at **support.dell.com** or the documentation CD:

- The *Dell OpenManage Server Administrator User's Guide* documents the features, installation, and services that make up Dell's primary suite of one-to-one server management tools.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* documents the Server Administrator SNMP management information base (MIB). The MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.
- The *Dell OpenManage Server Administrator CIM Reference Guide* documents the Server Administrator CIM provider, an extension of the standard management object format (MOF) file. The CIM provider MOF documents supported classes of management objects.
- The *Dell OpenManage Installation and Security User's Guide* documents how to install the Dell OpenManage systems management software on your system, as well as how to configure Active Directory and extend the schema for IT Assistant.

You can access the *IT Assistant Online Help* in two places: either by clicking the **Help** link at the top right of the browser window, or by clicking the **Help** button within the dialog or wizard you are using.

2

Getting Started With Dell OpenManage™ IT Assistant

You can use Dell OpenManage IT Assistant to monitor and manage systems on a local area network (LAN) or a wide area network (WAN), as well as identify the groups of systems that you want to manage remotely and consolidate your view of all systems, giving you a central launch point for managing these systems.

To be able to use IT Assistant, you will need to:

- "Plan your IT Assistant installation"—It is important to plan because depending on your network management objectives, you may want to use IT Assistant:
  - as a discovery or status polling tool
  - to monitor performance of the various devices on your network and perform software updates
  - to only receive alerts about problems on your managed systems.
- "Install IT Assistant"—IT Assistant can be obtained from:
  - The *Dell Systems Management Consoles* CD. See the *Dell OpenManage Installation and Security User's Guide* for more information on the systems management software components.
  - The Dell Support website at **support.dell.com**.

    To download IT Assistant, perform the following steps:

    1 Connect to the Dell Support website at **support.dell.com**.

    In the search bar at the top right-hand corner, select **Technical Support** and type **OMI-50-MgmtStat-WIN_A00.exe** as the search text.

    NOTE: In the search text, **50** indicates the version of Dell OpenManage that packages the management station components including IT Assistant.

    2 Click **Search**.

    3 Click the hyperlink that appears in the search results page. The **Drivers and Downloads** page appears.

    4 Select **OMI-50-MgmtStat-WIN_A00.exe**. The download page for **OMI-50-MgmtStat-WIN_A00.exe** appears.

    5 Click **Download Now** and save the file to a location on the management station.

Management station is the system where IT Assistant is installed. A management station can be used to remotely manage one or more managed systems from a central location. The systems which are monitored by IT Assistant are referred to as managed system.

Ensure that you have the Windows SNMP Service installed before installing IT Assistant.

NOTE: All other prerequisites, except the Windows SNMP Service, can be installed using the IT Assistant installer.

NOTE: Ensure that you have the operating system installation CD to install the SNMP components on the management station. IT Assistant installation will fail if you do not have the SNMP components.

To install SNMP Service on the management station, perform the following steps:

1. Click the **Start** button. Point to **Settings→Control Panel→Add or Remove Programs→Add/Remove Windows Components**.
2. Select **Management and Monitoring Tools**.
3. When prompted for location to install, select the operating system CD that contains the SNMP service components.

To configure the Windows SNMP Service on the management station, perform the following steps:

1. Right-click the **My Computer** icon on the desktop and select **Manage**. The **Computer Management** window appears.
2. Expand the **Services and Applications** tree.
3. Click **Services**. The services list is displayed in the right pane.
4. Locate and double-click **SNMP Service**. The **SNMP Service** properties window is displayed.
5. Select the **Security** tab and click **Add** under **Accepted community names**. The **SNMP Service Configuration** window appears.
6. Select **READ ONLY** in the **Community rights** drop-down menu and type a case-sensitive string in the **Community name** field.

   NOTE: The **Community name** string acts as a password for SNMP communications.
7. Click **Add**.
8. Select **Accept SNMP packets from these hosts**, and click **Add** again.
9. In the **SNMP Service Configuration** dialog box type `localhost` or the IP address of the management station in **Host name, IP or IPX address**.
10. Click **Add**.
11. Click the **Traps** tab. Enter a case-sensitive string in the **Community name** field and click **Add to list**.

    NOTE: You may enter the same string that you entered in step 6.
12. Click **Add** under the **Trap destinations** field and type `localhost` or the IP address of the management station in **Host name, IP or IPX address** and click **Add**.

13 Click **OK**.

14 Right-click **SNMP Service** and select **Restart**.

15 Select **SNMP Trap Service** and ensure that the status is displayed as **Started** and the Startup Type is **Automatic**.

To configure Windows SNMP Service on the managed system, perform the following steps:

1 Click the **Start** button. Point to **Settings→Control Panel→Add or Remove Programs→Add/Remove Windows Components**.

2 Select **Management and Monitoring Tools**.

3 When prompted for location to install, select the operating system CD that contains the SNMP service components.

To configure the Windows SNMP Service on the management station, perform the following steps:

1 Right-click the **My Computer** icon on the desktop and select **Manage**. The **Computer Management** window appears.

2 Expand the **Services and Applications** tree.

3 Click **Services**. The services list is displayed in the right pane.

4 Locate and double-click **SNMP Service**. The **SNMP Service** properties window is displayed.

5 Select the **Security** tab and click **Add** under **Accepted community names**. The **SNMP Service Configuration** window appears.

6 Select **READ ONLY** in the **Community rights** drop-down menu and type a case-sensitive string in the **Community name** field.

NOTE: The **Community name** string acts as a password for SNMP communications.

7 Click **Add**.

8 Select **Accept SNMP packets from these hosts**, and click **Add** again.

9 In the **SNMP Service Configuration** dialog box type `localhost` or the IP address of the management station in **Host name, IP or IPX address**.

10 Click **Add**.

11 Click the **Traps** tab. Enter a case-sensitive string in the **Community name** field and click **Add to list**.

NOTE: You may enter the same string that you entered in step 6.

12 Click **Add** under the **Trap destinations** field and type `localhost` or the IP address of the management station in **Host name, IP or IPX address** and click **Add**.

13 Click **OK**.

14 Right-click **SNMP Service** and select **Restart**.

If you downloaded IT Assistant from the Dell Support website at **support.dell.com**, perform the following steps:

1 Double-click **OMI-50-MgmtStat-WIN_A00.exe**. This is a Winzip self-extractor package.

2 Specify a temporary folder to save the unzipped files.

3 Locate the temporary folder and double-click **setup.exe**.

The installer first runs the Prerequisites Checker to check if all prerequisites are installed. If a prerequisite is not already installed, you can install it by clicking the appropriate hyperlink in the installer window and then following the instructions in the setup screens.

When all the prerequisites are installed, install IT Assistant by clicking **Install, Modify, Repair or Remove Management Station** and follow the setup screens.

After IT Assistant is installed, to run IT Assistant, do one of the following:

- Double-click the IT Assistant icon on your desktop.
- Open a supported Web browser and connect to the IT Assistant management station by typing:

  ```
  <IT Assistant hostname>:<port number>
  ```

  in the Address bar.

  NOTE: The default IT Assistant port number is 2607.

If you access the IT Assistant UI from a system running supported Windows operating system that does not have a minimum supported Java Runtime Environment (JRE) version of 5.0 update 6, then IT Assistant would automatically start installation of JRE on that system.

NOTE: If the system that accesses the IT Assistant user interface has JRE version 5.0 update 1 to update 5, then IT Assistant does not automatically update the JRE to version 5.0 update 6. In this case, update the JRE version manually by pointing the browser to **https://<host name>:<port number>/jre-1_5_0_06-windows-i586-p.exe.**

However, if you are accessing IT Assistant from a system running supported Linux operating system, perform the following steps:

1 Save the JRE installer (**jre-1_5_0_06-linux-i586-rpm.bin**) in the location of your choice.

2 Extract the RPM and install JRE.

3 Create a soft link to this JRE in the **plugins** folder of the browser.

4 Close the Web browser and run IT Assistant again.

- "Set up protocols"—You must configure the appropriate protocols (SNMP, CIM, and IPMI) to discover the systems in your network and to receive alerts that report the status of their components. For more information, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."
- "Configure IT Assistant to monitor your systems"—IT Assistant can perform a variety of tasks for each system in your network. To be able to perform these tasks, configure IT Assistant to:
  - Discover systems, printers, switches, and storage devices. For more information, see "Configuring Discovery Settings."
  - Collect inventory information about memory, processor, power supply, embedded devices, and software and firmware versions. For more information, see "Configuring Inventory Settings."
  - Define status polling settings to perform a power and connectivity health check for all discovered devices. This determines whether a device is operating normally, is in a non-normal state, or is powered down. For more information, see "Configuring Status Polling Settings."
  - Define a discovery range. A discovery range is a network segment (subnet, range of IP addresses on a subnet, individual IP addresses, or an individual host name) that IT Assistant uses to discover devices. For more information, see "Configuring Discovery Ranges."
- Perform various tasks, such as:
  - Creating an Alert Action
  - Creating a Performance Monitoring Task
  - Creating a Software Deployment Task
  - Creating a New Report

3

What’s New for Dell OpenManage™ IT Assistant Version 8.0?

The following features are new in this release of IT Assistant:

Performance Monitoring

Performance Monitoring helps you monitor the performance of a group of supported Microsoft® Windows® or Linux systems in your network environment over a specified period of time. Performance is monitored with the help of performance counters available for each component. You can select and monitor the performance counters. You can also configure threshold alerts to flag and notify you of under- or over-utilized systems on your network. For more information, see "Performance Monitoring."

Simple Network Management Protocol (SNMP) Event Source Import Utility

You can import multiple event sources, that are not natively supported in IT Assistant, into the IT Assistant database. For more information, see "Simple Network Management Protocol Event Source Import Utility."

IPMI Discovery Support

IT Assistant discovers systems equipped with baseboard management controllers (BMC) that support Intelligent Platform Management Interface (IPMI) versions 1.5 or later. IT Assistant communicates with the BMC directly or through the Windows IPMI Provider on a Microsoft Windows Server® 2003 R2 system.

IT Assistant discovers and classifies the BMC of the discovered system through IPMI. However, if the Dell agent is installed on this system, IT Assistant will correlate the information with the discovered system through the service tag.

Software Deployment

You can use this feature to deploy Dell OpenManage Server Administrator on Dell systems that do not have Server Administrator installed. Server Administrator assists in discovering, classifying, inventorying, monitoring systems, and updating software on your network.

Using this feature, you can also update Server Administrator to a newer version.

Digital Signature Verification

IT Assistant checks the authenticity and integrity of the update packages and MSI files using digital signature verification.

Digital signature verification of each Dell™ Update Package (DUP) will happen when you manually import the packages from the *Dell Server Update Utility* CD or a repository on a network share.

IT Assistant also supports signature verification for the Server Administrator MSI package.

Custom Bundles

With IT Assistant, you can create a custom System Update Set or bundle.

You can create custom bundles that contain only the packages you want. For example, you can create a custom bundle out of an existing Dell custom bundle that will enable you to update just the device drivers on a given set of target devices.

This custom bundle can be subsequently used to drive system compliance reports and do custom updates.

Favorite Application Launch

IT Assistant supports launching user-configured applications for multiple devices or a group of devices, such as printers and switches. For more information, see the *IT Assistant Online Help*.

Storage Integration

IT Assistant discovers Dell|EMC arrays in your storage environment and displays them in the **Dell/EMC Arrays** category present in the **Storage Devices** group.

For more information, see the *IT Assistant Online Help*.

Printer Integration

IT Assistant version 8.0 supports discovery of Dell network-enabled printers and classifies them under the **Printers** category in the **Device** tree.

IT Assistant uses SNMP to communicate with the printer devices. Dell printers have implemented a standard Printer MIB, enabling standardized access to important information.

NOTE: You can also use this feature of IT Assistant to discover non-Dell printers in your network environment.

For more information, see the *IT Assistant Online Help*.

Tape Integration

IT Assistant version 8.0 supports discovery of those Dell tape library devices that have an out-of-band management port. IT Assistant classifies them under the **Tape Devices** category under the **Storage Devices** tree. For more information, see the *IT Assistant Online Help*.

FRU Support

With IT Assistant version 8.0, you can view the field replaceable units (FRU) information for a managed system. IT Assistant retrieves FRU information from Dell OpenManage Server Administrator during an inventory cycle and stores it in the database.

For more information, see the *IT Assistant Online Help*.

Power Control Tasks

Starting with IT Assistant 8.0, before trying SNMP power control tasks, IT Assistant will try the **omremote** command on the managed system. This applies only if the managed system has Dell OpenManage version 4.3 or later installed.

NOTE: For Dell OpenManage versions earlier than 4.3, the Power Control tasks remain unchanged.

NOTE: The **omremote** command uses the operating system credentials for authentication.

IT Assistant version 8.0 supports performing remote power control operations and alert processing for Alert Standard Format (ASF) 2.0 compliant devices.

NOTE: See the system documentation for enabling remote power control through ASF.

NOTE: IT Assistant uses the in-band Broadcom Windows Management Instrumentation (WMI) provider to verify if a device has ASF capabilities.

4

Planning Your Dell OpenManage™ IT Assistant Installation

It is important to plan before installing Dell OpenManage IT Assistant. Depending on your company's network management objectives, you may want to use IT Assistant primarily as a discovery and status polling tool that quickly scans the network to retrieve managed system information. On the other hand, you may want IT Assistant to also receive and forward alerts to support personnel about problems on specific managed systems. Or maybe you want a combination of both.

Decisions That You Make Before Installation

After you have determined your network size and network management objectives, you must then make configuration decisions specific to your network management goals. If your network is well established and you already have a well-defined IT Assistant management plan, many of these decision-points may have already been addressed. Pre-installation planning includes choosing the following:

- Event filtering and notification strategy
- Database that will be used to store IT Assistant data
- Hardware configuration
- Operating system
- Systems management protocol(s)
- Agents for your managed systems

NOTE: This document assumes that your systems are connected through a TCP/IP network and makes no assumption regarding your network's complexity or whether you are already using any systems management applications. In addition, no assumption is made regarding the type of systems and devices that exist on your network. See "Installing, Uninstalling, and Upgrading Dell OpenManage™ IT Assistant" for all installation, uninstallation, and upgrade procedures.

Primary Planning Questions

System types and network management objectives differ among enterprises. Answering the following questions can better prepare you for an IT Assistant installation that will support your company's goals for network management. After reading this section, see Table 4-4 before performing your installation.

1. What are the basic hardware and operating system requirements for installing IT Assistant? Does my enterprise meet them?
2. Is there any reason to select a particular operating system among those that are supported when installing IT Assistant?
3. Is there any reason to select a particular hardware configuration when installing IT Assistant?
4. Do I want to use the default installed database (Microsoft® SQL Server 2005 Express) or should I install the Microsoft SQL Server database?
   - How many systems do I want to discover or manage?
   - How dense do I expect the event traffic to be on my network?
5. Which systems management protocol(s) should I plan to install or enable?
   - What type of systems do I want to manage?
   - What agents and instrumentation are currently installed on my managed systems?
   - What agents do I want to eventually run on my managed systems?
   - Which protocols do these agents require or support?
6. How should I organize my managed systems' IP addresses if I am using more than one systems management protocol on a subnet?

Selecting the Operating System

You can install IT Assistant on any system that is running one of the operating systems in Table 4-1.

Table 4-1. Minimum Supported Operating System Requirements for IT Assistant

Small (up to 500 Managed Systems)	Large (500+ Managed Systems)
Microsoft Windows® XP Professional with SP2	Windows Server 2003 with SP1
Windows 2000 with SP4	Windows 2000 with SP4
Windows Server® 2003 with SP1	

NOTE: IT Assistant is not supported on Microsoft Windows Small Business Server 2003.

NOTE: See your Microsoft operating system documentation when installing and configuring Terminal Services or Remote Desktop.

NOTE: IT Assistant cannot be installed on Dell systems running Red Hat® Enterprise Linux or SUSE® Linux Enterprise Server operating systems. These systems can, however, launch IT Assistant through supported browsers (Mozilla version 1.7.3 and later, and Firefox version 1.0.1 or later).

NOTE: If you use the performance monitoring feature, see Table 7-3 for hardware and operating system requirements.

Selecting a Hardware Configuration

The hardware configuration you choose must meet or exceed the recommended configuration for IT Assistant. Depending on your specific IT Assistant deployment and your network environment, it may be advisable to exceed the recommended configurations for processor speed, amount of memory, and hard-drive space. For example, you may want to exceed or choose the upper end of the recommended configuration if you:

- Anticipate heavy managed systems alert traffic
- Have complex alert filters with configured alert actions
- Are performing frequent discovery, inventory, status polls, or performance monitoring
- Are running Microsoft SQL Server tuned to maximum performance

The recommended minimum hardware configuration for IT Assistant is shown in Table 4-2.

Table 4-2. Recommended Minimum Hardware Configuration for IT Assistant (by Enterprise Size)

Component	Small (up to 500 Managed Systems)	Large (500+ Managed Systems)
Processor	1 processor (1.8-GHz minimum)	2 to 4 processors (800-MHz minimum)
Memory	512 MB	1–2 GB
Disk Space	at least 1 GB	at least 5 GB

NOTE: The amount of disk space needed may increase if you import numerous Dell Update Packages (DUPs) and MSI files for software update and deployment.

NOTE: If you use the performance monitoring feature, see Table 7-3 for hardware and operating system requirements.

Selecting the SQL Server 2005 Express Default Database or SQL 2005 Server

In general, the number of systems you expect to manage and the number of alerts you expect from your managed systems determine the database to use with IT Assistant. If you will be managing fewer than 500 systems, the SQL Server-compliant default database that ships with IT Assistant, SQL Server 2005 Express, is most likely a suitable data repository. However, if you are going to manage 500 systems or more and/or are receiving several alerts per second, you should use Microsoft SQL Server 2000 or later as your database. You will also need to consider the impact of the performance monitoring feature on your database choice. For more information, see the "Performance Monitoring." In addition, if you are performing frequent discoveries or status polls, you may benefit by the increased performance offered by SQL 2005 Server over SQL Server 2005 Express.

NOTE: You can configure IT Assistant version 6.3 and later to use Microsoft SQL Server running on a remote, dedicated server instead of configuring on the IT Assistant system. For more information, see "Remote Microsoft SQL Server and IT Assistant."

NOTE: IT Assistant version 8.0 is backward-compatible with the SQL Server-compliant default database that ships with IT Assistant 7.*x*.

NOTE: SQL Server 2005 Express and SQL 2005 Server run only on Windows 2000 with SP4, Windows Server 2003 SP1, or Windows XP with SP2.

E-Mail Notification Features

E-mail Alert Actions are useful in environments in which a system administrator does not want to use the IT Assistant user interface (UI) to visually monitor the status of managed systems. By coupling e-mail alert actions with alert action filters, an administrator may identify a person to be electronically notified when a specific system sends alerts to the IT Assistant network management station. This individual can then choose to take the appropriate corrective action for that system. By configuring alert filters with corresponding alert actions, constant monitoring of system status in the IT Assistant user interface becomes unnecessary because e-mail notification is set up to occur whenever the event criteria is met.

Determining Systems Management Protocols

One of the most important decisions you will make in planning your IT Assistant installation is determining the protocols to use with IT Assistant. In general, your choice of protocols is determined by the systems you want to monitor and the respective agent protocols they support. If the systems you want to monitor have agents that use the Simple Network Management Protocol (SNMP), Common Information Model (CIM) or the Intelligent Platform Management Interface (IPMI) protocols, these protocols must also be configured in IT Assistant.

Supported Protocols

IT Assistant supports three systems management protocols: SNMP, CIM, and IPMI. These protocols allow communication between the IT Assistant network management station and the managed systems on your network. For communication between IT Assistant and each managed system to occur successfully, agents (instrumentation) must be installed on each of the systems you want to manage. For systems management, it is strongly recommended that you enable and configure all protocols.

NOTE: If the appropriate protocol is not configured correctly on the managed systems, IT Assistant will fail to classify the systems properly, which may limit the manageability for those systems.

NOTE: The Dell|EMC storage arrays use both SNMP and NaviCLI protocols.

SNMP

In order to successfully perform an IT Assistant installation, you must install and enable the operating system SNMP service.

CIM

CIM is used for managing both client and server systems. It can also be used for monitoring server instrumentation in a network that does not allow SNMP management.

IPMI

Intelligent Platform Management Interface (IPMI) operates independently of the operating system and allows administrators to manage a system remotely even in the absence of the operating system or the systems management software, or even if the monitored system is not powered on. IPMI can also function when the operating system has started, and offers enhanced features when used with the systems management software.

In order to successfully discover systems through IPMI, you must have a baseboard management controller (BMC) running IPMI version 1.5 or later on your systems.

NOTE: The BMC does not monitor the storage subsystem on your network. To monitor these devices, you must install Server Administrator on your managed systems.

Factors That Affect Protocol Choice

Two factors affect protocol choice:

- The systems that you want to monitor
- Agents on the systems that you want to monitor

Systems That You Want to Monitor

Your network may consist of a combination of client and server systems, Dell|EMC storage arrays, printers, and tape libraries. When planning for IT Assistant installation, you will be surveying these systems, as well as any systems you plan to add to your network, and determining which of these you want to monitor. During this assessment, you will be looking not only at the number of client and server systems, but also at any systems management agents and operating systems installed on these systems. The following section discusses the agents and corresponding protocols that you may need to configure in IT Assistant. Correctly configuring these protocols within IT Assistant is required to successfully manage your network.

Agents on the Systems That You Want to Monitor

The agents that you run on your managed systems may support a specific systems management protocol. If you want to retain the agents that are already installed on these systems, you must continue to manage them with their respective protocols. If the protocols used by certain agents are older, you can choose, in most cases, to replace or upgrade these agents with those that support newer protocols. Table 4-3 lists a number of agents and instrumentation that may be installed on Dell clients and servers. As long as the corresponding protocol is enabled in IT Assistant, these systems can be discovered and managed on your network.

Agent is a general term applied to the software components of systems management instrumentation. The following table provides the management and alerting agents supported by IT Assistant. Degrees of support vary among agents. For example, IT Assistant automatically discovers, displays, receives alerts from, and can perform actions on the systems managed by Dell OpenManage Server Administrator, but IT Assistant can only receive alerts from certain storage device agents.

NOTE: IT Assistant no longer supports the Desktop Management Interface (DMI) protocol. As a result, systems running DMI using Dell OpenManage Server Agent 4.5.1 (and earlier) and Dell OpenManage Client Instrumentation 6.0 (and earlier) will not be discovered by IT Assistant.

Table 4-3. Agents Supported by IT Assistant

Device	Version(s) Supported	Auto Discoverable	Alerting
Dell PowerEdge Agents			
Server Administrator	1.5 and later	Yes	Yes
Baseboard Management Controller Firmware	1.0 and later Supports only Dell PowerEdge™ *x8xx* and *x9xx* systems	Yes	Yes
Array Manager	3.7	Yes	Yes
DRAC 5	1.0 and later	Yes	Yes
DRAC 4	1.0 and later	Yes	Yes
DRAC III, DRAC III/XT	1.0 and later	Yes	Yes
ERA, ERA/O	1.0 and later	Yes	Yes
DRAC/MC	Supports only PowerEdge 1855 and 1955 systems	Yes	Yes
ERA/MC	Supports only PowerEdge 1655	Yes	Yes
PowerEdge 1655MC Integrated Switch	N/A	Yes	Yes
Dell PowerVault™ Agents			
PowerVault 701N	N/A	Yes	Yes
PowerVault 705N	N/A	Yes	Yes
PowerVault 735N	N/A	Yes	Yes
PowerVault 750N	N/A	Yes	Yes
PowerVault 755N	N/A	Yes	Yes
PowerVault 715N	N/A	Yes	Yes
PowerVault 725N	N/A	Yes	Yes
PowerVault 770N	N/A	Yes	Yes

Table 4-3. Agents Supported by IT Assistant *(continued)*

Device	Version(s) Supported	Auto Discoverable	Alerting
PowerVault 775N	N/A	Yes	Yes
PowerVault 745	N/A	Yes	Yes
PowerVault Adaptec CIO	4.02	No	Yes
Dell PowerConnect™ Agents and PowerConnect Firmware Versions Supported by IT Assistant			
PowerConnect 3024	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	Yes	Yes
PowerConnect 3048	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	Yes	Yes
PowerConnect 3248	1.0.1.*x*, 2.0.0.*x*, 2.1.0.*x*	Yes	Yes
PowerConnect 3324	1.0.0.*x*, 1.1.0.*x*, 1.2.0.*x*	Yes	Yes
PowerConnect 3348	1.0.0.*x*, 1.1.0.*x*, 1.2.0.*x*	Yes	Yes
PowerConnect 3424	1.0.0.*x*	Yes	Yes
PowerConnect 3424P	1.0.0.*x*	Yes	Yes
PowerConnect 3448	1.0.0.*x*	Yes	Yes
PowerConnect 5012	5.2.5.*x*, 6.0.4.*x*, 6.1.2.*x*	Yes	Yes
PowerConnect 5212	1.0.0.*x*, 3.1.0.*x*	Yes	Yes
PowerConnect 5224	1.0.1.*x*, 2.0.0.*x*, 2.1.0.*x*, 3.1.0.*x*	Yes	Yes
PowerConnect 5316M	1.0.0.*x*	Yes	Yes
PowerConnect 5324	1.0.0.*x*	Yes	Yes
PowerConnect 6024	1.0.2.*x*, 2.0.0.*x*	Yes	Yes
PowerConnect 6024F	1.0.2.*x*, 2.0.0.*x*	Yes	Yes
Cisco Switch (only in Modular Chassis)	N/A	Yes	Yes
Digital KVM Agents			
2161 DS	N/A	Yes	Yes
4161 DS	N/A	Yes	Yes

Table 4-3. Agents Supported by IT Assistant *(continued)*

Device	Version(s) Supported	Auto Discoverable	Alerting
Network Adapter Agents			
Intel® PRO	N/A	No	Yes
Broadcom	N/A	No	Yes
ASF	1	No	Yes
Client Agents			
Dell OpenManage Client Instrumentation	7.0 and later	Yes	Yes
Dell|EMC			
CX300	N/A	Yes	Yes
CX500	N/A	Yes	Yes
CX700	N/A	Yes	Yes
AX100	N/A	Yes	Yes
AX100i	N/A	Yes	Yes
CX3-20	N/A	Yes	Yes
CX3-40	N/A	Yes	Yes
CX3-80	N/A	Yes	Yes
AX150	N/A	Yes	Yes
Printer			
5210n	N/A	Yes	Yes
5310n	N/A	Yes	Yes
3110cn	N/A	Yes	Yes
3115cn	N/A	Yes	Yes
1700n	N/A	Yes	Yes
W5300cn	N/A	Yes	Yes
M5200cn	N/A	Yes	Yes
5310	N/A	Yes	Yes
5210	N/A	Yes	Yes
1710	N/A	Yes	Yes
5100cn	N/A	Yes	Yes
5100cn w HD	N/A	Yes	Yes
5100cn w MPC	N/A	Yes	Yes

Table 4-3. Agents Supported by IT Assistant *(continued)*

Device	Version(s) Supported	Auto Discoverable	Alerting
5100cn w HD & MPC	N/A	Yes	Yes
3100cn	N/A	Yes	Yes
3000cn	N/A	Yes	Yes
1710n	N/A	Yes	Yes
1600n	N/A	Yes	Yes
Tape Automation			
PowerVault 132T	N/A	Yes	Yes
PowerVault 136T	N/A	Yes	Yes
ML6000	N/A	Yes	Yes
NOTE: You can configure SNMP only through the panel on the device. **NOTE:** The default community string is publicCmtyStr.			

Summary of Pre-Installation Decisions

This section lists the major factors you must consider before installing and using IT Assistant to manage systems on your network. Table 4-4 summarizes questions raised in the previous sections, the option(s) and action(s) available, and the section of this guide where you can find the corresponding procedure for performing that action.

Table 4-4. Pre-Installation Questions, Options, and Actions

Question	Option/Action	Option/Action	Next Step
Is there any reason to select a particular operating system among those that are supported when installing IT Assistant?	Ensure that the operating system is supported for the components you are installing.	For a large network, install IT Assistant on a server operating system.	See the latest IT Assistant **readme.txt** either on the Dell Support website at **support.dell.com** or on the *Dell Systems Management Consoles* CD.
Is there any reason to select a particular hardware configuration when installing IT Assistant?	Ensure that your hardware configuration meets or exceeds the recommended requirements for the components that will be installed on the system.		

Table 4-4. Pre-Installation Questions, Options, and Actions *(continued)*

Question	Option/Action	Option/Action	Next Step
Should I use the default installed database (SQL Server 2005 Express) or should I install the Microsoft SQL 2005 Server database?	Generally, SQL Server 2005 Express is adequate if you are managing fewer than 500 systems. However, heavy event traffic or the usage of the performance monitoring subsystem may lead you to select SQL 2005 Server.	Selection of the SQL database and heavy event traffic are examples of choices that require higher processor speed and/or extra processors, more memory, and greater hard-drive space to ensure IT Assistant performance.	
Which systems management protocol(s) should I plan to install or enable?	Survey the agents that you want to run on your managed systems and find out which protocols they support; consider the type of system you are managing.		See "Installing, Uninstalling, and Upgrading Dell OpenManage™ IT Assistant" and "Configuring Dell OpenManage™ IT Assistant to Monitor Your Systems."
How should I organize my managed systems' IP addresses if I am using more than one systems management protocol on a subnet?	Where possible, group systems using the same systems management protocol into contiguous subnets. This strategy increases manageability during the creation of IT Assistant discovery ranges.		
Will I use role-based access to assign user levels in IT Assistant?	IT Assistant supports standard role-based access levels. The three levels supported are User, Power User, and Administrator.	Using these access roles in your enterprise can provide an added level of security.	See "Ensuring a Secure Dell OpenManage™ IT Assistant Installation"

5

Installing, Uninstalling, and Upgrading Dell OpenManage™ IT Assistant

Installation Requirements

When installing Dell OpenManage IT Assistant, it is important to see the latest **readme.txt** file on your *Dell Systems Management Consoles* CD or on the Dell Support website at **support.dell.com**. This file defines the most current supported operating systems and hardware requirements for IT Assistant. In addition to meeting these requirements, there are additional IT Assistant installation requirements as well as requirements for the systems that will be managed by IT Assistant. See "Planning Your Dell OpenManage™ IT Assistant Installation" for more information.

NOTE: The *Systems Management Consoles* CD is available for download as a Web Pack and an ISO image.

TCP/IP Protocol Support

For IT Assistant to function properly, your network must support the TCP/IP protocol.

Setting Up or Enabling Protocols for Agent Communication

Before installing IT Assistant, you must install your operating system's Simple Network Management Protocol (SNMP) service. Additionally, to ensure that systems are visible to IT Assistant discovery and inventory functions, make sure that agents and instrumentation on managed systems are accessible through the Common Information Model (CIM), Simple Network Management Protocol (SNMP), or Intelligent Platform Management Interface (IPMI) protocol.

NOTE: CIM is installed by default on Microsoft® Windows® 2000, Windows Server® 2003, and Windows XP Professional.

Installing SNMP on the IT Assistant System

The SNMP service must be installed and running on the IT Assistant system. SNMP (or CIM) must also be installed on the systems that you want to discover and manage.

NOTE: The following example uses Windows 2000 Advanced Server.

1. Click the **Start** button, point to **Settings**, and double-click **Control Panel**.
2. Double-click the **Add or Remove Programs** icon.

   This launches the **Add or Remove Programs** window.

3. Click the **Add/Remove Windows Components** icon on the left menu bar.

   This launches the **Windows Components Wizard** window.

4. In the **Windows Component Wizard** window under **Components**, scroll to **Management and Monitoring Tools**.
5. Select **Management and Monitoring Tools**, click **Details**, select **Simple Network Management Protocol**, and click **OK**.
6. Click **Next** in the **Windows Components Wizard** window.

   The **Windows Components Wizard** will install SNMP.

7. Once the installation is complete, click **Finish**.
8. Close the **Add or Remove Programs** window.

   SNMP is now installed on your system.

IT Assistant can be installed only on systems running Windows 2000, Windows XP Professional, or Windows Server 2003. For information on how to install and configure SNMP on managed systems running Microsoft Windows, Red Hat® Linux, or SUSE® Linux Enterprise Server operating systems, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Enabling CIM

The CIM/WMI (Windows Management Instrumentation) service is installed by default on Windows 2000, Windows Server 2003, and Windows XP Professional. CIM discovery requires proper user ID and password credentials. Failure to supply proper credentials on a subnet configured for CIM discovery can result in account lockout.

For examples on how to set up CIM, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Setting Up RBAC User Information

IT Assistant supports role-based access control (RBAC) to define the specific operations each user can perform. However, the IT Assistant installation process does not require these user roles to be set up prior to installation. To set up RBAC users either before or after installing IT Assistant, see "Ensuring a Secure Dell OpenManage™ IT Assistant Installation."

Installing IT Assistant

If you are installing IT Assistant for the first time, follow the steps shown here. If you are upgrading from a previous version, see "Upgrading from a Previous Version of IT Assistant."

You can install IT Assistant from the *Dell Systems Management Consoles* CD or download and install IT Assistant from the Dell Support website at **support.dell.com**. The Dell OpenManage Management Station installer program is used to install IT Assistant as well as other Dell OpenManage software. To install a product other than IT Assistant, refer to the installation instructions specific to that product.

To install IT Assistant for the first time:

1. Insert the *Dell Systems Management Consoles* CD into your CD drive.

   If the installation program does not start automatically, navigate to the **/windows** directory and click **setup.exe**. The **Dell OpenManage Management Station** screen is displayed.

   The installer automatically scans your system for any dependencies, such as whether you have SNMP installed or have a supported database application. If a missing dependency is found, an information window is displayed and you may be prompted to install the required package.

2. If no missing dependencies are found, click **Install, Modify, Repair or Remove Management Station**.

   The Dell OpenManage Management Station install wizard is displayed. Click **Next**.

3. If you agree with the Dell Inc. software license agreement, click **Next**.
4. Select **Typical** or **Custom** installation from the **Setup Type** window.

   Choosing **Custom** allows you to select specific Dell OpenManage applications to install and change the installation directory path and port settings for IT Assistant.

   Choosing **Typical** installs all Dell OpenManage applications (including IT Assistant) that have passed dependency checking with pre-selected default settings for location and port. If you choose **Typical**, skip to the last step.

5. Ensure that **IT Assistant** is selected in the list of installable components, then click **Next**.
6. If you selected the **Custom** installation option, enter port settings or accept the defaults. If you selected the **Typical** installation option, this dialog does not appear.
7. Click **Next**.
8. Ensure that **IT Assistant** is included in the installation summary window, then click **Install** to begin the installation.

Upgrading from a Previous Version of IT Assistant

NOTE: Only IT Assistant versions 6.2 and later support upgrades from previous versions. The Dell OpenManage Management Station installer program detects whether you currently have an upgradable version of IT Assistant on your system.

NOTE: IT Assistant does not support a direct upgrade from version 6.*x* to version 8.0. You will be required to first upgrade IT Assistant version 6.*x* to version 7.0 and then to IT Assistant version 8.0.

NOTE: While upgrading to IT Assistant version 8.0 if you also plan to upgrade the Microsoft SQL server, see "Selecting the SQL Server 2005 Express Default Database or SQL 2005 Server" for the appropriate combination of the operating system and SQL Server.

To upgrade IT Assistant:

1 Insert the *Dell Systems Management Consoles* CD into your CD drive.

If the installation program does not start automatically, navigate to the /**windows** directory and click **setup.exe**. The **Dell OpenManage Management Station** screen is displayed.

2 The installer automatically scans your system for any missing dependencies, such as whether you have SNMP installed or have a supported database application. If a missing dependency is found, an information window is displayed and you may be prompted to install the required packages.

NOTICE: IT Assistant 8.0 installer removes all previous Management Station applications and re-installs the applications you select. All Dell OpenManage Server Administrator applications are also removed.

NOTE: If you have IT Assistant version 6.*x*, install IT Assistant 7.0 before installing version 8.0.

3 If no missing dependencies are found, click **Install, Modify, Repair or Remove Management Station**.

The Dell OpenManage Management Station install wizard is displayed. Click **Next**.

4 If you agree with the Dell Inc. software license agreement, click **Next**.

5 Select **Typical** or **Custom** installation from the **Setup Type** window.

Choosing **Custom** allows you to select specific Dell OpenManage applications to install and change the installation directory path and port settings for IT Assistant.

Choosing **Typical** installs all Dell OpenManage applications (including IT Assistant) with pre-selected default settings for location and port.

6 Ensure that **IT Assistant** is selected in the list of installable components, then click **Next**.

7 If you selected the **Custom** installation option, enter port settings or accept the defaults. If you selected the **Typical** installation option, this dialog does not appear.

8 If you are upgrading from IT Assistant 6.*x* to 7.0, by default, **Migrate IT Assistant Database Settings** is selected. When this option is selected, the following database settings in your existing IT Assistant installation are preserved in your new installation:

- Global configuration
- Event stored action
- Discovery configuration

NOTE: **Migrate IT Assistant Database Settings** is not available if you are upgrading from IT Assistant version 7.*x* to version 8.0.

9 Click **Next**.

10 Ensure that **IT Assistant** is included in the installation summary window and click **Install** to begin the installation.

NOTE: When upgrading from IT Assistant version 6.*x* to version 7.2, you have to qualify the CIM user names. This qualification is necessary because CIM is enabled/disabled only per discovery range and requires each CIM user to be qualified with a domain, or local host if no trusted domain is configured. It is critical to provide this qualification when configuring CIM through a discovery range (for example: <*domain**username*>, or <*localhost**username*>) to authenticate and use the CIM protocol.

NOTE: You cannot upgrade IT Assistant in a remote database environment. See the "Remote Microsoft SQL Server and IT Assistant" section for details.

Uninstalling IT Assistant

To uninstall IT Assistant:

1 Click the **Start** button, point to **Settings**, and double-click **Control Panel**.

2 Double-click **Add or Remove Programs**.

3 Select **Dell OpenManage Management Station** from the list of currently installed programs and click the **Change** button.

NOTE: To uninstall the entire Management Station suite of products (including IT Assistant), select **Remove** in the previous step. If you select **Remove**, the uninstallation may appear to be unresponsive for several minutes if IT Assistant is performing discovery or polling.

The Management Station install wizard appears. Click **Next**.

4 In the **Program Maintenance** window, select **Modify** and click **Next**.

5 In the **Custom Setup** screen, deselect IT Assistant and click **Next**.

6 In the summary screen, ensure that IT Assistant is included in the list of applications to be removed. Click **Install**.

7 When the uninstallation is complete, click **Finish**.

8 Reboot your system (optional).

Remote Microsoft SQL Server and IT Assistant

This section describes how to configure IT Assistant version 8.0 and later to use Microsoft SQL Server 2005 running on a remote server as the IT Assistant database.

Configuring IT Assistant to Use a Remote Database

IT Assistant ships with the SQL Server-compliant default database—SQL Server 2005 Express. The IT Assistant Network Monitoring Service and the IT Assistant Connection Service access the SQL Server-compliant default database—SQL Server 2005 Express that ships with IT Assistant.

When the database resides outside the IT Assistant management station, as in the case of a remote database, it is necessary to make the IT Assistant Network Monitoring Service and the IT Assistant Connection Service on the management station to access the remote database.

To do this, ensure that:

- The SQL Server service (MSSQLServer) is running through the service control panel on the management station as well as the remote database. You can start the SQL Server 2005 services either through the SQL Server Service Manager on the system tray or through the SQL Server Enterprise Manager's SQL Server group.
- The SQL Server-compliant database versions on management station and the remote database are the same.
- SQL Server 2005 uses the same authentication that is used on the SQL Server 2005 Express on the management station.
- The management station and the remote database use the same authentication with Administrator rights, are logged in with the same account, and that the SQL Server databases on both systems are configured to use this account. This is because IT Assistant services log into SQL Server 2005 Express using the Windows NT® Authentication.

In this example, let us assume that the user name is administrator on both servers with identical passwords and that both systems reside in the same NT domain.

Deploying the IT Assistant Database to the Remote Database

On the management station, stop the IT Assistant Connection Service and the IT Assistant Network Monitoring Service from the Service Control Manager. This stops the IT Assistant services from accessing the local IT Assistant database. Ensure that no other program is accessing the local IT Assistant database. If a database program such as the SQL Server's Enterprise Manager and/or Query Analyzer is running, close the program or ensure that the program is not accessing local IT Assistant database.

On the management station, detach the IT Assistant database from the local SQL Server by running the IT Assistant database management utility on the command line.

Run the following command from the IT Assistant **bin** directory:

```
dcdbmng /r
```

When the IT Assistant database has been successfully detached, the **Detach database** dialog box is displayed.

To ensure that the database is detached, perform the following steps:

1 Start the ODBC Data Source Administrator by clicking the **Start** button. Select **Settings→Control Panel→Administrative Tools→Data Sources (ODBC)**.

2 Select the **System DSN** tab.

   Ensure that there no system data source with the name **ITAssist** (local IT Assistant database).

   If such a system data source exists, click **Remove** to delete this data source.

On the management station, navigate to the **Data** folder under the SQL Server installation directory. By default, the installation path is **C:\Program Files\Microsoft SQL Server\MSSQL**. Copy the IT Assistant database file, **ITAssist_Data.mdf** to a location on the remote database system. For this example, let us consider the desired path to be **DB_PATH**.

On the remote database system, attach the database file, **ITAssist_Data.mdf** located in **DB_PATH** to the local SQL Server. You can do this by executing the following SQL statement against the local master database:

```
exec sp_attach_single_file_db @dbname='ITAssist',@physname=
'DB_PATH\ITAssist_Data.mdf'
```

NOTE: The first argument **@dbname** specifies the name of the database and should always be **ITAssist**. The second argument **@physname** specifies where the database file is located and you should always use the correct location of file, **ITAssist_Data.mdf**.

If there are several instances of the SQL Server on the remote database system, then you can execute the above SQL statement and attach **ITAssist** to any one instance of your SQL Server. However, it is recommended that **ITAssist** be attached to the default instance of the local master database. This can be viewed in the SQL Server group of the SQL Enterprise Manager. All non-default instances of the SQL Server will have the instance name attached to it. For this example, consider **MYINST1** and **MYINST2** as the two non-default instances of the SQL Server. These SQL Server instances will be: **REMOTE_DB_SERVER\MYINST1** and **REMOTE_DB_SERVER\MYINST2**. This can also be viewed in the SQL Server group of the SQL Enterprise Manager. If the remote database system's SQL Enterprise Manager does not have a complete list of all the SQL Server instances on the system, register these non-default instances so that they are displayed in the SQL Server group.

Connecting IT Assistant to the Remote Database

1 On the management station, navigate to the IT Assistant installation directory and edit the configuration file, **dconfig.ini**, by replacing each `(local)` string with the name of the SQL Server that resides on the remote database system. You can find the string under the sections [ITAssist_Odbc_Attributes] and [Master_Odbc_Attributes].

2 If the IT Assistant database resides in the default instance of the SQL Server, IT Assistant database will be <*name of the database server*>. If the IT Assistant database resides in a non-default instance of the SQL Server, for example **MYINST1**, then the IT Assistant database will be <*name of the database server*>/MYINST1. In other words,

   Attribute3=Server, <*name/IP address of the database server*> -- in case of default instance

   Attribute3=Server, <*name of the database server*>/MYINST1 -- in case of named instance

3. On the management station, change the IT Assistant services logon credentials from **Local System account** to the common account used to log into the local SQL Server on both management station and the remote database system. Let us assume that in this case, it is the local Administrator account.

4. You should change the logon credentials for the IT Assistant Connection Service and IT Assistant Network Monitoring Service. To do this, right-click the individual services from the **Service Control Manager** and select **Properties**. Select the **Log On** tab to change the logon credentials.

   If you are configuring these services to run under a different user account, the user account used for **Logon** must have the following user privileges:

   - Act as part of the operating system (this privilege is required on the Windows 2000 system)
   - Replace a process level token
   - Log on as a service

   To set these privileges, perform the following steps:

   - Run `secpol.msc` in the Command Prompt dialog box.
   - Select **Security Settings→Local Policies→User Rights Assignments.**
   - Right-click the policy and select **Properties** (or **Security**, in case of Windows 2000).
   - Add the user name to this policy.
   - Restart the system to apply the settings.

5. This step is optional and is required only if you plan to stop the SQL Server service from running on the management station.

   During IT Assistant installation, IT Assistant services are created to depend on the SNMP service and the SQL Server's MSSQLServer service. You can remove the dependency of the IT Assistant services on SQL Server's MSSQLServer service by editing the registry for the IT Assistant services on the management station.

   NOTICE: Before editing the registry, ensure that you save a copy of the registry and understand how to restore it if a problem occurs.

   On the management station, open the Microsoft Windows Registry Editor by typing `regedit` on the command prompt. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dcnetmon**

   Double-click the **DependOnService** value name to edit its properties. This registry value is a UNICODE multiple string and its initial Value Data is `SNMP MSSQLServer`.

   Delete **MSSQLServer** and save the changes. This removes the dependency of the IT Assistant Network Monitoring Service on the SQL Server service.

   Next, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dcconnsvc** Double-click the **DependOnService** value name to edit its properties. This registry value is a UNICODE multiple string and its initial Value Data is `SNMP, MSSQLServer, dcnetmon`

Delete **MSSQLServer** and save the changes. This removes the dependency of the IT Assistant Connection Service on the SQL Server service.

Check the dependencies of the IT Assistant Network Monitoring Service and the IT Assistant Connection Service on management station by right-clicking the individual services from the **Service Control Manager** and select **Properties**. Select the **Dependencies** tab. There should be no dependency on MSSQLServer Service. Restart the management station to let these changes take effect.

6 On the management station, start the IT Assistant Connection Service and IT Assistant Network Monitoring Service. IT Assistant now connects to the IT Assistant database deployed on the SQL Server of the remote database system.

NOTE: If the IT Assistant services dependency on the local SQL Server service has not been removed as described in previous step, the SQL Server service on management station needs to be running for IT Assistant services to be started, even if the SQL Server database is not actually used by IT Assistant.

7 To verify that the management station has successfully connected to the IT Assistant database on the remote database system, start the ODBC Data Source Administrator from the **Control Panel→ Administrative Tools** on the management station. Select the **System DSN** tab. The **ITAssist** system data source is displayed.

8 On the management station, open the IT Assistant user interface. The IT Assistant services on management station are now ready to use the IT Assistant database residing on the remote database system.

Configuring IT Assistant to Upgrade the Remote Database

IT Assistant does not upgrade the database which is configured on a remote system. This section discusses the steps required to upgrade the IT Assistant (version 7.0 and later) database.

Deploying IT Assistant Database to ITA_STATION

1 On the ITA_STATION, stop IT Assistant Connection Service and IT Assistant Network Monitoring Service from the Service Control Manager. This stops IT Assistant services from accessing the remote IT Assistant database. Also, make sure that no other program is accessing the IT Assistant database, **ITAssist**, of REMOTE_DB_SERVER. If a database program such as SQL Server's Enterprise Manager and/or Query Analyzer is running, close the program or ensure that the program is not accessing the IT Assistant database named ITAssist.

2 On the REMOTE_DB_SERVER, detach the IT Assistant database from the local SQL Server by executing the following SQL statement against local master database:

```
exec sp_detach_db @dbname='ITAssist'
```

3 To ensure that the database is detached, go to ITA_STATION system, start ODBC Data Source Administrator from **Start→Settings→Control Panel→Administrative Tools→Data Sources (ODBC)**. Click the **System DSN** tab. Ensure that there is no system data source with the name ITAssist. If there is, remove that data source by clicking on the **Remove** tab.

4 On the REMOTE_DB_SERVER, navigate to the Data folder under MSDE or SQL Server installed location. By default this is **C:\Program Files\Microsoft SQL Server\MSSQL**. Copy the IT Assistant database file, **ITAssist_Data.mdf** to the desired path on the ITA_STATION. For this example, let us consider the desired path to be DB_PATH.

5 On ITA_STATION, attach the database file, **ITAssist_Data.mdf** located in DB_PATH to the local SQL Server. This can be done by executing the following SQL statement against the local master database:

```
exec sp_attach_single_file_db @dbname='ITAssist', @physname=
'DB_PATH\ITAssist_Data.mdf'
```

NOTE: Ensure that there are no ITAssist_Data and ITAssist_Log files on the ITA_STATION system.

First argument @dbname specifies the name of the database and must be kept as **ITAssist**. Second argument @physname specifies where the database file is located. You should customize it to reflect the correct location of **ITAssist_Data.mdf**. Ensure that there is no **ITAssist_log.ldf** file in the same path. If a file of the same name exists, delete it before executing this command.

Connecting IT Assistant to Database on ITA_STATION

1 On the ITA_STATION, navigate to the configuration directory where IT Assistant is installed. Edit the configuration file, **dconfig.ini**, by replacing each REMOTE_DB_SERVER (name of the database) string under the sections [ITAssist_Odbc_Attributes] and [Master_Odbc_Attributes] with **(local)**.

2 On the ITA_STATION, change the IT Assistant services logon credentials from Common account to Local System account. This operation should be done for both the IT Assistant Connection Service and IT Assistant Network Monitoring Service. To perform these actions, right-click each service from the Service Control Manager and select Properties. Now select the **Log On** tab to change the logon credentials. Save the changes and start the IT Assistant services.

3 Launch IT Assistant.

Upgrading IT Assistant

Upgrade IT Assistant using the latest *Dell OpenManage Installation and Server Management* CD. After the upgrade is completed, launch IT Assistant.

Deploy the IT Assistant Database to REMOTE_DB_SERVER

See "Deploying the IT Assistant Database to the Remote Database" to move IT Assistant database to the remote system.

6

Configuring Dell OpenManage™ IT Assistant to Monitor Your Systems

Dell OpenManage IT Assistant can discover, inventory, and perform a variety of change management tasks for each system in your enterprise. Managed systems can include a mixture of client systems (desktops, portable components, and workstations), servers, printers, tape devices, storage devices, systems with remote access cards, Dell™ PowerConnect™ switches, and digital keyboard/video/mouse (KVMs) switches used with rack-dense systems.

IT Assistant in Real-World User Scenarios

This section illustrates how IT Assistant can be used in two different customer scenarios:

- A small-to-medium size business
- A large enterprise environment

Although fictional, both scenarios presented in this section illustrate how administrators in charge of managing network environments might configure IT Assistant. While many configuration concepts are the same for both scenarios, others depend on the type and number of systems being managed. Use the scenario that best suits your situation as a general guide for configuring IT Assistant.

Regardless of the size of your network, it is useful to read through both scenarios to gain a more complete understanding of IT Assistant procedures and concepts.

NOTE: Neither scenario shown in this section is intended to illustrate the full capabilities of IT Assistant. Based on your enterprise, you may choose to use options and features in IT Assistant not shown here. For more information on IT Assistant's full range of capabilities, see the *IT Assistant Online Help*.

Having Multiple Java Runtime Environments On Your System

IT Assistant uses Java Runtime Environment (JRE) version 5.0. However, you may want to use a different version of the JRE, for example, to run a third-party application. You can use an older version of JRE in conjunction with version 5.0.

Switching Between Various Versions of the JRE

NOTE: For more information, see Sun Microsystem's J2SE 5.0 documentation at **http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html**, and navigate to the Java **Applet Runtime Settings** section.

If the system you use to run the IT Assistant console is also used to run applets that use a different version of the JRE, perform the following steps. These steps enable you to switch between two versions of the JRE.

1 Locate the **jpicpl32.exe** of the JRE version you want to use and execute.

For example, if you want to use JRE version 1.4.2, you can locate **jpicpl32.exe** under **C:\Program Files\Java\j2re1.4.2_05\bin**.

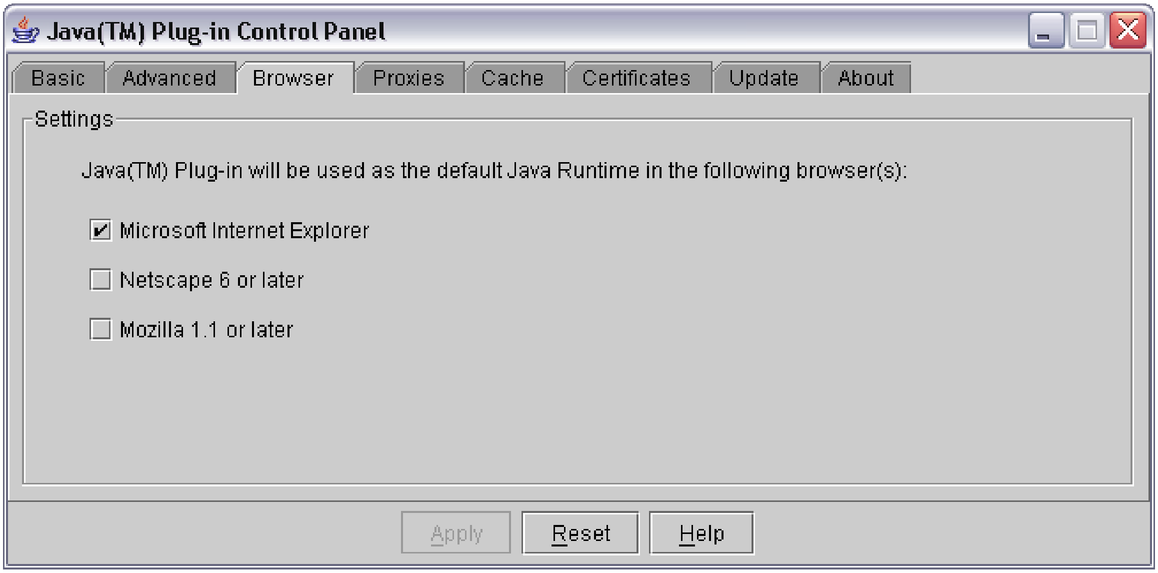
NOTE: This file is available for all JRE versions earlier than version 5.0.

The Java Plug-in Control Panel appears.

2 In the **Browser** tab, deselect Microsoft Internet Explorer, and click **Apply**.

3 Now select Microsoft Internet Explorer, and click **Apply** (see Figure 6-1). This integrates JRE 1.4.2 with Internet Explorer.

Figure 6-1. Java Plug-in Control Panel for JRE 1.4.2



Java(TM) Plug-in Control Panel

Settings

Java(TM) Plug-in will be used as the default Java Runtime in the following browser(s):

☑ Microsoft Internet Explorer

□ Netscape 6 or later

□ Mozilla 1.1 or later

4 Start Internet Explorer.

5 Do one of the following to check the Java Plug-in version number:

   - From the **Tools** menu, select **Sun Java Console**. The Java Plug-in version number will be 1.4.2_05.
   - Go to **www.java.com/en/download/faq/top_issues.jsp**, and locate the **Test your Java Virtual Machine (JVM)** issue. This test checks and displays the Java Plug-in version on your system as 1.4.2_05.

You can now run applets that use this version of the JRE.

If you want to use JRE version 5.0, perform the following steps:

1 In the **Java Control Panel** (for JRE 5.0), under the **Advanced** tab, expand the **<Applet> tag support** component in the **Settings** tree. See Figure 6-2.

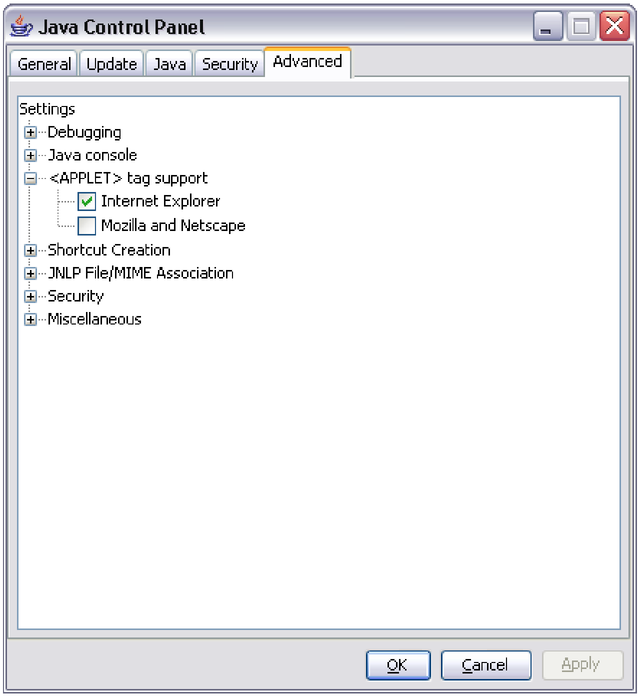
   NOTE: Java Control Panel is found under **Settings→Control Panel→Java**.

   NOTE: On supported Linux systems, run the **ControlPanel** executable in the **bin** folder of the JRE installation on the Linux system.

2 Deselect **Internet Explorer**, and click **Apply**.

3 Now select **Internet Explorer** from the **Java Control Panel**, and click **Apply** (see Figure 6-2). This integrates JRE 1.5.0 with Internet Explorer.

Figure 6-2. Java Control Panel for JRE 5.0



Settings
- Debugging
- Java console
- <APPLET> tag support
  - ☑ Internet Explorer
  - □ Mozilla and Netscape
- Shortcut Creation
- JNLP File/MIME Association
- Security
- Miscellaneous

4 Start Internet Explorer.

5 Do one of the following to check the Java Plug-in version number:

- From the **Tools** menu, select **Sun Java Console**. The Java Plug-in version number will be 1.5.0.
- Go to **www.java.com/en/download/faq/top_issues.jsp**, and locate the **Test your Java Virtual Machine (JVM)** issue. This test checks and displays the Java Plug-in version on your system as 1.5.0.

Ensure That Agents and Instrumentation Are Installed and Running

Dell agents required for managed systems are contained in Dell OpenManage Server Administrator; Dell agents required for client systems (workstations, desktops, and portable components) are contained in Dell OpenManage Client Instrumentation.

These agents gather status information from BIOS or other firmware on the systems they are installed on, then provide that information to IT Assistant. Systems that are monitored by IT Assistant are generally referred to as *managed systems*—the systems that manage them are referred to as *network management stations*, or *IT Assistant systems*.

If either of these agents is not installed, see the *Dell OpenManage Server Administrator* and *Dell OpenManage Client Instrumentation* documentation before continuing with IT Assistant configuration. If the appropriate agent is installed and running correctly, start IT Assistant and read on.

NOTE: Starting with IT Assistant version 8.0, you can discover devices using the IPMI Discovery support feature. See "Configuring IPMI for System Manageability" for more information.

Start IT Assistant

NOTE: IT Assistant supports role-based access control (RBAC) to define the specific operations each user can perform. To set up RBAC users, see "Ensuring a Secure Dell OpenManage™ IT Assistant Installation."

To log on to IT Assistant:

1 Double-click the **IT Assistant** icon on your system’s desktop.

2 The **Log in** dialog box appears. (If Single Sign-On is configured as described in "Ensuring a Secure Dell OpenManage™ IT Assistant Installation," the **Log in** dialog box does not appear.)

3 Enter a user name and password.

4 Select **Active Directory Login** if you have configured user information using the Microsoft® Active Directory® plug-in. The privileges you have in IT Assistant are dependent on the user settings defined.

NOTE: For more information on setting up role-based access, see "Ensuring a Secure Dell OpenManage™ IT Assistant Installation." For information on installing the Active Directory plug-in and extending the Active Directory schema for IT Assistant, see the *Dell OpenManage Installation and Security User's Guide*.

NOTE: To access IT Assistant remotely, you must enter `https://<hostname>:<portnumber>`. The default port number is 2607.

5 Enter your password.

NOTE: As IT Assistant starts up, an authentication certificate pop-up box will appear. You must click **OK** to accept these certificates within 5 minutes or IT Assistant will not load properly and certain critical features will not function.

NOTE: You may see several pop-ups during IT Assistant startup. Pop-ups prompting you to accept an authorization certificate can be avoided by selecting **View Certificate→Install Certificate** (if available) or choosing **Always** in response to the request to accept the certificate.

Configuring SNMP for System Manageability

Before configuring SNMP for system manageability, let us look at the two scenarios we will use to illustrate IT Assistant in this section:

Two systems administrators—let us call them Jane and Tom—are responsible for managing two separate network environments. Jane represents the small-to-medium size business (50 servers, plus over 200 client systems), while Tom represents a much larger enterprise (1,000 servers). Although Jane and Tom both use IT Assistant to discover and manage their systems, the way they configure and use IT Assistant will differ significantly. However, before highlighting the differences, let us look at some basic steps both must perform.

Both Jane and Tom must configure the Simple Network Management Protocol (SNMP) systems management protocol to discover their systems and to receive traps (asynchronous, alert notifications) that report the status of their components. On managed systems, the Server Administrator agent generates SNMP traps in response to changes in the status of sensors and other monitored parameters on a managed system. In order to correctly send these traps, the operating system's SNMP service must be configured with one or more trap destinations that correspond to the system where IT Assistant is installed.

Details on Configuring the SNMP Service

For detailed information about SNMP configuration for the IT Assistant system and for all supported managed system operating systems, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Configuring SNMP on Systems You Want to Manage

In addition to having the SNMP service installed and running on the IT Assistant system, each managed system's operating system must have the SNMP service or daemon configured.

SNMP Best Practices

When configuring SNMP, adhere to the following requirements:

- Use a host name or a static IP address for the IT Assistant system.
- On all managed systems, configure the static IP address or host name as the SNMP trap destination. If you use a host name as the SNMP trap destination (the IT Assistant system name), you must correctly configure name resolution on your network.
- Ensure that **Get** and **Set** community names for SNMP are different.
- When assigning community names to managed systems, keep the total number of different community names low. The fewer community names, the easier it will be to manage your network.

Information on the Managed System Needed for Optimal SNMP Configuration

For every system (running the Windows operating system) to be discovered and managed using SNMP protocol, ensure that SNMP is installed and properly configured.

The two community names that are to be set up are the **Get** (or read) community name and the **Set** (or write) community name. The read community name, which is sometimes labeled *read only*, allows IT Assistant to read information from the managed system, while the write community name, sometimes labeled *read write*, allows IT Assistant to read and write information to the managed system.

NOTE: Community names are case sensitive.

NOTE: Although you can set up just one community name as both read and read/write, it is advisable to create a separate name for each to allow restricted access to the write action.

The community names that you assign for SNMP for managed systems in the operating system must also be recorded in IT Assistant when you set up SNMP discovery ranges.

In the **Discovery Range** dialog box under the protocols section, make sure that the **Get** (or read) and **Set** (or write) community names of all of the managed systems are entered. If there is more than one community name per field, separate each community name with a comma.

For more information, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Configuring CIM for Manageability

Depending on your network environment, configuring CIM may be a required task. CIM is the preferred systems management protocol for newer client instrumentation and is required for Dell systems instrumented with OMCI version 7.*x*. CIM is also used for performing remote Windows software updates.

In her small-to-medium size network, Jane must install, enable, and configure CIM to be able to manage client systems running the latest Client Instrumentation (OMCI 7.*x*). Although Tom's group of managed systems are made up entirely of servers, he will also install and enable CIM. Generally, CIM should be enabled if your enterprise includes any managed system running a Microsoft Windows® operating system.

Configuring CIM in the Operating System

IT Assistant uses the Windows Management Interface (WMI) core to make CIM connections. The WMI core uses Microsoft network security to protect CIM instrumentation from unauthorized access.

For more information on operating system CIM configuration, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

NOTE: IT Assistant requires the CIM user name and password with administrator rights that you established on the managed systems. If you are using a domain user, be sure to specify the correct domain in the user name field. A user name must always be qualified with a domain, or **localhost** if a domain is not present. The format is either *<domain>**<user>* or *<localhost>**<user>*.

NOTE: CIM discovery requires proper user ID and password credentials. Failure to supply proper credentials on a subnet configured for CIM discovery can result in account lockout.

Best Practices for Setting Up Discovery Targets

Regardless of the size of your network, the following table shows Dell's recommendations for the best way to set up discovery targets. IT Assistant users define discovery target systems and ranges on a network to identify the systems that they want to locate and record in their database. When you set up a discovery target and range in IT Assistant, you are given the option of selecting a host name, an IP address, or a subnet range to identify the systems that you want IT Assistant to discover. This section shows which discovery type is best for the network environment you have.

Table 6-1. Best Practice Recommendations for Setting Up Discovery

Preferred Discovery Range Type	DHCP	Primarily Static IP Addresses
Host name	Recommended	Recommended if DNS is present and IP addresses are spread among many different network segments
IP address	Not recommended	Recommended if IP addresses are spread among many different network segments
IP range	Recommended if located on one or a few network segments	Recommended if located on one or a few network segments

Configuring IPMI for System Manageability

To be able to use the Intelligent Interface Management Protocol (IPMI) discovery feature, ensure that you have:

- Dell PowerEdge™ *x8xx* system and above. This feature will not work for other systems.
- All systems equipped with a baseboard management controller (BMC).
- BMC with IPMI version 1.5 and later.
- Configured the BMC of every managed system.

NOTE: For more information on configuring the BMC, see the "Configuring Your Managed System" section in the *Dell OpenManage Baseboard Management Controller Utilities User's Guide* on the Dell Support website at **support.dell.com** or on the documentation CD.

Using the Microsoft IPMI Provider

Microsoft Windows Server® 2003 R2 is equipped with an IPMI driver and an IPMI Common Information Model (CIM) Provider. The CIM Provider exposes system information that is exposed by the BMC through the IPMI interface. IT Assistant uses this feature to extract information. You can use IT Assistant to discover and classify the BMC through IPMI.

However, ensure that you have the following to be able to use the Microsoft IPMI Provider to send information about your systems:

- Windows Server 2003 R2 operating system on the managed systems
- All managed systems have BMC with IPMI version 1.5 or later
- CIM is configured on the managed systems

  For more information, see step 6 of "Configuring Discovery Configuration Settings."
- IPMI drivers are loaded
- Hardware Management MSI

For more information, see the *Dell OpenManage IT Assistant Online Help*.

Best Practices for Using the IPMI Discovery Feature

IPMI discovery provides you with information about a system even if the system is powered down. IPMI uses the Remote Management Control Packets (RMCP) protocol to communicate with the BMC of the managed systems.

NOTE: RMCP is a UDP-based protocol, which communicates over port 623. The IPMI messages are encapsulated in the RMCP packets. RMCP protocol enables remote server control in all states where the system is powered on.

- Configure the BMC on managed systems that will be discovered using the IPMI Discovery support feature.
- Connect the BMC network interface card (NIC) to the network.

  If your systems have a Dell Remote Access Controller (DRAC) 5, then the RAC should be connected to the network.

  NOTE: For *x8xx* systems, you should enable the DRAC 4 and the BMC if you want to use the functionality of both. However, for *x9xx* systems, DRAC 5 takes over the full functionality of the BMC. Therefore, you need to enable only the DRAC 5.
- In the discovery ranges, provide the SNMP/CIM IP address and credentials (user name and password) for the device as well as the BMC IP address and credentials.

Connectivity using IPMI is inherently slow due to the RMCP protocol. It is, therefore, recommended that you create a separate discovery range for devices that do not have a Dell agent installed on them. For this discovery range alone you can enable the IPMI discovery feature.

NOTE: Systems discovered only through the IPMI protocol are identified on the IT Assistant UI through the BMC IP address. For this reason, tasks such as software deployment and performance monitoring cannot be run on such systems.

Configuring IT Assistant to Discover Storage Devices

Starting with IT Assistant version 8.0, you can discover and monitor Dell|EMC storage devices.

You can display the status of the discovered Dell|EMC storage arrays in the **Dell/EMC Arrays** category under **Storage Devices** group. The status of Dell|EMC storage arrays will be red for failed/critical and green for normal. The Dell|EMC storage arrays recognize all SNMP traps from the device including logging, filtering, and actions information.

NOTE: Use IT Assistant's Event Management System to associate actions, such as e-mailing an administrator or creating a trouble ticket in a help-desk system through an Application Launch, with the critical event sources associated with the arrays. For more information, see the *Dell OpenManage IT Assistant Online Help*.

Prerequisites

You should have the following software configured to enable the Storage Integration feature:

- EMC® Navisphere® Secure CLI on the same system that is running IT Assistant
- SNMP enabled on your Dell|EMC array
- FLARE® operating environment version 19 or later on your Dell|EMC array

Navisphere Secure CLI

IT Assistant uses Navisphere Secure CLI for getting inventory information from the storage devices. The IT Assistant installer detects if the Navisphere Secure CLI is not installed on the management station and gives you the option of installing it.

NOTE: EMC releases new versions of Navisphere Secure CLI periodically, and you may need to update the version of the CLI on the IT Assistant management station.

NOTE: As new versions of IT Assistant are released, the Navisphere Secure CLI version will be updated.

If your storage environment has storage arrays, you can navigate to the element manager to manage the Dell|EMC device.

See the *Dell OpenManage IT Assistant Online Help* for connecting to the remote array for troubleshooting Navisphere agent issues.

See the EMC Navisphere online help for details on monitoring SNMP alerts.

Setup and Configuration

- IT Assistant supports discovery on Dell|EMC storage arrays (for example, AX100 or AX150) arrays that have been upgraded to Navisphere Manager.

  NOTE: IT Assistant does not manage arrays running Navisphere Express.

  NOTE: If you are discovering an AX100i storage array, see the IT Assistant readme for the latest information.

- IT Assistant uses SNMP for discovering the Dell|EMC arrays. Use the Navisphere Manager to enable SNMP on your Dell|EMC array, before it can be discovered in IT Assistant. Set SNMP in Navisphere under the Network settings of the Storage Processor properties.

  NOTE: The storage processors on the Dell|EMC CX3-20, CX3-40, CX3-80 products each have one management port and one service local area network (LAN) port. Do not connect the service ports to the network for general use. Connecting these ports to the network may result in unpredictable status and event reporting within IT Assistant.

- Ensure that the following ports are open on the firewall:
  - TCP 80/443 (Web and SSL)
  - TCP 6389 (Navisphere CLI)
  - UDP 161/162 (SNMP and bi-directional)

  NOTE: These are default ports. If you have changed the port configuration, ensure that the correct ports are open.

  NOTE: For more information on ports used by IT Assistant, see the *Dell OpenManage Installation and Security User's Guide*.

- IT Assistant discovers and displays the information for the storage processor value stored in the discovery range. Since the storage processors are redundant, you only need to enter the IP address of one storage processor for discovery and inventory purposes.

Using the Troubleshooting Tool

The EMC connectivity test can be used to test the communication between the IT Assistant management station and the Navisphere agent on the storage device. The test requires the IP address of the storage processor as well as Navisphere credentials.

NOTE: The Navisphere credentials should have a global scope.

Creating Reports

You can create custom reports for the Dell|EMC arrays. The report wizard of the IT Assistant allows you to select fields from a variety of tables including Device, NIC, Physical disk, Virtual disk, Enclosure, and Controller.

The reports can be created in HTML, XML, and comma-separated value (CSV) format.

NOTE: IT Assistant has pre-defined controller and enclosure reports for the Dell|EMC arrays.

Discovery in Jane's Small-to-Medium Size Business

Jane wants to discover all of the systems on her network. Discovery is a process whereby IT Assistant identifies each system and records identifying information for that system in the IT Assistant database.

As we mentioned previously, Jane is the sole system administrator of a mixed network of systems that includes:

- 50 Dell PowerEdge systems
- 200 Dell OptiPlex™ desktops
- 10 Dell PowerConnect switches

Jane is going to use IT Assistant to monitor global status for her systems, as well as to receive notification when a PowerEdge system or a PowerConnect switch on her network is in the warning or critical state. Jane does not plan to use IT Assistant to notify her when one of her desktop systems generates an alert.

Determining Requirements for a Mixed Server-Client System

Before using IT Assistant to configure discovery, Jane needs to make some basic decisions about her network. Specifically, she must decide the:

- Systems management protocols needed to manage the systems and devices on her network
- Community names and trap destinations for systems to be managed by SNMP
- SNMP requirements for PowerConnect switches
- CIM authentication credentials
- Host names, IP addresses, or IP subnet ranges of systems she wants to monitor

Systems Management Protocols Needed for Jane's Network

In planning to configure discovery, Jane has a mixture of system types (server, client, and switches). The systems management protocols that Jane requires to manage these networked systems and devices are:

- SNMP for her PowerEdge systems and PowerConnect switches
- CIM for her systems running Windows, assuming that Jane has newer, CIM-compatible client instrumentation installed on her client systems

For a review of protocol requirements, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Community Names and Trap Destinations

Jane's requirements for configuring **Get** and **Set** community names and trap destinations for SNMP on her managed systems are not affected by the size of her business. For SNMP configuration requirements associated with servers, see "Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant."

Configuring SNMP for PowerConnect Switches

Jane can monitor her ten PowerConnect switches by using IT Assistant. Each model of PowerConnect switch has documentation that provides the following information on setting up the SNMP service for that switch:

- Community names
- Trap destinations
- The hosts from which the switch will accept SNMP packets

Initial Tasks for Finding Systems on Jane's Network

Now that Jane has reviewed the prerequisite information for her discovery configuration, she is ready to perform first-time discovery configuration. Jane must perform the following tasks:

- Configure communication protocols on the managed systems.
- Configure discovery settings.
- Enter all of the discovery ranges.

Using IT Assistant to Find and Manage Jane's Networked Systems

If this is the first time IT Assistant has been launched since installation, Jane is presented with a welcome screen indicating that IT Assistant has not yet been configured. The four basic steps of configuration are listed:

Step 1—Discovery Configuration – controls how often IT Assistant polls the network for the addition of new systems

Step 2—Inventory Configuration – controls how often IT Assistant retrieves a detailed inventory of all discovered systems

Step 3—Status Polling – controls how often IT Assistant retrieves the health and network connectivity status of discovered systems

Step 4—Ranges – identifies specific ranges for IT Assistant to either limit or expand its discovery, inventory, or polling tasks

Clicking any of the steps will take her to the corresponding dialog box under the **Discovery and Monitoring** menu bar in IT Assistant. Steps 1 through 3 are single-window dialog boxes; step 4 is a wizard-based procedure for defining discovery ranges.

Configuring Discovery Settings

Jane begins by configuring the discovery settings for her systems using the **Discovery Configuration Settings** dialog box. This dialog is displayed either automatically when she clicks *Step 1: Discovery Configuration* from the IT Assistant or by choosing **Discovery Configuration** from the menu bar. Here, Jane enters information that IT Assistant will use for discovery. These values remain unchanged and apply to the corresponding discovery ranges that she will create later in this procedure. However, she can change these values at any time.

To configure discovery settings in IT Assistant, Jane performs the following steps:

1 Jane selects **Discovery and Monitoring→Discovery Configuration** from the IT Assistant menu bar.

The **Discovery Configuration Settings** dialog box appears. **Enable Device Discovery** is selected by default.

2 In the dialog box under **Initiate Device Discovery**, Jane selects the period she wants IT Assistant to perform discovery.

Jane selects all seven days of the week at 6:00:00 AM because the data maybe dynamic, but she wants to select a non-peak period.

NOTE: Dell recommends that you schedule discovery at non-peak times.

3 Under **Discovery Speed**, Jane uses the sliding bar to indicate how much network bandwidth and system resources she wants to allocate to discovery.

NOTE: The faster you set the discovery speed, the more network resources discovery will consume. Faster discovery speeds may impact network performance.

4 Under **Discover**, Jane can choose whether to discover **All Devices** or **Only Instrumented Devices**.

She chooses **Only Instrumented Devices** since she wants IT Assistant to discover only devices that have SNMP or CIM instrumentation. If she wanted to discover any device that responded to a **ping** command, she would have chosen **All Devices**. For a list of supported agents, see "Agents Supported by IT Assistant."

NOTE: Dell recommends that if you have Domain Name System (DNS) configured on your network, select the default, **DNS Name Resolution**.

5 Under **Name Resolution**, Jane selects **DNS Name Resolution** or **Instrumentation Name Resolution**.

DNS name resolution matches the IP address of a system to a host name. Instrumentation name resolution queries the managed system's agent instrumentation for its name. See your device or system documentation for more information on how to configure instrumentation name resolution.

NOTE: Dell recommends that if you have DNS configured on your network, select the default, **DNS Name Resolution.**

6 Jane clicks **OK**.

Configuring Inventory Settings

Next, Jane needs to enter inventory settings. IT Assistant collects inventory information about software and firmware versions, as well as device-related information about memory, processor, power supply, PCI cards and embedded devices, and storage. This information is stored in the IT Assistant database and can be used to generate customized reports.

To set inventory settings, Jane performs the following steps:

1 Jane selects **Discovery and Monitoring→Inventory Configuration** from the menu bar.

The **Inventory Poll Settings** dialog box is displayed. **Enable Inventory** is selected by default.

2 Under **Initiate Inventory**, Jane selects when she wants IT Assistant to perform inventory.

Jane selects all seven days of the week at 6:00:00 AM, a non-peak period for network traffic.

3 Under **Inventory Speed**, Jane uses the sliding bar to indicate how much network bandwidth and system resources she wants to allocate to inventory.

NOTE: The faster you set the inventory speed, the more network resources discovery will consume. Faster inventory speeds may impact network performance.

4 Jane clicks **OK**.

NOTE: IT Assistant version 8.0 can now display the inventory information for printers, tapes, and storage devices. For more information, see the *Dell OpenManage IT Assistant Online Help*.

Configuring Status Polling Settings

Next, Jane defines status polling settings for her systems. IT Assistant performs a power and connectivity health check for discovered devices, determining whether a device is operating normally, is in a non-normal state, or is powered down. Status messages in IT Assistant include *healthy*, *warning*, *critical*, and *powered down*. Status icons also indicate if a system is not instrumented, there is no information for the system, or the state the system was in before it was last powered down.

To set status polling settings, Jane performs the following steps:

1 Jane selects **Discovery and Monitoring→Status Polling Configuration** from the menu bar.

The **Status Polling Configuration Settings** dialog box is displayed. **Enable Status Polling** is selected by default.

2 Under **Status Polling Interval**, Jane selects the interval that she wants IT Assistant to use to perform status polling.

3 Under **Status Polling Speed**, Jane uses the sliding bar to indicate how much network bandwidth and system resources she wants to allocate to status polling.

NOTE: The faster you set the status polling speed, the more network resources discovery will consume. Faster speeds may impact network performance.

4 Jane clicks **OK**.

Configuring Discovery Ranges

IT Assistant maintains a register of network segments that it uses to discover devices. A discovery range can be a subnet, a range of IP addresses on a subnet, an individual IP address, or an individual host name.

To identify her systems to IT Assistant, Jane must define a discovery range.

To define an *include* range, Jane performs the following steps:

1 Jane selects **Discovery and Monitoring→Ranges** from the menu bar.

The **Discovery Ranges** navigation tree is displayed on the left side of the IT Assistant window.

2 Jane expands **Discovery Ranges**, right-clicks **Include Ranges** and selects **New Include Range**.

The **New Discovery Wizard** starts.

NOTE: To *exclude* a specific system or host name from discovery, right-click **Exclude Range** in the **Discovery Ranges** navigation tree and enter the name or IP address of the system. In most small-to-medium businesses like Jane's, this option is not used.

3 In step 1 of the wizard, Jane enters an IP address (or range) or host name.

   She clicks **Add** to add multiple ranges of IP addresses or host names.

   She clicks **Next** to go to the next step.

   NOTE: Acceptable values for the include range are subnet range, host name, or IP address of a single system. Jane refers to the IP subnet ranges she wrote down for her servers, desktop systems, and switches. On Jane's list, Jane may have 192.166.153.* and 192.166.154.*, where the first subnet range is for Jane's servers, the second subnet range is for Jane's desktops, and the switches are spread out on both subnets.

   NOTE: The Import Node List utility offers a convenient way to specify a list of host names, IP addresses, and subnet ranges for IT Assistant to discover. See the *IT Assistant Online Help* for instructions on how to run the utility from the command line. The **importnodelist.exe** file is in the **bin** directory of the IT Assistant base directory.

4 In step 2 of the wizard, Jane uses the default values for Internet Control Message Protocol (ICMP) time-out and retry for the range. She uses the Troubleshooting Tool to determine these values.

   NOTE: IT Assistant offers a troubleshooting tool that can be useful in gathering system information and subnet ranges. Access the tool by selecting **Tools**→**Troubleshooting Tool** from the menu bar. For more information, open the Troubleshooting Tool dialog box and click **Help**.

5 In step 3 of the wizard, Jane configures the SNMP parameters to be used during discovery:

   - Jane ensures the **Enable SNMP Discovery** option is selected.
   - She enters a case-sensitive value for the **Get Community** name.

     Jane's considerations:

     Jane is managing 50 servers, so she wants to configure SNMP. The **Get Community** name is a read-only password that SNMP agents installed on managed systems use for authentication. Jane considers the following as she selects a **Get Community** name:

     Each SNMP-enabled managed system has a **Get Community** name. Jane ensures that she lists each of the community names on all of the systems that she wants to manage. If Jane's managed systems have more than one community name, she enters multiple community names separated by commas in the **Get Community** name field.

     Although the **Get Community** name affects read-only information retrieved by IT Assistant from managed systems, such as the results of discovery, status polling, and alert logs, Jane wants to limit access to this data. Therefore, she changes the default **Get Community** name (**public**) to a name known only to her and her designated backup.

     NOTE: Community names entered in the SNMP Get and Set community name fields for the managed system's operating system must match the Get Community and Set Community names assigned in IT Assistant.

- Jane enters a case-sensitive value for the **Set Community** name.

  Jane's considerations:

  The **Set Community** name is a read-write password that allows access to a managed system. SNMP agents running on the managed system use this password for authentication when actions are attempted on the system, only power cycle tasks use SNMP sets.

  NOTE: Although Dell server instrumentation has an authentication layer above the SNMP Set community name (which requires a host name and password), many SNMP agents do not. Agents without this added security layer may allow any user who knows the SNMP Set community name to gain control of the managed system.

  NOTE: IT Assistant only uses SNMP sets to power cycle systems if the Server Administrator remote command line is not available. If SNMP sets are not required for this purpose, do not enter an SNMP set community name in the discovery wizard.

  Jane chooses a **Set Community** name that matches the SNMP Set community value on the system she is managing. She also makes sure the name she chooses follows the secure password standards in place across her enterprise.

  NOTE: If you want to specify more than one SNMP Get or Set community name in an individual discovery range (for example, one community name for each IP subnet range), separate your community names with commas.

- Jane enters the SNMP time-out and retry values for the discovery range. In Jane's type of network, the default values are usually good choices.

6 In step 4 of the wizard, Jane configures the CIM parameters to be used during discovery.

  Since Jane has a mix of servers and client systems in her managed group running Windows, she will configure CIM.

  - Jane ensures **Enable CIM Discovery** is selected.
  - In **Domain\User Name**, she enters the same name she used to configure CIM on the managed system.
  - She enters the same password she used for the CIM password on the managed system.

  NOTE: You should enable the CIM Discovery option if you want to use the Microsoft hardware agent for IPMI in Microsoft Windows Server 2003 R2.

7 In step 5 of the wizard, Jane does not select **Enable Dell/EMC Array Discovery** because she does not have Dell|EMC storage devices on her network.

8 In step 6 of the wizard, Jane does not configure the IPMI parameters because she does want to monitor her systems through IPMI.

9 In step 7 of the wizard, Jane chooses what action IT Assistant will take upon completion of the wizard.

10 In step 8 of the wizard, Jane reviews her selections and clicks **Finish** to complete the wizard.

  NOTE: You can click **Back** to change your selections.

Changing Discovery, Inventory, and Status Polling Settings After Original Setup

You can return to the **Discovery and Monitoring** menu at any time to edit the settings you entered. The new settings you enter will become effective the next time you perform the corresponding action.

Creating Alert Action Filters and Alert Actions for Jane's Small-to-Medium Size Business

Jane creates an *Alert Action Filter* in IT Assistant by specifying a set of conditions. When tied to an *Alert Action*, IT Assistant will automatically execute whatever action Jane has defined.

IT Assistant has three types of Alert filters:

Alert Action Filters – used to trigger actions when an alert condition is met

Ignore/Exclude Filters – used to ignore SNMP traps and CIM indications when they are received.

Alert View Filters – used to customize the Alert Log view

Jane chooses to use an Alert Action Filter in IT Assistant to filter *warning* and *critical* events for her servers and PowerConnect switches. That way, she will be able to create an Alert Action that will automatically send her an e-mail notification when her server and switch components enter these states. From there, she can take action to prevent a more serious event, such as a system failure. Being the only system administrator of her network, Jane must be selective about which systems she monitors, as well as the Alert Action Filters she creates. She decides to reserve these filters and actions only for her most mission-critical equipment and most severe events.

Creating an Alert Action Filter

1. Select **Alerts→Filters** from the menu bar.

   The **Alert Filters** window appears.

2. Expand the Alert Filters in the navigation tree and right-click **Alert Action Filters**. Select **New Alert Action Filter**.

   The **Add Filter Wizard** appears.

3. Enter a descriptive name for the filter. For example, *Jane's Network Warning and Critical*.
4. Under **Severity**, select the severity of the events for which you want to receive alerts and logs.

   Jane selects **Warning** and **Critical**.

   Click **Next**.

5. Under **Alert Category Configuration**, either select **Select All**, or select the categories of events to include in the alert filter.

   Jane selects **Select All** because she wants to be notified of any warning or critical event that affects her network switches or servers.

   Click **Next**.

6 Under **Device/Group Configuration**, select the devices or groups to associate with the new action alert filter.

Jane selects **Servers and Network Devices**.

Click **Next**.

7 Under **Date/Time Range Configuration**, enter values for any or all of the optional categories.

Jane leaves these options unselected since she wants the filter to apply at all times.

Click **Next**.

8 Under **Alert Action Associations**, select whether you want the event captured by the filter to trigger an alert or be written to a log file.

Jane selects **Alert** to get a console notification.

9 The **New Filter Summary** shows your selections. Click **Finish** to accept, or **Back** to make changes.

10 Verify that the filter name you created in step 3 of the wizard appears in the **Summary of Alert Action Filters** window.

Creating an Alert Action

Now, Jane wants to create an Alert Action that is triggered by the Alert Action Filter she just set up.

To create an Alert Action:

1 Jane selects **Alerts→Actions** from the menu bar.

2 Jane right-clicks **Alert Actions** in the navigation tree and selects **New Alert Action**.

The **Add Alert Action Wizard** appears.

3 Jane gives the action a logical name in the **Name** field.

4 From the **Type** pull-down menu, Jane chooses **Email**.

NOTE: Jane could also choose **Trap Forwarding** or **Application Launch** from the action type pull-down list. **Trap Forwarding** allows large-scale enterprise managers to send SNMP traps to a specific IP address or host. **Application Launch** allows an administrator to specify an executable to run when the alert action filter is met.

NOTE: Any trap forwarded by IT Assistant will not have the **EnterpriseOID**, **Generic TrapId**, and **Specific Trap ID** of the original trap. These values will appear in the description of the forwarded trap.

5 In the **E-mail Configuration** dialog, Jane specifies a valid e-mail address (within your enterprise's SMTP server group) to receive the automatic notification.

NOTE: Jane can test the e-mail configuration she specified by using the **Test Action** button. A success/failure message will be issued. A success should be interpreted as IT Assistant sending the message, not that the recipient received it. For more information on using the **Test Action** button, see the Troubleshooting topic in the *IT Assistant Online Help*.

NOTE: To send e-mail through IT Assistant, the enterprise's SMTP server must be correctly configured. To configure the SMTP server, go to **Preferences→Web Server** on the top navigation bar, and configure the **SMTP Server Name (or IP Address)** and **DNS Suffix for SMTP Server**.

6 In **Alert Filter Associations**, Jane identifies the Action Alert filter that will trigger this e-mail.

She selects *Jane's Network Warning and Critical*—the name she gave the Alert Action Filter she set up earlier.

7 A summary dialog shows Jane's selections.

Jane verifies that the name of the Alert Action she assigned in step 3 appears in the **Summary of Alert Actions** window.

Jane clicks **Finish** to accept the changes.

As a result of how Jane has configured Alert Action Filters and Alert Actions in IT Assistant, here is what will happen:

- IT Assistant will continuously monitor all servers and network switches on Jane's network.
- When any server or network switch reaches a warning or critical state, the Alert Action Filter that Jane set up in IT Assistant will automatically trigger the accompanying Alert Action.
- The Alert Action will send Jane an e-mail notification to the address she specified.
- Jane then decides what action to take on the affected system, such as power cycling the system, shutting it down, or running a remote command using other IT Assistant capabilities.

Many more features are available in IT Assistant than those illustrated here. Click the **Help** button in the appropriate IT Assistant dialog box to see detailed online help about that feature.

Now, let us look at how a much larger enterprise might use IT Assistant to accomplish basically the same tasks as Jane did for a small enterprise.

Discovery in Tom's Enterprise-Size Business

In a larger enterprise, Tom is the systems administrator for a network of 1,000 servers. Tom also supervises four technicians who assist him by taking corrective action on servers when notified that a critical or warning event has occurred. Tom's four technicians have the following areas of responsibility:

- One administrator responsible for all remote systems
- One technician for the first shift (12 hours)
- One technician for the second shift (12 hours)
- One technician for weekends who works 24-hour shifts but who responds only to critical and warning events when notified

Configuring the Discovery Settings

Since Tom is monitoring a network of servers and no clients, his primary choice for a systems management protocol is SNMP. However, since he also manages systems running Windows, he will also enable CIM (like Jane).

To configure the discovery settings for his servers, he will need to perform the following tasks:

- Determine subnet ranges, IP addresses, and/or host names for the servers that he wants to monitor.
- Determine the subnet ranges, host names, or IP addresses that he does not want to monitor.
- Determine SNMP read-only (Get) and read-write (Set) community names that he will use for his network.
- Install and configure the SNMP agents and the operating system SNMP service on each system he wants to monitor.
- Determine appropriate discovery time-out values for the network.

IP Subnet Ranges for Servers

Tom's first decision is to determine which of the 1,000 servers he wants to monitor with IT Assistant. Tom may want to record the IP subnet range of each subnet he wants to include in his discovery, any systems or ranges he wants to exclude from discovery, corresponding community names used on each subnet, and any other data he determines is relevant to his network. An example of a form that captures this data appears in Table 6-2. Note that Tom may monitor systems based on subnet range, host name, or IP address. Although it is advisable to limit the number of community names used in a network, Tom may also define multiple read-only and read-write community names in his network environment. For example, Tom may decide that he wants a common Get community name for all systems on this network but unique Set community names for certain data centers.

NOTE: IT Assistant offers a troubleshooting tool that can be useful in gathering system information and subnet ranges. Access the tool by selecting **Tools→Troubleshooting Tool** from the menu bar. For more information, open the Troubleshooting Tool dialog box and click Help.

Configuring SNMP on Each Managed System

Before configuring discovery, Tom needs to determine the Get and Set community names he wants to use for his network, and install and configure the SNMP agent and operating system SNMP service of each server he wants to manage. See "Configuring SNMP for Server Manageability (Both Scenarios)."

Table 6-2 provides information about the remote systems that Tom is monitoring.

Table 6-2. Example Subnet Ranges, IP Addresses, or Host Names and Corresponding Information for Data Center and Remote Servers

System Group Name	Include Subnet Range	Exclude Hosts or Subnet Range	Read-Only/Read-Write Community Names	Number of Devices on Subnet	Longest Ping Response Time Observed on Subnet (milliseconds)
Data Center Servers 1	192.166.153.*	192.166.153.2	dcp123/dcsecure01	100	64
Data Center Servers 2	192.166.154.*	examplehost	dcp123/dcsecure01	100	128
Data Center Servers 3	192.166.155.*	192.166.155.10-25	dcp123/dcxprivall	100	78
Data Center Servers 4	192.166.156.*		dcp123/dcxprivall	100	32
Data Center Servers 5	192.166.157.*		dcp123/dcxprivall	100	146
Data Center Servers 6	192.166.158.*		dcp123/dcxprivall	100	148
Data Center Servers 7	192.166.159.*		dcp123/dcxprivall	100	132
Data Center Servers 8	192.166.160.*		dcp123/dcxprivall	100	59
Data Center Servers 9	192.166.161.*		dcp123/dcxprivall	50	128
Remote Servers 1	10.9.72.*		dcp123/dcxprivrem	50	5600
Remote Servers 2	10.9.73.*		dcp123/dcxprivrem	100	2400
Dell|EMC Storage Devices	192.166.162.1-10		dcp123/NA	5	32
Printers	192.166.163.51-100		dcp123/NA	25	32
Tape Devices	192.166.163.1-20		dcp123/NA	10	59

Selecting An Appropriate Discovery Time-Out Value for the Network

Since Tom is monitoring remote systems across a WAN, time-out values may differ significantly between local systems and those further removed. In this case, it is recommended that Tom determine and set an appropriate time-out for the discovery of the systems located over the WAN.

In environments with long network latency times, such as global WANs, Tom may want to consider increasing ping time-outs across the enterprise. He can determine the ping times of systems that exhibit the greatest latency on the network by using the **Tools→Troubleshooting Tool** and selecting the **Device Connectivity** tab. From there, Tom can test the connection of high-latency systems to see whether he should increase specific ping times for better WAN performance.

Configuring Discovery Settings for the First Time in the Enterprise Network

Like Jane, if this is the first time IT Assistant has been launched since installation, Tom is presented with a welcome screen indicating that IT Assistant has not yet been configured. The four basic steps of configuration are listed:

Step 1: Discovery Configuration

Step 2: Inventory Configuration

Step 3: Status Polling

Step 4: Ranges

Clicking any of the steps will take him to the corresponding dialog box under the **Discovery and Monitoring** menu bar in IT Assistant. Steps 1 through 3 are single-window dialog boxes; step 4 is a wizard-based procedure for defining discovery ranges.

Configuring Discovery Configuration Settings

Tom also begins by configuring the discovery settings for his systems using the **Discovery Configuration Settings** dialog box. This dialog is displayed either automatically when he clicks *Step 1: Discovery Configuration* from the IT Assistant welcome screen or by choosing **Discovery Configuration** from the menu bar. Here, Tom enters information that IT Assistant will use for discovery. These values remain unchanged and apply to all the discovery ranges he will create later in this procedure. However, he can change these values at any time using this dialog box.

To configure discovery settings in IT Assistant for a large enterprise, Tom performs the following steps:

1 Tom selects **Discovery and Monitoring→Discovery Configuration** from the IT Assistant menu bar.

The **Discovery Configuration Settings** dialog box appears. **Enable Device Discovery** is selected by default.

2 Under **Initiate Device Discovery**, Tom selects when he wants IT Assistant to perform discovery.

Tom wants to perform discovery every day, so he selects **Every Week On**, each day of the week, and 2:00 a.m. for the start time. His network traffic is the lightest at this time.

3 Under **Discovery Speed**, Tom uses the sliding bar to indicate how much network bandwidth and system resources he wants to allocate to discovery.

Tom sets the discovery speed to **Fast** (all the way to the right). Tom wants to discover all of the systems he is going to manage with IT Assistant rapidly and get them in the database. For subsequent discoveries, if Tom finds that this setting dramatically impacts the network performance while he is attempting to perform other tasks on the network, he can change the **Discovery Speed** to consume fewer network resources.

4 Under **Discover**, Tom can choose whether to discover all devices or only instrumented devices.

5 Under **Name Resolution**, Tom can select **DNS Name Resolution** or **Instrumentation Name Resolution**.

Domain Name System (DNS) name resolution matches the IP address of a system to a host name. Instrumentation name resolution queries the managed system's agent instrumentation for its name. See your device or system documentation for more information on how to configure instrumentation name resolution.

NOTE: If you are managing a cluster, you must use instrumentation name resolution to be able to discern each independent node (system); otherwise, using DNS name resolution is recommended.

6 Tom clicks **OK**.

Configuring Inventory Settings

Next, Tom enters inventory settings. IT Assistant collects inventory information about software and firmware versions, as well as device-related information about memory, processor, power supply, PCI cards and embedded devices, and storage. This information is stored in the IT Assistant database and can be used to generate customized reports.

To set inventory settings, Tom performs the following steps:

1 Tom selects **Discovery and Monitoring→Inventory Configuration** from the menu bar.

The **Inventory Poll Settings** dialog box is displayed. **Enable Inventory** is selected by default.

2 In the dialog box under **Initiate Inventory**, Tom selects when he wants IT Assistant to perform inventory.

Tom sets inventory for weekly on Saturday at 3:00 a.m.

3 Under **Inventory Speed**, Tom uses the sliding bar to indicate how much network bandwidth and system resources he wants to allocate to inventory.

NOTE: The faster you set the inventory speed, the more network resources discovery will consume. Faster inventory speeds may impact network performance adversely.

4 Tom clicks **OK**.

NOTE: IT Assistant version 8.0 can now display the inventory information for printers, tapes, and storage devices. For more information, see the *Dell OpenManage IT Assistant Online Help*.

Configuring Status Polling Settings

Next, Tom defines status polling settings for his systems. IT Assistant performs a power and connectivity health check for discovered devices, determining whether a device is operating normally, is in a non-normal state, or is powered down. Status messages in IT Assistant include *healthy*, *warning*, *critical*, and *powered down*. Status icons also indicate if a system is not instrumented, if there is no information for the system, or the state the system was in when it was last powered down.

To set status polling settings, Tom performs the following steps:

1 Tom selects **Discovery and Monitoring→Status Polling Configuration** from the menu bar.

  The **Status Polling Configuration Settings** dialog box is displayed. **Enable Status Polling** is selected by default.

2 Under **Status Polling Interval**, Tom selects the interval he wants IT Assistant to use to perform status polling.

3 Under **Status Polling Speed**, Tom uses the sliding bar to indicate how much network bandwidth and system resources he wants to allocate to status polling.

  NOTE: The faster you set the status polling speed, the more network resources discovery will consume. Faster speeds may impact network performance.

4 Tom clicks **OK**.

Configuring Discovery Ranges

IT Assistant maintains a register of network segments that it uses to discover devices. A discovery range can be a subnet, range of IP addresses on a subnet, individual IP address, or an individual host name.

Tom's enterprise network is organized into a number of subnets. There are 850 servers in the datacenter and 150 remote servers. Tom refers to the IP subnet ranges he wrote down for his servers (see Table 6-2).

Tom's datacenter servers are divided into eight separate subnets, and his remote servers are divided into two subnets.

To identify his systems to IT Assistant, Tom must define a discovery range.

To identify an *include* range, Tom performs the following steps:

1 Tom selects **Discovery and Monitoring→Ranges** from the menu bar.

  The **Discovery Ranges** navigation tree is displayed on the left side of the IT Assistant window.

2 Tom expands **Discovery Ranges**, right-clicks **Include Ranges** and selects **New Include Range**.

  The **New Discovery Wizard** starts.

3 In step 1 of the wizard, Tom can enter an IP address, an IP address range, or a host name.

  Based on the information about Tom's systems in Table 6-2, he must add different IP address ranges. Tom can combine those ranges that have common settings (community name, timeouts, retry intervals, choice of protocol for discovery, and user credentials). For example, he can combine the Data Center Servers 3 to Data Center Servers 9 groups.

  He enters the IP address range as:

  192.166.155.*

Instead of completing this wizard multiple times with same entries in all the wizard panes to include all these systems, Tom clicks **Add** to add multiple ranges of IP addresses. The second time, he enters:

192.166.156.*

and so on.

NOTE: Ensure that you have a separate range for Dell|EMC devices. This is because apart from the SNMP credentials, Dell|EMC devices also require the Navisphere credentials.

Tom clicks **Next** to go to the next step.

NOTE: The Import Node List utility offers a convenient way to specify a list of host names, IP addresses, and subnet ranges for IT Assistant to discover. See the *IT Assistant Online Help* for instructions on how to run the utility from the command line. The **importnodelist.exe** file is in the **/bin** directory.

4 In step 2 of the wizard, Tom enters the Internet Control Message Protocol (ICMP) time-out and retry values for the range. Tom chooses the highest time-out retry value for the ranges that he combines. For example, in Table 6-2 for Data Center Servers 3 to Data Center Servers 9, Tom chooses 148 milliseconds, the highest time-out interval in that range.

5 In step 3 of the wizard, Tom configures the SNMP parameters to be used during discovery:

- Tom ensures the **Enable SNMP Discovery** option is selected.
- Tom enters a case-sensitive value for the **Get Community** name. The **Get Community** name is a read-only password that SNMP agents installed on managed systems use for authentication.

  Tom's considerations:

  Tom considers the following as he selects a **Get Community** name:

  Each SNMP managed system has a **Get Community** name. Tom ensures that he lists each of the community names on all of the systems he wants to manage. If Tom's managed systems have more than one community name, he can enter multiple community names separated by commas in the **Get Community** name field.

  Although the **Get Community** name affects read-only information retrieved by IT Assistant from managed systems, such as the results of discovery, status polling, and alert logs, Tom wants to limit access to this data. Therefore, he changes the default **Get Community** name (**public**) to a name known only to him and his system administrators.

  NOTE: Community names entered in the SNMP Get and Set community name fields for the managed system's operating system must match the Get Community and Set Community names assigned in IT Assistant.

- Tom enters a case-sensitive value for the **Set Community** name.

  Tom's considerations:

  The **Set Community** name is a read-write password that allows access to a managed system. SNMP agents running on the managed system use this password for authentication when actions are attempted on the system, including shutting down, configuring action alerts, and updating software.

  NOTE: Although Dell server instrumentation has an authentication layer above the SNMP Set community name (which requires a host name and password), many SNMP agents do not. Agents without this added security layer allow any user who knows the SNMP Set community name to gain control of the managed system.

  Tom chooses a **Set Community** name that matches the SNMP Set community value on the system he is managing. He also makes sure the name he chooses follows the secure password standards in place across his enterprise.

  NOTE: If you want to specify more than one SNMP Get or Set community name in an individual discovery range (for example, one community name for each IP subnet range), separate your community names with commas.

  NOTE: IT Assistant only uses SNMP sets to power cycle systems if the Server Administrator remote command line is not available. If SNMP sets are not required for this purpose, do not enter an SNMP set community name in the discovery wizard.

- Tom enters time-out and retry values for the SNMP discovery range.

6 In step 4 of the wizard, Tom configures the CIM parameters to be used during discovery.

Since Tom also has systems running Windows, he needs to configure CIM.

- Tom ensures **Enable CIM Discovery** is selected.
- In **Domain\User Name**, Tom enters the same name that he used to configure CIM on the managed system.
- Tom enters the same **Password** that he used for the CIM password on the managed system.

NOTE: You can enable the CIM Discovery option if you want to use the IPMI discovery support feature. This option is available only on *x*8*xx* and *x*9*xx* systems running the Windows Server 2003 R2 or other releases that support the Microsoft Hardware Management Provider.

7 In step 5 of the wizard, Tom selects the **Enable Dell/EMC Array Discovery**.

In this screen, Tom gives the following details:

- Navisphere Username
- Navisphere Password

NOTE: You can use this field only if you have Dell|EMC devices in the discovery range.

8 In step 6 of the wizard, Tom configures the following IPMI parameters of the BMC of his managed systems.

- User name
- Password
- KG Key

NOTE: KGKey is applicable only on *x9xx* systems, which support IPMI version 2.0. By default, KGKey is disabled on the BMC.

NOTE: If you have both *x8xx* and *x9xx* systems on your network and you enable the KGKey on *x9xx* systems, you will need to specify two separate ranges to discover these systems.

Since Tom has new uninstrumented (without any Dell agent installed) PowerEdge *x9xx* systems, he can discover these systems using IPMI discovery.

For more information, see "Using IPMI Discovery in Tom's Enterprise-Size Business."

9 In step 7 of the wizard, Tom can choose what action IT Assistant will take upon completion of the wizard.

10 In step 8 of the wizard, Tom reviews his selections and clicks **Finish** to complete the wizard.

NOTE: IT Assistant version 8.0 can now discover printers, tapes, and storage devices. For more information, see the *Dell OpenManage IT Assistant Online Help*.

Exclude Systems From Discovery

IT Assistant also provides the capability to exclude specific systems from discovery. This feature is normally used in larger enterprise environments to improve speed, to isolate a system with a problematic agent, or to enhance security and convenience.

Tom has one system in his enterprise that contains highly sensitive information. So sensitive, in fact, that he doesn't even want the system visible to his system administrators. Therefore, he sets an **Exclude Range** to isolate that system from routine network discovery.

1 Tom selects **Discovery and Monitoring→Ranges** from the menu bar.

The **Discovery Ranges** navigation tree is displayed on the left side of the IT Assistant window.

2 Tom expands **Discovery Ranges**, right-clicks **Exclude Ranges** and selects **New Exclude Range**.

The **New Exclude Range** dialog box appears.

3 Tom enters the IP address for the system and clicks **OK**.

As a result, that system is hidden from routine discovery by IT Assistant.

Changing Discovery, Inventory, and Status Polling Settings After Original Setup

Tom can return to the **Discovery and Monitoring** menu at any time and edit the settings he entered. The new settings will become effective the next time he performs the corresponding action.

Creating Alert Action Filters and Alert Actions for Tom's Large Enterprise

IT Assistant offers Tom the ability to set up Alert Action Filters that specify a set of system conditions. When these conditions are met, Tom can also create an Alert Action in IT Assistant that is triggered by the Alert Action Filter. The Alert Action takes whatever action Tom has defined.

IT Assistant has three types of filters:

Alert Action Filters – used to trigger actions when an alert condition is met

Ignore/Exclude Filters – used to ignore SNMP traps and CIM indications when they are received.

Alert View Filters – used to customize the Alert Log view

Before Tom creates Alert Action Filters or Alert Actions for his 1,000-server environment, he creates two custom groups to better facilitate event notification. According to the scenario outlined previously, most of Tom's servers are housed in a datacenter while some are remote. Tom's decides on this strategy for setting up IT Assistant.

He decides to:

1. Create one custom group for the datacenter servers and one custom group for the remote servers.
2. Create an Alert Action Filter for each of the four administrators who help Tom with the remote and datacenter servers on different days and different shifts.
3. Create an Alert Action that will be triggered by the corresponding Alert Action Filter to automatically e-mail the appropriate administrator at the appropriate day and time.

Tom's Administrators

Tom has three administrators; all are responsible for keeping the datacenter servers operational, and they work the following hours:

- Bob works onsite for the first shift Monday through Friday (7 A.M. to 7 P.M.)
- John works onsite second shift Monday through Friday (7 P.M. to 7 A.M.)
- Jill is on call weekends from 7 P.M. Friday to 7 A.M. Monday

Therefore, Tom wants to configure IT Assistant to:

- Notify Bob, John, and himself by e-mail any time a datacenter server warning or critical events occur
- Notify Jill by e-mail of any warning or critical events, but only if they occur during the time that she is on call

Creating Custom Groups

Tom requires two custom groups to manage notification of his four administrators who are going to take action on the critical and warning events for his 1,000 servers. The custom groups are remote servers and datacenter servers.

1 From the IT Assistant menu bar, Tom selects **Views→Devices.**

2 Tom right-clicks the top-level root in the IT Assistant navigation tree and selects **New Group**.

  The **Add Group Wizard** appears.

3 Tom enters a name and description for the group he wants to add.

  Tom names the group **Datacenter Servers**.

4 In the **Group Membership** dialog, Tom can either select the devices to include in the new group or, if a query-based group, he selects the query from the pull-down menu.

5 Tom review his selections in the summary screen and clicks **Finish** to complete the wizard.

6 Tom repeats the previous steps to create a second group named **Remote Servers**.

Creating an Alert Action Filter

Now, Tom will create an Alert Action Filter that includes each of the four administrators who work for him. In the following procedure, you can see how creating custom groups for the two types of servers make it easier to create the filters.

To create an alert action filter, Tom performs the following steps:

1 Tom selects **Alerts→Filters** from the menu bar.

  The **Alert Filters** window appears.

2 Tom expands the Alert Filters in the navigation tree and right-clicks **Alert Action Filters**. He selects **New Action Alert Filter**.

  The **Add Filter Wizard** appears.

  Tom plans to create three filters, one for each of the notification event actions that he is going to create for each of his administrators. Tom has to create each of his three filters one at a time. Tom creates filters for the following:

  - Datacenter first shift (M–F, 7 A.M.–7 P.M.)
  - Datacenter second shift (M–F, 7 P.M.–7A.M.)
  - Weekend administrator (7 P.M. Friday to 7 A.M. Monday)

3 Tom enters a descriptive name for the filter.

  Tom chooses **DC 1st Shift** as his name for the first filter. The names he chooses for the other two filters will be **DC 2nd Shift**, and **Weekend Admin**.

4 Under **Severity**, Tom selects the severity of the events for which he wants to receive alerts and logs.

  For the DC 1st Shift filter, Tom selects **Warning** and **Critical** and clicks **Next**.

5. Under **Alert Category Configuration**, Tom selects **Select All** because he wants to monitor all of the servers in his enterprise and clicks **Next**.

6. Under **Device/Group Configuration**, Tom selects the name of device or group to associate with the new action alert filter.

   Tom selects **Datacenter Servers**, the name of one of the custom groups he created previously and clicks **Next**.

7. Under **Date/Time Range Configuration**, Tom enters values for any or all of the optional categories.

   Tom selects different time and day values for each of the three filters. Tom does not select date filters, but could use this value if he wanted to create a filter and action for a vacation, an outside service vendor, or another special situation.

   For the DC 1st Shift filter, Tom enables the time range 7:00:00 A.M. to 7:00:00 P.M. and enables the days Monday through Friday.

   For the DC 2nd Shift filter, Tom enables the time range 7:00:00 P.M. to 7:00:00 A.M. and enables the days Monday through Friday.

   For the Weekend Admin filter, Tom specifies two filters (WA1 and WA2):

   - For WA1, Tom enables the time range 7:00:00 P.M. to 7:00:00 A.M. and selects the days Friday to Monday.
   - For WA2, he enables the time range 7:00:00 A.M. to 7:00:00 P.M. and selects the days Saturday and Sunday.

   Tom clicks **Next**.

8. Under **Alert Action Associations**, Tom decides whether he wants the event captured by the filter to trigger an action or be written to a log file.

   Tom selects **Alert**, since he wants IT Assistant to notify the selected administrators by e-mail when the system enters a Critical or Warning state.

   Click **Next**.

9. The **New Filter Summary** shows Tom's selections.

   He verifies that the filter name he assigned in step 3 appears in the **Summary of Alert Action Filters** window.

   Tom clicks **Finish** to accept the changes.

Notification Alert Actions in the Enterprise Environment

Tom's alert action filters and groups are now configured so that he can set up e-mail alert actions to automatically notify himself and his three administrators. Tom's strategy is as follows:

- Set up IT Assistant to send e-mail to his administrators when any warning or critical events occur, depending on their on-call or shift status
- Copy himself on all messages so he can to stay aware of overall server events

Tom is configuring e-mail for himself, as well as for his first- and second-shift datacenter administrators and his weekend administrator. Therefore, he will repeat the following procedure four times—for himself, Bob, John, and Jill.

NOTE: To send e-mail through IT Assistant, go to **Preferences→Web Server** on the top navigation bar, and configure the **SMTP Server Name (or IP Address)** and **DNS Suffix for SMTP Server**.

Creating an Alert Action

To create an alert action:

1 Tom selects **Alerts→Actions** from the menu bar.

2 Tom right-clicks **Alert Actions** in the navigation and selects **New Alert Action**.

The **Add Alert Action Wizard** appears.

3 Tom gives the action a logical name in the **Name** field.

Tom is configuring a separate Alert Action for himself, Bob, John, and Jill. Each time he repeats the procedure here, he uses the following names in the **Name** field:

- Tom ADMIN MGR e-mail
- DC 1st Shift Bob e-mail
- DC 2nd Shift John e-mail
- Weekend Admin Jill e-mail

4 From the **Type** pull-down menu, Tom chooses **Email**.

5 In the **E-mail Configuration** dialog, Tom specifies a valid e-mail address (within your enterprise's SMTP server group) to receive the automatic notification.

NOTE: Tom can test the e-mail configuration he specified by using the **Test Action** button. A success/failure message will be issued. Tom can specify multiple e-mail addresses, separated by a comma or semi-colon.

6 In **Alert Filter Associations**, Tom identifies the Action Alert filter that will trigger this e-mail.

Tom supplies the names of the Alert Filters he set up in the previous procedure—either **DC 1st Shift**, **DC 2nd Shift**, or **Weekend Admin—**each time he performs this step.

7 A summary dialog shows Tom's selections. He clicks **Finish** to accept the changes.

He verifies that the Alert Action he defined in step 3 appears in the **Summary of Alert Actions** window.

As a result of how Tom has configured Alert Action Filters and Alert Actions in IT Assistant, here is what will happen:

- IT Assistant will continuously monitor all servers on Tom's network.
- When any server reaches a warning or critical state, IT Assistant will automatically send Tom an e-mail notification at the address he specified in the Alert Action wizard.
- When any server reaches a warning or critical state, IT Assistant will automatically send either Bob, John, or Jill an e-mail notification depending on the date range specified in the Alert Action Filter wizard.

Using IPMI Discovery in Tom's Enterprise-Size Business

Let us say that Tom has purchased 100 Dell PowerEdge *x9xx* systems for his enterprise. These systems are equipped with the BMC that support IPMI versions 1.5 or later. These new systems are uninstrumented, that is, they do not have any Dell agent installed on them.

IT Assistant version 8.0 communicates with the BMC directly or through the Windows IPMI Provider on a Windows Server 2003 R2 system and classifies these systems under the **Server** category in the **Device** tree.

Using the IPMI discovery feature, Tom can:

- Classify his uninstrumented Dell devices
- View information about the uninstrumented devices
- Launch the Serial-Over-LAN (SOL) Proxy
- Launch the IPMI Shell (IPMISH) and perform remote power control tasks on the managed systems

NOTE: You should be logged on to the system before you turn off the system. Microsoft Windows does not allow turning off a system without a logging on to it.

Classification and Display of Non-Dell Systems

Devices discovered through IPMI will display under **Out of Band Unclassified Devices→IPMI Unclassified Devices**.

NOTE: This is applicable for non-Dell devices.

Each device will display in the tree as <*server hostname*>.

NOTE: If the host name is unavailable, the device will display the device IP address.

Devices with IPMI version 1.5 support only a limited notion of system health, including intrusion, fans, power supplies, and drives (off the internal backplane only). This health is a yellow or green indicator. Devices with IPMI version 2.0 support all health states, including normal, warning, and critical.

NOTE: PowerEdge *x8xx* systems support IPMI version 1.5 and *x9xx* systems support IPMI version 2.0.

Hardware Logs

Devices under the **IPMI Discovered Devices** group have a tab for viewing the hardware logs. Each time the view is refreshed, a connection will be made by the IT Assistant management system to the target system to retrieve the up-to-date logs. The connection will be closed after all the records are retrieved to free up resources and minimize connection usage, since the BMC has a limit on open connections.

The **Hardware Logs** tab is used for log retrieval through all supported protocols.

Launch Points

Tom right-clicks each device under **IPMI Discovered Devices** to access the launch point for Serial-Over-LAN (SOL). SOL is the only pre-configured application that can be launched from the **IPMI Discovered Devices** group.

NOTE: The Dell Remote Access Controller (DRAC) also has a telnet launch point to connect to the DRAC.

IPMISH Tasks

Tom can run IPMI Shell (IPMISH) tasks on the devices discovered through IPMI. If he selects devices from the **IPMI Enabled Devices** group, he can use either $IP or $BMC_IP.

NOTE: Use the -k parameter on the Baseboard Management Utility (BMU) command line to enter the IPMI encryption key.

Viewing Information on a Non-Dell System

Tom can view the embedded logs on a non-Dell device with Windows Server 2003 R2 (with System Management MSI installed), as well as view information available through the standard operating system instrumentation.

He should have enabled CIM discovery for the include range corresponding to the device, using the administrator privilege user account for CIM discovery.

NOTE: For non-administrator user accounts, the hardware management agent will not be discovered.

Click a device in the Device tree to view device information. The Hardware Logs tab contains information corresponding to the embedded logs.

The device summary tab contains information retrieved through the standard operating system instrumentation. This data includes NIC, operating system, BIOS, contact, memory, and processor information. The device will be listed under the **Unknown** category, as there is no device type information available through the standard operating system instrumentation.

Summary

This chapter has covered IT Assistant configuration in both the small-to-medium business and large enterprise network environments. Following the examples shown here will allow you to more successfully configure IT Assistant.

Many more features are available in IT Assistant than those illustrated here. Click the **Help** button in the appropriate IT Assistant dialog box to see detailed online help about that feature.

7

Performance Monitoring

Performance Monitoring helps you monitor the performance of a group of devices with supported Microsoft® Windows® or Linux operating systems over a specified period of time. Performance is monitored with the help of a set of performance counters available for each component. You can select and monitor these performance counters. You can configure thresholds for each performance counter and also configure alerts to be sent when the thresholds are crossed.

Using the Performance Monitoring feature, you can view the performance of individual devices rolled up on the **Device** tree. The overall performance of a device is calculated as the worst case status of the individual performance counter attributes monitored for the device. For example, if the status for the CPU Utilization counter is critical and the status of the memory paging counter is warning, the overall performance status of the devices is displayed as critical. From the **Device** tree, you can drill down to the performance counters and take appropriate actions.

To view details of how each performance counter is performing on a Dell™ PowerEdge™ system, do the following:

1. From the **Device** tree, expand the Server category
2. Select the PowerEdge system you want information on.
3. On the right hand side pane, select the **Performance** tab.

   This tab displays the performance counter information for the selected system.

   From this view, you can create multiple tasks to monitor multiple devices and manage these tasks, view results, and logs of these tasks.

NOTE: Performance monitoring enables you to monitor the usage of your systems as against monitoring the health of the systems.

Performance Monitoring in Tom's Enterprise-Size Business

Tom wants to use this feature to monitor how the PowerEdge *x9xx* systems on his network are being used.

His main considerations for using this feature are:

- Are the systems on my network under- or over-utilized?
- Do I need to move my hardware (for example, CPU) or applications to another system?
- How are my systems performing during peak and non-peak hours?
- Would I need to balance the load among my systems?

To be able to answer these questions, Tom would need to perform the following:

- Create a performance monitoring task
- Monitor the systems over a period of time
- View the data on the IT Assistant console
- Export the data into comma-separated values and save it for later use

Creating a Performance Monitoring Task

To create a performance monitoring task, Tom performs the following steps:

1. Tom selects **Manage→Performance Monitoring** from the menu bar.
2. Tom right-clicks **Performance Monitoring Task** and selects **New Task...**.

   The **New Task Wizard** appears.

3. Tom enters a descriptive name for the task. For example, *All x9xx systems*.

   Tom clicks **Next**.

4. Under **Select Schedule**, Tom selects a start date and an optional end date to measure the performance attribute. He selects a 24-hour schedule to monitor his systems during peak and non-peak hours.

   Tom also adjusts the sampling interval based on how often he wants to sample his systems.

   NOTE: Tom should take the network capacity into consideration. A bigger sampling interval would not give an accurate picture and a smaller interval may load the network and the monitored systems.

5. Under **Select Attributes**, Tom selects the CPU and Memory attributes and sets their warning and critical threshold values. For example, he sets the warning threshold for:

   - %**Kernel Utilization Time** as > 70% for 10 samples
   - %**Processor Utilization Time** as > 70% for 10 samples

   And the critical threshold for:

   - %**Kernel Utilization Time** as > 90% for 15 samples
   - %**Processor Utilization Time** as > 90% for 15 samples

   Tom can select **Send Warning Alert** or **Send Critical Alert** to receive warning or critical alerts.

   NOTE: If Tom sets a smaller sampling interval but selects a large number of counters, and devices, he may see a warning message indicating excess resource utilization. Tom should set a higher sampling interval or decrease the number of counters and devices to avoid this situation.

6. Under **Device Selection**, Tom selects the groups having his x9xx systems from the tree or provides a query.
7. Under **Enter Credentials**, Tom enters the operating system **User ID** and **Password**, which is valid for all selected devices.
8. Tom reviews his selection in the **Summary** screen and clicks **Finish**.

   The *All x9xx systems* task appears on the tree under the **Performance Monitoring Tasks** parent node.

Monitoring the Usage of the Systems on the Network

To monitor the usage of all PowerEdge *x9xx* systems on the network, Tom performs the following steps:

1. Tom clicks the *All x9xx systems* task under the **Performance Monitoring Tasks** parent node.
2. The summary of the task is displayed under the **Summary** tab on the right hand side of the screen.
3. To view the monitoring in greater detail, Tom selects the **Execution Results** tab.

   This tab displays the counters Tom chose in step 5 of the "Creating a Performance Monitoring Task."

   The counters keep a count of how a system is utilized.

   Tom can sort on the counters to view how a particular component, for example, the **%Kernel Utilization Time** for each system is being utilized.

   If the counters have been appropriately set, the counter colors would fairly indicate how well that systems are being utilized. Hover the mouse over the counter to get an indication of how the system component is performing.

   For example,

   If the counter is green for most of the time, it could indicate that the counter is well within the specified limits and could indicate that the system component is under- or partially-utilized

   If the counter is red for a small amount of time, it could indicate that the system component is partially-utilized

   If the counter is red for most samples, it could indicate that the system component is over-utilized.

   See Table 7-1 for a sample of how systems on Tom's network may be utilized.

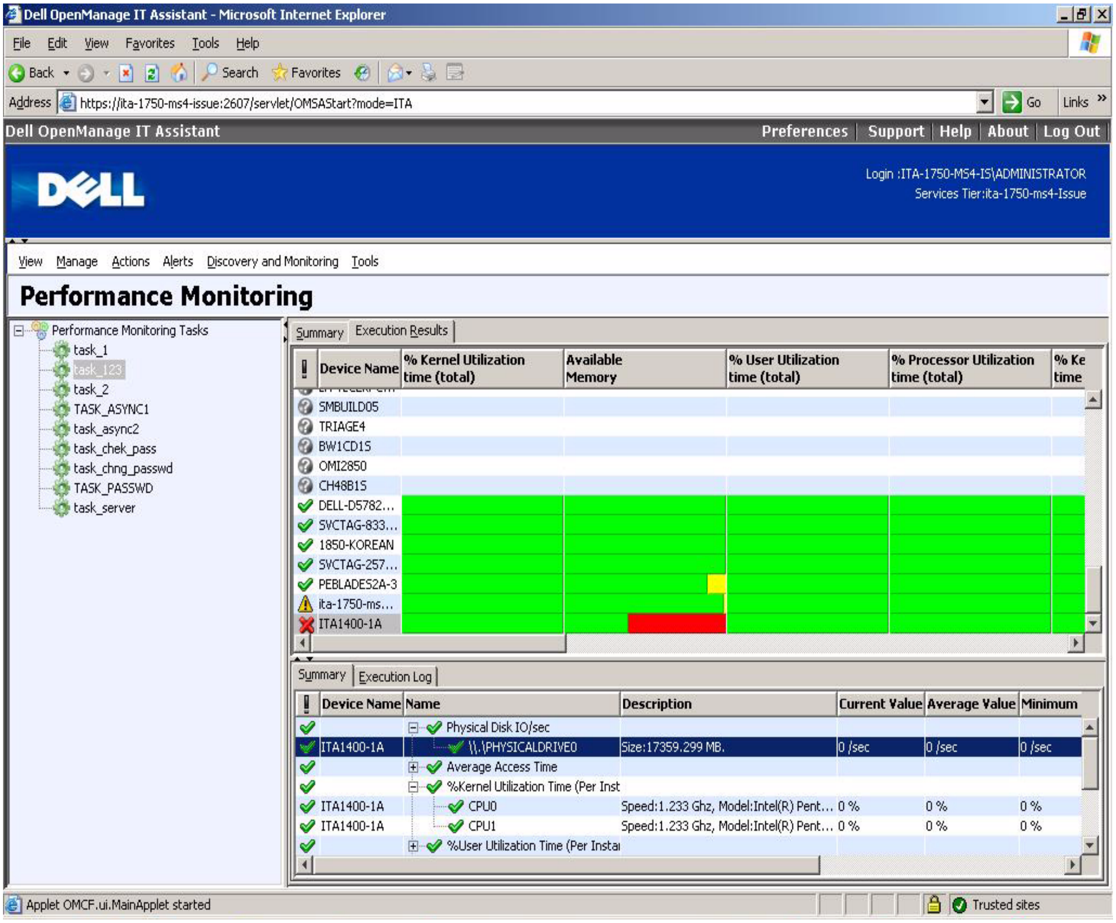
Table 7-1. Sample of Tom's network utilization

	CPU Utilization	Memory Utilization	Network Usage
System 1	High	Low	Medium
System 2	Low	High	Medium

If **%CPU Utilization Time** is red for most of the samples collected (highly used), it could mean that some application is over-utilizing the CPU. Tom could consider moving this application to a system for which the **%CPU Utilization Time** is green for most samples. In this case, from System 1 to System 2. Tom could also move a memory module from System 1 to System 2 to balance the load, or he could consider upgrading the hardware or purchasing new memory modules.

If Tom monitors his systems over the *weekend*, and finds out the network and CPU utilization counters are green (within the specified range) for 70% of the samples, yellow (non-critical) for 20% of the samples, and red (critical) for 10% of the samples collected, it could mean that the network and CPU utilization counters could be red for most samples during the *weekdays*. The systems will be overloaded, and Tom could decide to add more systems to his network or decide on some other form of load-balancing.

Figure 7-1. Sample Performance Monitoring Screen



Dell OpenManage IT Assistant - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ita-1750-ms4-issue:2607/servlet/OMSAStart?mode=ITA
Go Links
Dell OpenManage IT Assistant
Preferences | Support | Help | About | Log Out
DELL
Login :ITA-1750-MS4-IS\ADMINISTRATOR
Services Tier:ita-1750-ms4-Issue
View Manage Actions Alerts Discovery and Monitoring Tools

Performance Monitoring

- Performance Monitoring Tasks
  - task_1
  - task_123
  - task_2
  - TASK_ASYNC1
  - task_async2
  - task_chek_pass
  - task_chng_passwd
  - TASK_PASSWD
  - task_server

Summary | Execution Results

!	Device Name	% Kernel Utilization time (total)	Available Memory	% User Utilization time (total)	% Processor Utilization time (total)	% Ke time
?	SMBUILD05					
?	TRIAGE4					
?	BW1CD15					
?	OMI2850					
?	CH48B15					
✓	DELL-D5782...	🟩	🟩	🟩	🟩	🟩
✓	SVCTAG-833...	🟩	🟩	🟩	🟩	🟩
✓	1850-KOREAN	🟩	🟩	🟩	🟩	🟩
✓	SVCTAG-257...	🟩	🟩	🟩	🟩	🟩
✓	PEBLADES2A-3	🟩	🟩🟨	🟩	🟩	🟩
⚠	ita-1750-ms...	🟩	🟩	🟩	🟩	🟩
✗	ITA1400-1A	🟩	🟩🟥	🟩	🟩	🟩

Summary | Execution Log

!	Device Name	Name	Description	Current Value	Average Value	Minimum
✓		⊟ ✓ Physical Disk IO/sec				
✓	ITA1400-1A	✓ \\.\PHYSICALDRIVE0	Size:17359.299 MB.	0 /sec	0 /sec	0 /sec
✓		⊞ ✓ Average Access Time				
✓		⊟ ✓ %Kernel Utilization Time (Per Inst				
✓	ITA1400-1A	✓ CPU0	Speed:1.233 Ghz, Model:Intel(R) Pent...	0 %	0 %	0 %
✓	ITA1400-1A	✓ CPU1	Speed:1.233 Ghz, Model:Intel(R) Pent...	0 %	0 %	0 %
✓		⊞ ✓ %User Utilization Time (Per Instai				

Applet OMCF.ui.MainApplet started

4 In the **Execution Results** tab, Tom can right-click a counter and do one of the following:

- Select **Export**. This will export the details into a comma-separated values (CSV) file. Tom can then use other tools like Microsoft® Excel to generate better reports.
- Click **View Chart** to view the graphical representation of the performance information of the device. Tom can give a time range and view the system usage graphically.

  NOTE: Tom can also view the charts and export them from the **Summary** tab, in the lower pane.
- Click **Delete Execution Results**.
- Right-click a column header and select **Customize View**. This view customizes the view for the devices.

5 In the **Execution Log** tab, Tom can view the execution summary information for each run of the task. He can also use the time selection fields to select the **From** time he wants to view the logs.

NOTE: The execution log entries will be purged if the execution log entries are older than 14 days.

6 In the **Performance** tab on the **Device** tree, Tom can view the performance counter information for the selected device.

Suggested Threshold Configuration for Performance Monitoring

Table 7-2 shows the sample threshold settings for each performance counter.

Table 7-2. Sample Threshold Settings for Performance Counters

Resource	Performance Counter Attribute	Suggested Threshold	Comments
CPU	%Processor Utilization Time	Less than 85%	Total processor usage should remain under 85%, infrequent spikes exceeding 85% for brief periods is acceptable.
System	Context Switch/second	Depends on the system activity	Continued spikes for a prolonged time may indicate an increase in system load.
System	Processor Queue Length	2	Depends on the number of processors in the system. This is an instantaneous number. Needs observation over several cycles.
Memory	Available Memory	Less than 10 -20% of installed RAM Less than 4MB for systems with large memory	If available memory is under 10% – 20% of the installed RAM for an extended period, it may indicate need for more memory.
Memory	Pages/Second	Less than 20	Should remain under 20 with the exception of brief spikes.
Memory	%Page File Usage	95%	Review this value in conjunction with Available Memory and Pages/Second.
Network	BytesReceived/Second PacketsReceived/Second BytesSent/Second PacketsSent/Second	Sharp deviation from average values for an extended period of time. Depends on the type of network	A sharp increase or decrease above normal levels is a strong indicator of network issues.
Physical Disk	Physical Disk I/O per Second	Depends on manufacturer's specifications	Check the specified transfer rate for your disks to verify that this rate does not exceed the specifications. In general, Ultra Wide SCSI disks can handle 50 to 70 I/O operations per second.
Logical Disk	Free Space	Less than 15%	Threshold value is relative to the total amount of disk space and the average I/O activity on the system.

Resource Usage by SQL Server and IT Assistant

Table 7-3 shows the recommended hardware configuration required for performance monitoring.

Table 7-3. Recommended Hardware Configuration for IT Assistant for Performance Monitoring

Minimum Number of CPUs	Minimum Memory Required	Database	Maximum Number of user sessions per user	Maximum Number of Performance Counters	Minimum Supported Sampling Frequency	Maximum Number of Devices
Single CPU 2.0 GHz	512 MB	MSDE/SQL Express 2005	1	10	2 minutes	15
Single CPU 2.0 GHz	512 MB	MSDE/SQL Express 2005	1	18	2 minutes	8
Single CPU 2.0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	10	2 minutes	30
Single CPU 2.0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	18	2 minutes	20
Dual CPU 2.0 GHz	1 GB	SQL 2000/ SQL 2005 Server	2	10	3 minutes	100
Dual CPU 2.0 GHz	1 GB	SQL 2000/ SQL 2005 Server Enterprise Edition	5	10	5 minutes	200

NOTE: The hardware configuration listed in this table refer to the minimum supported configuration. For the most recent update on these requirements, see the IT Assistant readme on the Dell Support website at **support.dell.com**.

8

Software Updates

The software update feature of Dell OpenManage™ IT Assistant version 8.0 comprises:

- Repositories: A repository is a container for Dell Update Packages and System Update Sets. Update Packages are available from the *Dell™ PowerEdge™ Installation and Server Management* CD, *Dell™ PowerEdge™ Server Update Utility* CD, or the Dell website at **ftp.dell.com**.
  The repositories are displayed in a hierarchical tree view, with **Software Update Repositories** as the parent and **IT Assistant Repository** as the child node.
- Custom update sets: You can create custom System Update Sets or bundles. These custom update sets can be subsequently used to drive system compliance reports and perform the updates.

  NOTE: You can create custom bundles only from the system bundles that have been imported into the IT Assistant Repository.
- Digital Signature verification: IT Assistant checks the authenticity and integrity of the update packages and MSI files using digital signature verification.

IT Assistant provides a centralized software update capability. You can load Dell Update Packages and System Update Sets into the IT Assistant repository, then run a compliance check of all the systems in your enterprise against the Update Packages. A System Update Set is a logical set of Dell-certified packages that work together without problems. Dell Update Packages are available from the Dell Support website at **support.dell.com** or from the *Dell PowerEdge Server Update Utility* CD. This CD is available through the Dell OpenManage Subscription Service or as an ISO image downloadable from the Dell Support website at **support.dell.com**. You can download the Dell OpenManage Subscription Service from **www.dell.com**.

The *Dell PowerEdge Server Update Utility* CD contains quarterly updates to the Dell Update Packages and System Update Sets (certified sets of packages for specific PowerEdge platforms).

To use the Dell Update Packages from within IT Assistant, perform the following steps:

1. Insert the *Dell PowerEdge Server Update Utility* CD into the CD drive
2. Navigate to **Manage→Software Updates**.
3. Right-click the root node (**Software Update Repositories**) and select **Open Repository (Update CD)…**.
4. Navigate to the CD location and locate the repository directory.
5. Select **catalog.xml** and click **Open**.
   The contents of the *Dell PowerEdge Server Update Utility* CD will be displayed on the IT Assistant UI. You can then perform operations such as importing packages, performing compliance checks, and performing software updates.

Using Software Updates in IT Assistant

Let us look at how Jane might use this feature in her enterprise.

Jane has downloaded an Update Package from the Dell Support website at **support.dell.com**. She knows that some of her systems need the firmware upgrade that the update package contains, but she wants to determine which ones without manually checking each of her 50 servers. She can use IT Assistant to quickly find out.

Here is how she would find out how many systems need an update:

1 Select **Manage→Software Updates** from the menu bar.

2 Right-click **IT Assistant Repository** in the left navigation pane and choose **Add**.

Jane navigates to the location on her system where she downloaded the Update Package. When she selects the file and clicks **Open**, IT Assistant adds the update package to the window.

3 Clicking the Update Package name in the left-hand pane shows a summary of its contents in the right-hand pane.

4 Click the **Compliance** tab, then click a specific group of devices (or a query) against which you want to check the package.

5 Click **Compare** to check the devices you selected against the contents of the Update Package.

IT Assistant performs a comparison and generates a compliance report that shows a graphical presentation of the differences, full version information on the selected devices, and other information that can help identify non-compliant systems or devices.

6 If IT Assistant finds servers or devices that need updating, Jane can select the devices she wants to update and click the **Update** button. This action automatically starts the **Software Updates** task wizard.

NOTE: You cannot upgrade the firmware on the system running IT Assistant. To upgrade the firmware on this system, run the software updates from another system.

Using Server Software Deployment

IT Assistant provides an integrated method to install Dell OpenManage Server Administrator on supported Dell systems.

NOTE: In the system where you run the IT Assistant user interface from, the Java Runtime Environment (JRE) should have at least 256 MB of free space for the JRE memory (heap memory). This memory requirement is recommended for IT Assistant to download the MSI file that contains the Dell agent. The MSI file size is typically in the range of 60–64 MB.

Setting the Java Runtime Parameter in Supported Windows Environment

1. Click the **Start** button. Point to **Settings**→**Control Panel**→**Java**.
2. In the **Java** tab, click **View** in the **Java Applet Runtime Settings** section.
3. Set **Java Runtime Parameters** to **-Xmx256M**.

Setting the Java Runtime Parameter in Supported Linux Environment

1. Navigate to the Java home directory. The default path is **/usr/java/jre1.5.xxx/bin/**.
2. Run **./ControlPanel**.
3. In the **Java** tab, click **View** in the **Java Applet Runtime Settings** section.
4. Set **Java Runtime Parameters** to **-Xmx256M**.

Installing the Dell Agent on a Remote Managed Node

If you are managing a corporate network using IT Assistant, you can install the latest Dell OpenManage Server Administrator on multiple systems in the environment. These systems may or may not have Server Administrator previously installed on them.

Obtain a Server Administrator MSI file from one of the following sources:

- *Dell™ PowerEdge™ Installation and Server Management* CD

  NOTE: IT Assistant version 8.0 supports Server Administrator deployment only on Microsoft® Windows® operating systems.

- Dell Support website at **support.dell.com** - FTP download

Use the task management feature in IT Assistant to create a Software Agent Deployment task to schedule the deployment of Server Administrator on multiple systems on the network. After Server Administrator is installed, the new status will display:

- Only if you forcibly discover, inventory, or do a manual status poll.
- After the next scheduled discovery, inventory, or status poll.

NOTE: The protocol configuration settings for inventory must be specified for the device during initial device detection and the corresponding services must be running on the device.

Creating a Software Deployment Task

1. Select **Manage**→**Tasks** from the menu bar.
2. Under the **Task** parent node, right-click **Software Deployment** and select **New Task...**.

   The **New Task Wizard** appears.

3. Under **Task Creation**, enter a descriptive name for the task and select the **Server Administrator Deployment** task.

   Click **Next**.

4 Under **Task Installer Specification**, specify the **Installation File Path**.

NOTE: The default installation path on the *Dell™ PowerEdge™ Installation and Server Management* CD is **<CD>\srvadmin\windows\SystemsManagement\SysMgmt.msi**.

NOTE: Ensure that you select only the version 5.0 or later **SysMgmt.msi** file. The **.msi** files of earlier versions of Dell OpenManage are not supported by IT Assistant 8.0. You can check the version of Server Administrator by right-clicking the **SysMgmt.msi** file and selecting **Properties**. The Server Administrator version is displayed in the **Summary** tab.

NOTE: Ensure that there is sufficient free space (at least 65 MB) on the management station for creating the task. The managed node should have about 130 MB of free space in **%SYSTEMDRIVE%** or the drive where the operating system is installed.

NOTE: This feature supports only ADDLOCAL parameter. For more information on this parameter and the arguments you use with it, see the *Dell OpenManage Installation and Security User's Guide*.

It is recommended that you select **Upgrade Installer Engine on target node (if required)**. This option ensures that the latest version of **msiexec** is installed on the managed systems.

If you do not select this option, and the managed systems do not have the required version, a error message is displayed.

NOTE: This option fails if the required upgrade engine files (**.exe** and **.bat**) are not found in the same folder as the Systems Management installer (**.msi**). If you deleted these files, go to **ftp.dell.com** and download them to the **SystemsManagement** folder.

5 Under **Device Selection**, select the appropriate systems on which Server Administrator is to be deployed.

NOTE: IT Assistant performs prerequisite checks at the time of task execution and execution details can be viewed in the **Task Execution Details** pane. If the task execution fails, correct the error (for example, inadequate disk space) and run the task again. For more information, see the *Dell OpenManage IT Assistant Online Help*.

6 Under **Select Schedule**, you can either schedule the task to run at a specified time, or run the task immediately.

7 Under **Enter Credentials**, enter your operating system credentials

8 View and verify your selections in **Summary**.

9 Click **Finish** to accept your selection, or **Back** to make changes.

NOTE: At this point, the files will be uploaded to the IT Assistant Repository. This process may take a few minutes.

Reporting and Task Management

Dell OpenManage™ IT Assistant provides the ability to:

- Create customized reports for all systems in your enterprise
- Execute command line instructions on managed devices from a central console, including shutdown and wake up
- Perform software compliance checking and updates on an individual managed system

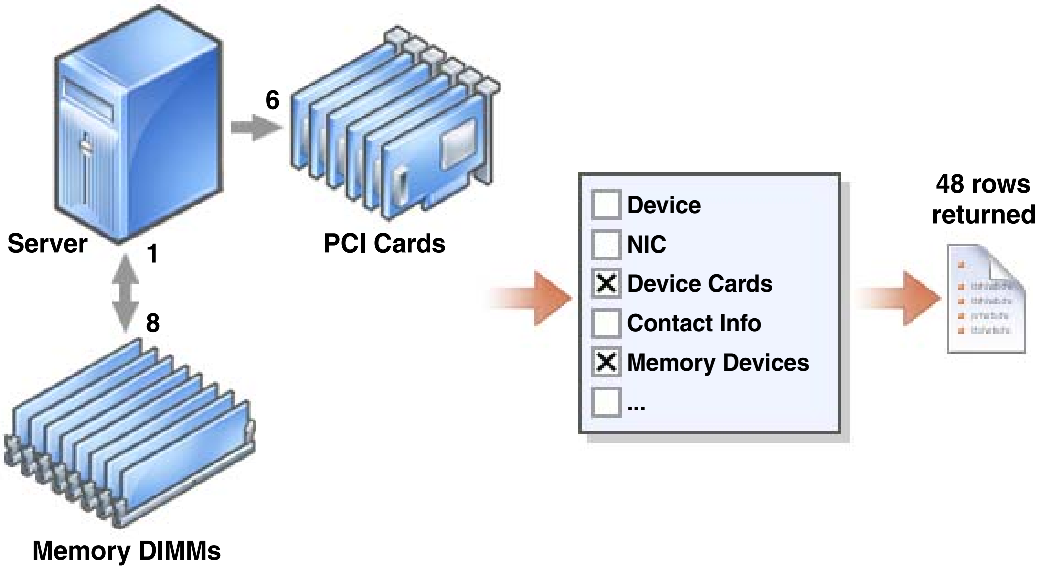
The basics of these capabilities are shown here using the same user scenarios presented in "Configuring Dell OpenManage™ IT Assistant to Monitor Your Systems." For more detailed information on these topics, see the *Dell OpenManage IT Assistant Online Help*.

Custom Reporting

IT Assistant uses data from the Microsoft® SQL Server database to create customized reports. These reports are based on data gathered during discovery and inventory cycles.

The devices or groups that you select to include in your report correspond to fields in the IT Assistant database. When you execute a report, a database query is created. The following figure provides an example.

Figure 9-1. Custom Reporting in IT Assistant



For example, you can compile a report containing:

- Details of the hardware devices being managed by IT Assistant, including servers, switches, and storage devices
- BIOS, firmware, and driver versions contained on specific devices
- Other asset or cost of ownership details

You can specify different output formats for any report, such as HTML, XML, or CSV (comma-separated values). Any customized report template you create can be saved and used later.

Creating a New Report

To illustrate IT Assistant's report capabilities, let us take another look at Jane's enterprise:

Among her group of managed systems, she has 50 Dell™ PowerEdge™ servers. However, she is not sure exactly which servers have which type of network interface card installed. She can answer that question quickly by using IT Assistant's reporting tool:

From IT Assistant, Jane will:

1. Select **Views→Reports**, then right-click **All Reports** in the left navigation pane.
2. Choose **New Report**.

   The Add Report wizard starts.

   She then specifies the following:

   - A **Name** for her report, not to exceed 64 characters
   - An optional **Description**

   Click **Next**.
3. In the **Select Devices** dialog box, Jane chooses **Select devices/groups from the tree below**, then **Servers** from the available devices list.

   NOTE: Selecting the top-level attribute in the device list automatically selects all of the attributes below it. Expanding the attributes in the tree allows you to select the specific attributes that you want to include. A check mark with a gray background for the group selection indicates that you have made individual selections within the group. A check mark with a white background indicates that you have selected the entire group. Consequently, as the group membership changes, the selection is applicable to the modified group members.

   Click **Next**.
4. Under **Select Attributes**, she chooses **NIC**.
5. Then, she specifies a preferred **Sort by** order and clicks **Next**.
6. On the **Summary** page, she either accepts her choices or goes back and changes them. This creates a new report with the name Jane specified in step 2.

When Jane has confirmed her configuration, she goes to the reports window in IT Assistant and right-clicks the report name she created and chooses **Execute→HTML Reports**.

An HTML format-based report showing NIC device information for each of the 50 PowerEdge servers in her enterprise is displayed.

Choosing a query-based report:

Jane could also opt for a query-based report. Instead of choosing **Select devices/groups from the tree below** in the report wizard, she could choose **Select a query**. Then, she can either select a query that she created earlier, or create a new query by clicking the **New** button. She can specify the parameters for a query report as shown in the following table:

Table 9-1. Query Report Parameters

Name of the Query	Specifies the name of the query.
Query Criteria	Specifies the query criteria. For example, to create a new query with the query criteria for all devices that correspond to a subnet, specify: `Where: IP Address Starts With 143.166.155` The query operators are: • Contains — Specifies that the query criteria string contain a certain set of characters. • Ends With — Specifies that the query criteria string ends with a certain set of characters. • Is — Specifies that the query criteria string exactly match these characters. • Starts With — Specifies that the query criteria string starts with these characters. You can expand the query with up to 10 subqueries, which together constitute the complete query. Join the subqueries by using AND/OR operators. **NOTE:** If you make any changes while editing an existing query and save that query, the original query is replaced.
Run Query	Runs the query and displays the results.
Save Query	Saves the query.
Cancel	Closes the **Query Editor** window without saving your input.

NOTE: You can click **Run Query** to test a query before saving it.

NOTE: If you want to run reports on RAC devices, and choose **RAC type** as one of the attributes to include in the report, the generated report may list the values 2, 8, or 16 against the RAC type column. These values are mapped as follows:
2 = DRAC II
8 = DRAC III/DRAC 4/DRAC 5
16 = Baseboard Management Controller (BMC)

Editing, Deleting, or Running Reports

Whichever type of report she creates, Jane can edit, delete, rename, or run it at any time by right clicking the report name in the **Reports** window.

Pre-defined Reports

IT Assistant provides several pre-defined reports you can use immediately. These reports will be displayed in the left portion of the **Reports** window. Click the report name to see a summary of the information the report is designed to gather.

IT Assistant Database Schema Information

IT Assistant gathers data that is stored in associated tables and is linked by the **DeviceID**, an internal identifier. The associated data is stored in the following tables.

NOTE: The primary keys for the tables are marked with an asterisk (*).

Table 9-2. IT Assistant Database Schema

Column Name	Data Type	Data Size	Nulls Allowed	Description
Device Table				
DeviceId*	int	4	No	Internal device identification used as a Foreign Key in all related tables.
DeviceName	nvarchar	256	Yes	The name IT Assistant uses to identify the device, which is the name shown in the **Device Tree** in the user interface (UI).
DeviceInstrumentationName	nvarchar	256	Yes	The name of the device retrieved from the MIB II SysName or CIM.
DeviceDNSName	nvarchar	256	Yes	Fully qualified name as returned by the DNS Server

DeviceType	int	4	Yes	The type of device.
				Workstations = 3
				Servers = 4
				Desktops = 5
				Portables = 6
				Network Switches = 8
				RACs = 9
				KVMs = 10
				Unknown = 2 or any value not listed

DeviceInventoryTime	datetime	8	Yes	The last time that IT Assistant collected inventory data from the device.
DeviceStatusedTime	datetime	8	Yes	The last time that IT Assistant collected the global health data from the device.
DeviceDiscoveredTime	datetime	8	Yes	The last time IT Assistant interrogated the system to determine what agents were present.
DeviceProtocols	int	4	Yes	Bitmask indicating what protocols the device supported. Bit 1 = SNMP Bit 4 = CIM Bit 8 = IPMI

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
DevicePreferredProtocol	int	4	Yes	The protocol by which the remote device prefers to be managed. 1 = SNMP 2 = CIM
DeviceAssetTag	nvarchar	64	Yes	This attribute defines the device's asset tag.
DeviceServiceTag	nvarchar	64	Yes	This attribute defines the device's service tag.
DeviceSystemId	int	4	Yes	The manufacturer's ID for the system model.
DeviceSystemModelType	nvarchar	64	Yes	The manufacturer's model name.
DeviceLocation	nvarchar	256	Yes	The device location as retrieved from the remote agent.
DellSystem	int	4	Yes	The Boolean flag indicating if the device has a Dell-enabled agent.
SubnetLastDiscoveredOn	nvarchar	256	Yes	The last discovery range that was used to discover the device.
Agent Table				
DeviceId*	int	4	No	The Foreign Key (FK) to the Device Table.
AgentName*	nvarchar	256	No	The name of the agent.
AgentVersion	nvarchar	64	Yes	The version of the agent.
AgentManufacturer	nvarchar	64	Yes	The manufacturer of the agent.
AgentDescription	nvarchar	256	Yes	A brief description of what the agent manages.

AgentGlobalStatus	int	4	Yes	The global status of the agent.
				Not Known = 0
				Unknown = 1
				Normal = 4
				Warning = 8
				Critical = 16

AgentInstallTime	datetime	8	Yes	The time the agent was installed, if available.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
AgentId	int	4	Yes	Internal ID used to distinguish between agents. RAC Out-Of-Band Agent = 1 Server Administrator = 2 Microsoft® WMI =3 OMCI = 4 Physical Manager = 6 Storage Manager = 7 Dell™ PowerEdge™1655MC Switch = 8 Dell PowerConnect™ 3248 = 9 PowerConnect 5224 = 10 PowerConnect 3024 = 11 PowerConnect 5012 = 12 PowerConnect 3048 = 13 PowerConnect 3000MIB = 14 KVM = 15 Inventory Agent = 16 RAC In-Band Agent = 17
AgentURL	nvarchar	256	Yes	The Web address of the management application (if the agent supports a Web-based access).
AgentData	ntext	16	Yes	Extended agent data; for internal use only.
Array Disk Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ArrayDiskNumber*	int	4	No	The instance number of this array disk entry.
ArrayDiskName	nvarchar	256	Yes	The array disk’s name as represented in Storage Management.
ArrayDiskVendorName	nvarchar	64	Yes	The array disk's (re)seller's name.
ArrayDiskModelNumber	nvarchar	64	Yes	The array disk’s model number.
ArrayDiskSerialNumber	nvarchar	64	Yes	The array disk's unique identification number from the manufacturer.
ArrayDiskPartNumber	nvarchar	64	Yes	The array disk’s part number.
ArrayDiskRevision	nvarchar	64	Yes	The array disk's firmware version.
ArrayDiskEnclosureId	nvarchar	64	Yes	The SCSI ID of the enclosure processor to which this array disk belongs.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
ArrayDiskChannel	int	4	Yes	The bus to which this array disk is connected.
ArrayDiskLength	int	4	Yes	The array disk's size in gigabytes. If the size is 0, it is smaller than a gigabyte.
ArrayDiskBusType	nvarchar	64	Yes	The array disk's bus type. Possible values: SCSI, IDE, Fibre Channel, SSA, USB, and SATA.
ArrayDiskTargetId	int	4	Yes	The SCSI target ID which this array disk is assigned.
ArrayDiskLUNId	int	4	Yes	The durable unique ID for this array disk.
Controller Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ControllerNumber*	int	4	No	The instance number of this controller entry.
ControllerName	nvarchar	64	Yes	The name of the controller in this subsystem as represented in Storage Management. Includes the controller type and instance, for example: PERC 3/QC 1.
ControllerVendor	nvarchar	64	Yes	The controller's reseller's name.
ControllerType	nvarchar	64	Yes	The type of controller.
ControllerState	nvarchar	64	Yes	The current condition of the controller's subsystem.
ControllerStatus	int	4	Yes	The controller's status
ControllerFWVersion	nvarchar	64	Yes	The controller's current firmware version.
ControllerCacheSize	int	4	Yes	The controller's current amount of cache memory.
ControllerPhysicalDeviceCount	int	4	Yes	The number of physical devices on the controller channel, including both disks and the controller.
ControllerLogicalDeviceCount	int	4	Yes	The number of virtual disks on the controller.
ControllerPartnerStatus	nvarchar	64	Yes	Indicates the availability of the redundant controller in a redundant configuration.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
ControllerMemorySize	int	4	Yes	The amount of memory on the controller.
ControllerDriveChannelCount	int	4	Yes	The number of redundant controller drive channels.
ControllerChargeCount	int	4	Yes	The number of charges that have been applied to the battery on this controller.
ControllerDriverVersion	nvarchar	64	Yes	The currently installed driver version for this controller.
ControllerSPAReadCacheSize	int		Yes	The read cache size on controller A.
ControllerSPAWriteCacheSize	int		Yes	The write cache size on controller A.
ControllerSPBReadCacheSize	int		Yes	The read cache size on controller B.
ControllerSPBWriteCacheSize	int		Yes	The write cache size on controller B.
ControllerCachePageSize	int		Yes	The page cache size for the controller.
ControllerSPAReadCachePolicy	nvarchar	64	Yes	The read cache policy on controller A.
ControllerSPAWriteCachePolicy	nvarchar	64	Yes	The write cache policy on controller A.
ControllerSPBReadCachePolicy	nvarchar	64	Yes	The read cache policy on controller B.
ControllerSPBWriteCachePolicy	nvarchar	64	Yes	The write cache policy on controller B.
Enclosure Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
EnclosureNumber*	int	4	No	The instance number of the enclosure entry.
EnclosurePartNumber	nvarchar	64	Yes	The part number of the enclosure entry.
EnclosureSerialNumber	nvarchar	64	Yes	The serial number of the enclosure entry.
EnclosureName	nvarchar	256	Yes	The enclosure's name.
EnclosureVendor	nvarchar	256	Yes	The enclosure's reseller's name.
EnclosureId	int	4	Yes	The SCSI address of the processor.
EnclosureLocationofManufacture	nvarchar	256	Yes	The enclosure’s manufacture location.
EnclosureServiceTag	nvarchar	64	Yes	The enclosure identification used when consulting customer support.
EnclosureAssetTag	nvarchar	64	Yes	The user-definable asset tag for the enclosure.
EnclosureAssetName	nvarchar	64	Yes	The user-definable asset name for the enclosure.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
EnclosureProductId	nvarchar	64	Yes	The enclosure's product identification, which also corresponds to the enclosure type.
EnclosureType	nvarchar	64	Yes	The type of enclosure.
EnclosureChannelNumber	int	4	Yes	The channel number, or bus, to which the enclosure is connected.
EnclosureBackplanePartNum	nvarchar	64	Yes	The part number of the enclosure's backplane.
EnclosureSCSIId	int	4	Yes	The SCSI ID of the controller to which this enclosure is attached.
Enclosure Management Module Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
EMMNumber*	int	4	No	The instance number of the enclosure management module.
EMMName	nvarchar	256	Yes	The name of the enclosure.
EMMVendor	nvarchar	256	Yes	The management module reseller's name.
EMMPartNumber	nvarchar	64	Yes	The part number of the enclosure memory module.
EMMFWVersion	nvarchar	64	Yes	Firmware version of the enclosure memory module.
VirtualDisk Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
VirtualDiskNumber*	int	4	No	Instance number of this virtual disk entry.
VirtualDiskName	nvarchar	256	Yes	The virtual disk's label generated by Storage Management or entered by the user.
VirtualDiskDeviceName	nvarchar	256	Yes	Device name used by this virtual disk's member disks.
VirtualDiskLength	int	4	Yes	The size of this virtual disk in gigabytes.
VirtualDiskWritePolicy	nvarchar	64	Yes	Indicates whether the controller's write cache will be used when writing to a virtual disk.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
VirtualDiskReadPolicy	nvarchar	64	Yes	Indicates whether the controller's read cache will be used when reading from a virtual disk.
VirtualDiskCachePolicy	nvarchar	64	Yes	Indicates whether the controller's cache is used when reading from or writing to a virtual disk.
VirtualDiskLayout	nvarchar	64	Yes	The virtual disk's RAID type.
VirtualDiskStripeSize	int	4	Yes	The stripe size of this virtual disk in bytes.
VirtualDiskStripeElementSize	int	4	Yes	The stripe element size of this virtual disk in blocks.
VirtualDiskTargetId	int	4	Yes	Unique ID for the virtual disk.
VirtualDiskLUNId	nvarchar	64	Yes	The durable unique LUN ID for this virtual disk.
Volume Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
VolumeNumber*	int	4	Yes	Instance number of the volume entry.
VolumeDriveLetter	nvarchar	64	Yes	The volume's path (or drive letter) according to the operating system.
VolumeLabel	nvarchar	256	Yes	The user-definable label for this volume.
VolumeSize	int	4	Yes	The size of the volume in megabytes.
Firmware Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
FirmwareChassisIndex*	int	4	No	The firmware chassis index (zero based).
FirmwareIndex*	int	4	No	The firmware index (zero based).
FirmwareType	nvarchar	64	Yes	The firmware type.
FirmwareName	nvarchar	64	Yes	The name of the firmware.
FirmwareVersion	nvarchar	64	Yes	The firmware version.
MemoryDevice Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
MemoryDeviceChassisIndex*	int	4	No	This attribute defines the index (one based) of the associated chassis.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
MemoryDeviceIndex*	int	4	No	This attribute defines the index (one based) of the memory device.
MemoryDeviceName	nvarchar	256	Yes	This attribute defines the location of the memory device.
MemoryDeviceBankName	nvarchar	256	Yes	This attribute defines the location of the bank for the memory device.
MemoryDeviceType	nvarchar	256	Yes	This attribute defines the type of the memory device.
MemoryDeviceFormFactor	nvarchar	256	Yes	This attribute defines the form factor of the memory device.
MemoryDeviceSize	int	4	Yes	This attribute defines the size of the memory device.
MemoryDeviceFailureMode	nvarchar	256	Yes	This attribute defines the failure mode of the memory device.
NIC Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
NICId*	int	4	No	The unique instance ID of the NIC.
NICIPAddress	nvarchar	40	Yes	The IP address assigned to the NIC.
NICNetmask	nvarchar	40	Yes	The subnet mask assigned to the NIC.
NICMACAddress	nvarchar	24	Yes	The MAC address of the NIC.
NICManufacturer	nvarchar	256	Yes	The reseller of the NIC.
NICPingable	int	4	Yes	A flag indicating that IT Assistant communicates with the device using this IP address.
Operating System Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
OSId*	int	4	No	The instance ID for the operating system.
OSName	nvarchar	64	Yes	The name of the operating system.
OSRevision	nvarchar	64	Yes	The revision of the operating system (for example, the Microsoft Windows® service pack or the Linux kernel version)

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
OSTotalPhysicalMemory	int	4	Yes	The total physical memory reported by the operating system in megabytes.
OSLocale	nvarchar	64	Yes	The locale for the operating system.
OSType	int	4	Yes	The type of operating system.
PowerSupply Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
PowerSupplyChassisIndex*	int	4	No	This attribute defines the index (one based) of the chassis.
PowerSupplyIndex*	int	4	No	This attribute defines the index (one based) of the power supply.
PowerSupplyType	nvarchar	256	Yes	This attribute defines the type of the power supply.
PowerSupplyLocation	nvarchar	256	Yes	This attribute defines the location of the power supply.
PowerSupplyOutputWatts	int	4	Yes	This attribute defines the maximum sustained output wattage of the power supply, in tenths of watts.
Processor Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ProcessorChassisIndex*	int	4	No	This attribute defines the index (one based) of the chassis.
ProcessorIndex*	int	4	No	This attribute defines the index (one based) of the processor.
ProcessorFamily	nvarchar	256	Yes	This attribute defines the family of the processor device.
ProcessorCurrentSpeed	int	4	Yes	This attribute defines the current speed of the processor device in MHz. Zero indicates that the current speed is unknown.
ProcessorSlotNumber	int	4	Yes	This attribute defines the slot that the processor occupies.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
SMBIOS Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ParallelPortConfiguration	nvarchar	64	Yes	Defines the parallel port configuration.
ParallelPortMode	nvarchar	64	Yes	The mode of the parallel port.
SerialPortYesConfiguration	nvarchar	64	Yes	Defines the serial port 1 configuration.
SerialPort2Configuration	nvarchar	64	Yes	Defines the serial port 2 configuration.
IDEController	nvarchar	64	Yes	Defines whether the IDE controller is enabled or disabled.
BuiltinNIC	nvarchar	64	Yes	Defines whether the built-in NIC is enabled or disabled.
BuiltinFloppy	nvarchar	64	Yes	Defines whether the built-in floppy disk controller is enabled, auto, or read-only.
BuiltinPointingDevice	nvarchar	64	Yes	Defines whether the built-in pointing device (mouse) port is enabled or disabled.
WakeupOnLAN	nvarchar	64	Yes	Defines whether Wake-On-LAN is disabled, enabled for on-board NIC only, or enabled for add-in NIC only. If **Enabled with boot to NIC** option is selected, the system boots from the NIC boot-ROM upon a remote wake up.
WakeupOnLANMethod	nvarchar	64	Yes	Defines the Wake-On-LAN method supported by the system.
AutoOn	nvarchar	64	Yes	Defines the auto-on configuration: disabled, every day or week days (Monday-Friday).
AutoOnHour	nvarchar	64	Yes	Defines the hour when the system is turned on (0-23).
AutoOnMinute	nvarchar	64	Yes	Defines the minutes when the system is turned on (0-59).
BootSequence	nvarchar	64	Yes	Defines the boot sequence for the next system boot.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
ChassisIntrusionStatus	nvarchar	64	Yes	Reports the status of the system with regard to **Chassis Intrusion** (**Detected** or Not **Detected**). A value of **Unknown** indicates either that chassis intrusion is not supported by this system, or that the chassis intrusion event reporting has been disabled by the user. If the value is **Detected**, you may set it to **Not Detected** to enable the system to receive the next event and to stop generating events for now.
IntegratedAudio	nvarchar	64	Yes	The status of the system's built-in sound device.
PCISlots	nvarchar	64	Yes	The status of the system's add-on PCI slots (enabled/disabled).
USBPorts	nvarchar	64	Yes	The status of the USB ports (on/off).
SoftwareInventory Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ComponentId	nvarchar	64	Yes	The component identifier for the software.
InstanceId*	nvarchar	32	No	The instance identifier for the hardware.
HWDeviceId	nvarchar	16	Yes	The hardware device identifier of the PCI ID.
HWVendorId	nvarchar	16	Yes	The hardware vendor identifier of the PCI ID.
HWSubDeviceId	nvarchar	16	Yes	The hardware subdevice identifier of the PCI ID.
HWSubVendorId	nvarchar	16	Yes	The hardware subvendor identifier of the PCI ID.
SubComponentId	nvarchar	64	Yes	The subcomponent identifier for the hardware.
HWDescription	nvarchar	128	Yes	The description of the hardware.
SoftwareType	nvarchar	64	Yes	The type of software, for example, driver (DRVR), firmware (FRMW), and so on.
SoftwareVersion	nvarchar	64	Yes	The software version number.
SoftwareDescription	nvarchar	128	Yes	The description of the software.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
SoftwareInventoryOS Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
OSVendor	nvarchar	64	Yes	The operating system vendor name.
OSMajorVersion	nvarchar	16	Yes	The major version of the operating system.
OSMinorVersion	nvarchar	16	Yes	The minor version of the operating system.
OSSPMajorVersion	nvarchar	16	Yes	The Service Pack major version.
OSSPMinorVersion	nvarchar	16	Yes	The Service Pack minor version.
SwitchDevice Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
SwitchIndex*	int	4	No	The index of the switch.
SwitchAssetTag	nvarchar	255	Yes	The asset tag of the switch.
SwitchServiceTag	nvarchar	255	Yes	The service tag of the switch.
SwitchSerialNumber	nvarchar	255	Yes	The serial number of the switch.
CostOfOwnership Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
CooIndex*	int	4	No	The index of the cost of ownership.
PurchaseCost	nvarchar	64	Yes	The initial purchase cost of the system.
WayBillNumber	nvarchar	64	Yes	The way bill number.
InstallationDate	nvarchar	64	Yes	The date that the system was installed.
PurchaseOrderNumber	nvarchar	64	Yes	The purchase order number.
PurchaseDate	nvarchar	64	Yes	The date that the system was purchased.
SigningAuthorityName	nvarchar	64	Yes	The signing authority reference.
OriginalMachineConfigurationExpensed	nvarchar	64	Yes	The original system configuration that was expensed.
OriginalMachineConfigurationVendorName	nvarchar	64	Yes	The original system configuration vendor name.
CostCenterInformationVendorName	nvarchar	64	Yes	The cost center information vendor name.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
UserInformationUserName	nvarchar	64	Yes	The user name.
ExtendedWarrantyStartDate	nvarchar	64	Yes	The extended warranty start date.
ExtendedWarrantyEndDate	nvarchar	64	Yes	The extended warranty end date.
ExtendedWarrantyCost	nvarchar	64	Yes	The extended warranty cost.
ExtendedWarrantyProviderName	nvarchar	64	Yes	The extended warranty provider name.
OwnershipCode	nvarchar	64	Yes	The ownership code.
CorporateOwnerName	nvarchar	64	Yes	The owner’s name.
HazardousWasteCodeName	nvarchar	64	Yes	The hazardous waste code name.
DeploymentDateLength	nvarchar	64	Yes	The deployment date length.
DeploymentDurationUnitType	nvarchar	64	Yes	The deployment duration unit type.
TrainingName	nvarchar	64	Yes	The training name.
OutsourcingProblemDescription	nvarchar	64	Yes	The outsourcing problem description.
OutsourcingServiceFee	nvarchar	64	Yes	The outsourcing service fee.
OutsourcingSigningAuthority	nvarchar	64	Yes	The outsourcing signing authority.
OutsourcingProviderFee	nvarchar	64	Yes	The outsourcing provider fee.
OutsourcingProviderServiceLevel	nvarchar	64	Yes	The outsourcing provider service level.
InsuranceCompanyName	nvarchar	64	Yes	The insurance company’s name.
BoxAssetTagName	nvarchar	64	Yes	The device’s asset tag.
BoxSystemName	nvarchar	64	Yes	The device’s host name.
BoxCPUSerialNumberName	nvarchar	64	Yes	The device’s CPU serial number.
DepreciationDuration	nvarchar	64	Yes	The depreciation duration.
DepreciationDurationUnitType	nvarchar	64	Yes	The depreciation duration units.
DepreciationPercentage	nvarchar	64	Yes	The depreciation percentage.
DepreciationMethod	nvarchar	64	Yes	The depreciation method.
RegistrationIsRegistered	nvarchar	64	Yes	The registration is registered.
ContactInfo Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ContactName*	nvarchar	64	No	The contact name.
ContactInformation	nvarchar	64	Yes	The information for this contact.
ContactDescription	nvarchar	64	Yes	The description for this contact.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
Cluster Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
ClusterIndex*	int	4	No	The cluster index.
ClusterType	int	4	Yes	The cluster type.
ClusterTypeName	nvarchar	64	Yes	The cluster type name.
ClusterName	nvarchar	255	Yes	The cluster name.
ClusterDescription	nvarchar	255	Yes	The cluster description.
FRU Information Table				
DeviceId*	int	4	No	The device ID.
FRUChassisindex*	int	4	No	The field replaceable unit (FRU) chassis index.
FRUIndex*	int	4	No	The FRU index.
FRUDeviceName	nvarchar	255	Yes	The FRU device name.
FRUManufacturer	nvarchar	255	Yes	The FRU manufacturer name.
FRUSerialNumber	nvarchar	255	Yes	The FRU serial number.
FRUPartNumber	nvarchar	255	Yes	The FRU part number.
FRURevision	nvarchar	255	Yes	The FRU revision number.
FRUManufacturingDate	date	8	Yes	The FRU manufacturing date.
Printer Supply Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
PrinterSupplyIndex*	int	4	No	The printer supply index.
PrinterSupplyDescription	nvarchar	64	Yes	The printer supply description.
PrinterSupplyLevel	nvarchar	16	Yes	The printer supply level.
PrinterSupplyMaxLevel	int	4	Yes	The maximum level of printer supply.
PrinterSupplyType	nvarchar	64	Yes	The printer supply type.
Printer Input Tray Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
PrinterInputTrayIndex*	int	4	No	The printer input tray index.
PrinterInputName	nvarchar	64	Yes	Name of the printer input.
PrinterInputVendorName	nvarchar	64	Yes	Name of the printer (re)seller.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
PrinterInputModel	nvarchar	64	Yes	Name of the input tray model.
PrinterInputDescription	nvarchar	64	Yes	The printer input description.
PrinterInputMaxCapacity	nvarchar	64	Yes	The maximum capacity of the printer input module.
PrinterInputCurrentCapacity	nvarchar	64	Yes	The current capacity of the printer input module.
PrinterInputMediaType	nvarchar	64	Yes	The media type.
Printer Output Tray Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
PrinterOutputIndex*	int	4	No	The printer output index.
PrinterOutputName	nvarchar	64	Yes	Name of the output unit.
PrinterOutputVendorName	nvarchar	64	Yes	Name of the printer (re)seller.
PrinterOutputModel	nvarchar	64	Yes	Name of the output tray model.
PrinterOutputDescription	nvarchar	64	Yes	The printer output description.
PrinterOutputMaxCapacity	nvarchar	64	Yes	The maximum output capacity of the printer.
Printer Cover Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
PrinterCoverIndex*	int	4	No	The printer cover index.
PrinterCoverDescription	nvarchar	64	Yes	The printer cover description.
PrinterCoverStatus	nvarchar	64	Yes	The printer cover status.
Tape Drive Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
TapeDriveIndex*	int	4	No	The tape drive index.
TapeDriveVendor	nvarchar	64	Yes	Name of the tape drive vendor.
TapeDriveModel	nvarchar	64	Yes	Name of the tape drive model.
TapeDriveType	nvarchar	64	Yes	The tape drive type.
TapeDriveFirmwareVersion	nvarchar	32	Yes	Firmware version of the tape drive.
TapeDriveSerialNumber	nvarchar	32	Yes	Serial number of the tape drive.
TapeDriveWMN	nvarchar	32	Yes	WMN for the tape drive.

Table 9-2. IT Assistant Database Schema *(continued)*

Column Name	Data Type	Data Size	Nulls Allowed	Description
TapeDriveCleaningRequired	nvarchar	32	Yes	Specifies whether the tape drive requires cleaning.
TapeLibraryScsiId	int			Specifies the SCSI ID of the Tape library
Tape Library Table				
DeviceId*	int	4	No	The Foreign Key to the Device Table.
TapeLibraryIndex*	int	4	No	The tape library index.
TapeLibraryVendor	nvarchar	64	Yes	Name of the tape library vendor.
TapeLibraryModel	nvarchar	64	Yes	Name of the tape library model.
TapeLibraryFirmwareVersion	nvarchar	32	Yes	Firmware version of the tape library.
TapeLibraryDriveCount	int	4	Yes	The number of drives.
TapeLibrarySlotCount	int	4	Yes	The number of slots.
TapeLibrarySerialNumber	nvarchar	32	Yes	Serial number of the tape library.

Managing Tasks

IT Assistant also allows you to remotely run certain tasks on managed systems across the enterprise remotely. These tasks include:

- Generic command line execution (the ability to invoke the Dell OpenManage Server Administrator command line interface remotely is also supported if Dell OpenManage 4.3 or later instrumentation is enabled)
- Device control, including shutdown and wake up
- Scheduled software updates
- Ability to execute Intelligent Platform Management Interface (IPMI) commands remotely
- Ability to execute Remote Client Instrumentation commands remotely
- Ability to deploy the Dell agent (Server Administrator) on systems

NOTE: IPMI and Remote Client Instrumentation command line options may not be available if IT Assistant does not detect the necessary components installed on the IT Assistant Services Tier.

These tasks can be configured to run on specific schedules or execute immediately. For more information, see the *Dell OpenManage IT Assistant Online Help*.

Creating a Device Control Task

For instance, Jane wants to power control a system through IT Assistant. To perform these tasks in IT Assistant, she would:

1. Select **Manage→Tasks** and right-click **Device Control** in the left navigation pane.
2. Select **New Task**.

   The Task Creation wizard appears.
3. Jane enters a **Task Name**, then chooses **Shutdown Device** from the **Task Type** pull-down menu and clicks **Next**.
4. From the **Select Shutdown Type** window, she chooses:

   a. **Reboot** to reboot a troublesome server that has issued several e-mail alerts

   b. **Power Cycle (if supported)**. This option performs a power cycle when IT Assistant communicates to the system through Dell instrumentation using the SNMP. The power to the device is turned off and turned on again. When the power is restored, the device is restarted.

   c. **Power On** to power on an ASF-enabled device.

   d. **Power Off** to power down the system.

   e. **Shutdown Operating System first**. This option performs a graceful shutdown of the operating system before performing the selected shutdown action.

   NOTE: **Shutdown Operating System first** will not display for ASF-enabled devices.
5. In the **Select Devices** window, she expands the **Servers** device list and selects only the server that she wants to reboot.
6. In **Select Schedule**, she chooses **Run Now**.
7. If she is rebooting an SNMP-enabled system, she must enter the instrumentation user name and password in the **Enter Credentials** window. If her system is CIM-enabled, she must enter the fully qualified domain user name and password.
8. In the **Summary** window, she either confirms her selections or chooses **Back** to make changes.

   The server she specified will begin a reboot immediately after she selects **Finish**.

   Alternately, Jane could choose to power up a device in her group by choosing **Wake Up Device** as the **Task Type** in the **Task Creation** wizard. She could also schedule the task to run at a specified time instead of immediately.

Other Tasks Available in IT Assistant

Other task types available in IT Assistant include:

Generic Command Line

Choosing **Generic Command Line** from the pull-down menu allows you to execute commands from within your network. **Remote Server Administrator Command Line** allows you to execute Server Administrator command line interface (CLI) commands remotely.

For a full list of the arguments accepted by IT Assistant, see the online help.

Software Update

Choosing **Server Software Upgrade** allows you to fully customize the software upgrade process on your managed systems, including defining separate schedules for each component of the upgrade.

For a complete explanation of each task and its function, see the *Dell OpenManage IT Assistant Online Help*.

IPMI Command Line

Choosing **IPMI Command Line** from the pull-down menu allows you to execute IPMI commands.

For additional information, see the online help.

Remote Client Instrumentation Command Line

Choosing **Remote Client Instrumentation Command Line** allows you to execute client instrumentation commands remotely.

For additional information, see the online help.

Server Administrator Software Deployment

Choosing **Software Deployment** under the **Task** parent node allows you to deploy the Dell agent on multiple systems.

For additional information, see "Using Server Software Deployment."

Shutdown Device(via in-band)

Choosing **Shutdown Device(via in-band)** allows you to specifiy the shutdown operation that you want to perform.

NOTE: This task requires CIM or SNMP discovery to be enabled, or Server Administrator to be installed on the managed node.

NOTE: The shutdown task is not supported for devices discovered using IPMI only.

Wake Up Device(via WakeOnLAN)

Choosing **Wake Up Device(via WakeOnLAN)** allows you to specify the port number of the device that you want to wake up. To wake up a device, IT Assistant uses the MAC addresses and subnet mask that were discovered for that device. If NIC teaming is configured on the device, only one MAC is advertised by the operating system. For Wake-on-LAN (WOL) to work, WOL must be enabled for all NICs in that team. For a WOL packet to reach its intended destination, directed broadcasting (also known as subnet broadcasting) must be enabled on the intermediate routers. Directed broadcasting is typically disabled on the routers, so you must configure this feature on the routers to enable it.

NOTE: Enable the WOL property in the NIC settings and the system BIOS.

Power Control Device(via ASF)

Choosing **Power Control Device(via ASF)** allows you to perform remote power control operations on the Alert Standard Format (ASF) 2.0 compliant devices.

NOTE: See the system documentation for ASF configuration and setup instructions.

NOTE: IT Assistant uses the in-band Broadcom Windows Management Instrumentation (WMI) provider to verify if a device has ASF capabilities.

IT Assistant also uses the in-band Broadcom WMI provider to detect if a device is enabled for remote secure Remote Management Control Packets (RMCP) operations and whether the administrator roles have sufficient privileges to perform power control operations.

NOTE: You can configure the power control operations through the Broadcom ASF Configuration Utility.

NOTE: Verify that **ASF Enabled**, **Remote Management**, and **Secure Management(ASF 2.0)** options are enabled in the Broadcom ASF Configuration Utility. Also ensure that the Authentication Key and the KG Key are entered in the correct format (Hex or ASCII).

The WMI provider is available as part of the Broadcom ASF Management suite—available on the Dell Support website at **support.dell.com**—and must be installed on the remote client device.

You can select the devices that are detected as being enabled, in the device selection pane of the ASF power control wizard. If the remote device does not have the WMI provider installed, is not enabled for remote secure RMCP operations, or if the administrator privileges have not been configured for the power control operation correctly, the device will appear disabled in IT Assistant.

NOTE: You can select the disabled devices, if you select the **Enable All** option.

If the settings are altered, rediscover the device to enable IT Assistant to use the updated configuration to enable/disable the client devices in the wizard.

10

Ensuring a Secure Dell OpenManage™ IT Assistant Installation

This section discusses several specific topics useful in implementing a more secure Dell OpenManage IT Assistant installation. IT Assistant leverages HTTPS for secure communications, as well as the Microsoft® Active Directory® for role-based access.

For detailed information on security across the Dell OpenManage platform, including IT Assistant, see the *Dell OpenManage Installation and Security User's Guide*.

TCP/IP Packet Port Security

A TCP/IP packet communicates a request to a target system. Encoded within this packet is a port number that is associated with a specific application. IT Assistant is accessed by specifying `https://<hostname>:<portnumber>`. Using `https` requires the application being used to encrypt the data according to the Secure Socket Layer (SSL) specification so that it is not possible for an observer to pick up and read sensitive information such as passwords by watching packets on the network. User are then authenticated through the IT Assistant login page and their credentials checked against whatever role is mapped in Active Directory or the local operating system. For information on the three roles supported by IT Assistant, see "Role-Based Access Security Management."

NOTE: The IT Assistant user interface communicates with the IT Services Tier over port 2607.

Securing Managed Desktops, Laptops, and Workstations

Securing the Managed System's Operating System

The first step in promoting a secure network environment is to ensure that all managed system operating systems are running the most current service pack and/or any additional critical security hotfixes. To simplify this process, Microsoft has introduced Software Update Services. See the Microsoft website for more details. Perform similar updates for other managed systems' operating systems as well.

Session Time-out

An IT Assistant UI session can be configured to time-out after a defined period of inactivity. To configure the session time-out interval, click **Preferences** on the top IT Assistant navigation bar and choose **Web Server Properties**. You can either disable session time-out altogether, or allow for up to 30 minutes of inactivity.

NOTE: If the data communication channel between the IT Assistant user interface and the Web server is active due to any asynchronous updates such as performance monitoring tasks, discovery of devices, status polling, and so on, the user session will not time-out even if session time-out is enabled.

ASF and the SNMP Protocol

A final security consideration, starting with Dell™ OptiPlex™ GX260 systems, is the support for the Alert Standard Format (ASF) for integrated Network Interface Controller (NIC). ASF issues Platform Event Traps (PET) corresponding to system health and security issues. Since these traps are supported by the SNMP protocol, the managed system NIC must be configured with the IP address and community string of the management station running IT Assistant.

In summary, to successfully and securely manage desktops, laptops, and workstations per the security measures introduced in the paragraphs above, system administrators should adhere to the following best practices:

- Ensure that the operating system is up-to-date with the most recent operating system security patches.
- For ASF-capable desktops, either disable ASF or implement SNMP community names that cannot be easily guessed.

Securing Managed Server Systems

Securing the Managed System's Operating System

As with desktops and workstations, the first step in securing a server is to ensure that it is running with the most current service pack and appropriate critical hot fixes installed. Microsoft Software Update Services, mentioned in the previous section, also applies to Microsoft Windows® 2000 and Windows Server® 2003 servers. Similar services should be checked for Red Hat® Linux and SUSE® Linux Enterprise Server.

Choosing the Most Secure Managed System Server Protocol

Dell OpenManage Server Administrator, the current Dell server instrumentation software, uses the SNMP and CIM protocols, which can be configured during a custom install.

CIM Monitoring, DCOM, and Windows Authentication

The CIM protocol, which uses DCOM security, leverages Windows challenge/response (user name/password) authentication. In addition, communication with the managed system is established through the domain/user name/password accounts specified in each of the configured IT Assistant discovery ranges. The format for these accounts is **<domain name>\<user name>** or **localhost\<user name>**.

NOTE: WMI security can be changed with utilities such as **dcomcnfg.exe**, **wmimgmt.msc**, and **wbemcntl**. However, due to the potential for undesired side effects, implementing changes through these methods is not recommended. See the Microsoft website for more information.

NOTE: Even in environments that intend to use only CIM for monitoring, SNMP is typically enabled because Server Administrator only provides error notification using SNMP traps.

Security and the SNMP Protocol

There are several actions that can be taken to better secure environments using the SNMP protocol. Although the following samples refer to Microsoft Windows operating systems, similar steps can be performed for the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems. By default, when SNMP is installed, the community name is set to **public**. This character string should be treated like a password and similar rules should be used in its selection—a string of adequate length, not easily guessed, and preferably consisting of mixed letters and numbers. In Windows operating systems, the SNMP community name can be configured through the **Security** tab of the SNMP services **Property** dialog box.

As a secondary precaution, SNMP should also be set to **Read Only** to prevent unauthorized configuration and control actions. This can also be enforced by using **snmpsets=no option** when installing Server Administrator. It would still be possible to make those changes through the user interface or Command Line Interface (CLI) of Server Administrator. In addition, it is also possible to configure the SNMP service to accept requests only from a particular server (in this case, the system running IT Assistant). This too can be configured on the Windows **Security** tab referenced previously by selecting the radio button labeled **Accept SNMP packets from these hosts** and then clicking **Add** to enter the IP address or name of the system running IT Assistant. See your operating system documentation for more details.

NOTE: To ensure that all the systems are properly configured, it is recommended that you use tools such as Group Policies in Active Directory to enforce these SNMP settings.

As a final security step, Server Administrator should be configured to deny access to user and possibly power user accounts, thereby limiting access to administrator accounts only. This can be done through the Server Administrator top navigation bar by selecting **Preference** and then unchecking the **User Access** boxes.

NOTE: You can also limit user access using the Server Administrator CLI command **omconfig preferences useraccess enable=admin**.

See the *Dell OpenManage Server Administrator Command Line Interface User's Guide* on the Dell Support website at **support.dell.com** or on the documentation CD for more information.

In summary, to successfully and securely manage servers per the security measures introduced here, system administrators should adhere to the following best practices:

- Ensure that the operating system is up-to-date with the most recent operating system security patches.
- Implement SNMP community names that cannot be easily guessed.
- Configure SNMP to be **Read Only** to limit configuration, update, and power control to Server Administrator only.
- Configure SNMP to accept requests only from the IP address of the system running IT Assistant.
- Use tools such as Group Policies in Active Directory to enforce the SNMP settings for all servers to be managed.
- Configure Server Administrator to deny user level access.

Ensuring Database Security When Using IT Assistant

If no Microsoft SQL Server database is detected when IT Assistant is installed, the process installs a copy of SQL Server 2005 Express, which is set to an authentication mode of trusted or Windows only. However, other applications that may have previously installed MSDE or SQL Server, including previous versions of IT Assistant, frequently chose either an authentication mode of SQL or mixed mode, which allows SQL Server to manage its own user IDs and passwords. In the case of early versions of IT Assistant, the supervisor account password was set to either `null` or `dell`. At a minimum, decrease the exposure to a network break-in by changing these passwords to strings that correspond to the best practices mentioned previously. A better option is to change the database authentication mode to trusted or Windows only.

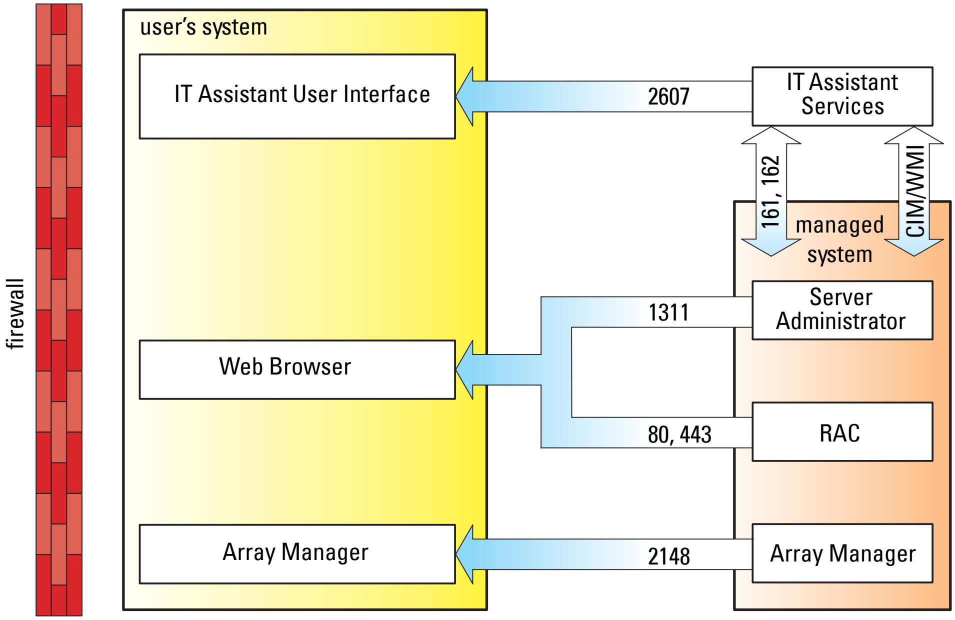
Running IT Assistant Behind a Firewall

Figure 10-1 illustrates a typical installation in which both IT Assistant and the systems being managed reside behind a firewall. The firewall denies passage to traffic on specified ports between the protected network and the rest of the world while still allowing an administrator to communicate freely with both IT Assistant and the managed system.

Typical security for the system running IT Assistant in an environment behind a firewall includes the following:

- Use trusted accounts instead of named or mixed for the database.
- Limit user interface connections to a known system.

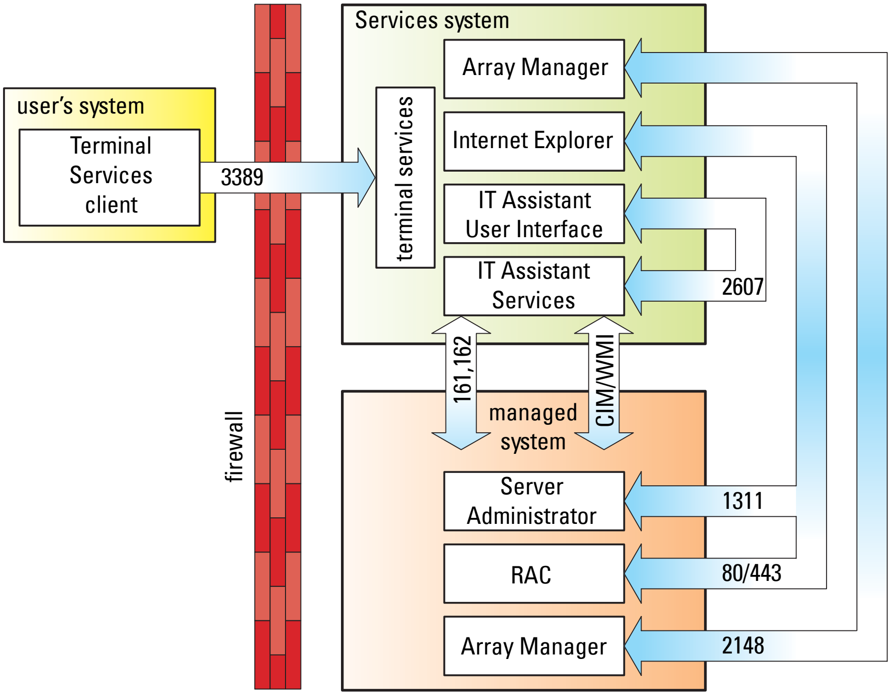
Figure 10-1. Typical Installation Behind a Firewall



Setting Up Additional Security for IT Assistant Access

So far in this section, security has been addressed with respect to the existing TCP/IP connection between IT Assistant and the managed system. In addition to these security precautions, Microsoft Terminal Services, which allows uncharted remote connection only by users with administrator accounts (administrative mode), can also be used to limit user interface connections to a system running IT Assistant user interface and Services. An example of a network which leverages Terminal Services is shown in Figure 10-2.

Figure 10-2. Using Terminal Services for Additional Security



In Figure 10-2, a user may connect to the IT Assistant management station through a locally installed Terminal Services client or Windows XP Remote Desktop connection. This connection requires a valid domain/user ID/password. See Microsoft's website for more information.

The additional level of security is derived by setting up restrictions on all managed systems to only accept SNMP traffic from the IP address of the system running the IT Assistant user interface ([UI] the network management station). Terminal Services and Remote Desktop sessions emulate traffic coming directly from the network management station; therefore, access to IT Assistant is restricted only to Terminal Services clients or a local network management station user. Any other connection, such as another remote IT Assistant UI installation, would be unable to effectively communicate with properly configured managed systems in the network since traffic identified as originating from a system other than the network management station would be refused.

NOTE: Terminal Services is an optional component of Microsoft Windows 2000 and Microsoft Windows Server 2003 that can be installed in either admin or application mode.

NOTE: When Terminal Services is installed in administrative mode, up to two users can log in as long as they are members of the administrators group. When Terminal Services is installed in application mode, non-administrator groups can log in and more than two sessions are supported. However, application mode installation has additional licensing implications. When installing IT Assistant on a system running Terminal Services in application mode, the installation must be performed locally and not through a terminal session.

Securing Ports for IT Assistant and Other Supported Dell OpenManage Applications

Securing port 2607 of the IT Assistant Services Tier and ports 1311, 623, 161, and 162 of the managed system can be done using IP Security (IPSec). To list ports that are currently running on your server, you can use the command **netstat -an** from a command prompt to show the status of all ports on your system. The results of this command should indicate that the IT Assistant management station should only accept a connection on port 2607 from the server hosting the IT Assistant UI (which would be connected through Terminal Services). Similarly, the managed systems should be configured to accept connections through ports 1311, 161, and 162 from the management station.

Single Sign-On

The Single Sign-On option on Windows systems enables all logged-in users to bypass the login page and access IT Assistant by clicking the **IT Assistant** icon on the desktop. The desktop icon queries the registry to see if the **Automatic Logon with current username and password** option is enabled in Internet Explorer. If this option is enabled, then Single Sign-On is executed; otherwise, the normal login page will be displayed. NT LAN Manager (NTLM) authentication must not be disabled on the Windows network.

To enable the **Automatic Logon with current username and password** option, perform the following steps in Internet Explorer:

1. Click **Internet Options** on the **Tools** menu.
2. Click the **Security** tab
3. Select the security zone that the IT Assistant system falls within, that is, **Trusted sites** and click **Custom Level**.
4. In the **Security Setting** dialog-box, under **User Authentication**, select the **Automatic Logon with current username and password**.
5. Click **OK** twice, and restart Internet Explorer.

For local system access, you must have an account on the system with the correct privileges (User, Power User, or Administrator). Other users are authenticated against Microsoft Active Directory.

To launch IT Assistant using Single Sign-on authentication against Microsoft Active Directory, the following parameters must be set:

```
authType=ntlm&application=[ita]
```

For example:

```
https://localhost:2607/?authType=ntlm&application=ita
```

To launch IT Assistant using Single Sign-on authentication against the local system user accounts, the following parameters must be set:

```
    authType=ntlm&application=[ita]&locallogin=true
```

For example:

```
https://localhost:2607/?authType=ntlm&application=ita&locallogin=true
```

Role-Based Access Security Management

IT Assistant provides security through role-based access control (RBAC), authentication, and encryption.

Role-Based Access Control

RBAC manages security by determining the operations that can be executed by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more user privileges that are permitted to users in that role. With RBAC, security administration corresponds closely to an organization's structure.

User Privileges

IT Assistant grants different access rights based on the user's assigned group privileges. The three user levels are: User, Power User, and Administrator.

Users have read-only access to all IT Assistant information.

Power Users can create tasks for immediate execution. They cannot modify discovery configuration settings, modify alert management settings, or schedule or delete tasks.

Administrators can perform all IT Assistant tasks and functions.

Microsoft Windows Authentication

For supported Windows operating systems, IT Assistant authentication is based on the operating system's user authentication system using Windows NT® LAN Manager (NTLM) modules to authenticate. This underlying authentication system allows IT Assistant security to be incorporated in an overall security scheme for your network.

Assigning User Privileges

You do not have to assign user privileges to IT Assistant users before installing IT Assistant.

The following procedures provide step-by-step instructions for creating IT Assistant users and assigning user privileges for Windows operating system:

NOTICE: You should disable guest accounts for supported Microsoft Windows operating systems in order to protect access to your critical system components. See "Disabling Guest and Anonymous Accounts" for instructions.

Creating IT Assistant Users for Supported Windows Operating Systems

NOTE: You must be logged in with Admin privileges to perform these procedures.

Creating Users and Assigning User Privileges for Supported Windows 2000 and Windows Server® 2003 Operating Systems

NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

1 Click the **Start** button, right-click **My Computer,** and point to **Manage**.

2 In the console tree, expand **Local Users and Groups**, and then click **Users**.

3 Click **Action**, and then click **New User**.

4 Type the appropriate information in the dialog box, select or clear the appropriate check boxes, and then click **Create**.

NOTICE: You must assign a password to every user account that can access IT Assistant to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log in to IT Assistant on a system running Windows Server 2003 due to operating system constraints.

NOTE: Do not use double or single quotes in passwords.

5 In the console tree, under **Local Users and Groups**, click **Groups**.

6 Click the group to which you want to add the new user: **Users**, **Power Users**, or **Administrators**.

7 Click **Action**, and then click **Properties**.

8 Click **Add**.

9 Type the user name that you are adding and click **Check Names** to validate.

10 Click **OK**.

New users can log in to IT Assistant with the user privileges for their assigned group.

Adding Users to a Domain

NOTE: For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

NOTE: You must have Active Directory installed on your system to perform the following procedures.

1. Click the **Start** button, and then point to **Control Panel→Administrative Tools→Active Directory Users and Computers**.
2. In the console tree, right-click **Users** or right-click the container in which you want to add the new user, and then point to **New→User**.
3. Type the appropriate user name information in the dialog box, and then click **Next**.

   NOTICE: You must assign a password to every user account that can access IT Assistant to protect access to your critical system components. Additionally, users who do not have an assigned password cannot log into IT Assistant on a system running Windows Server 2003 due to operating system constraints.

   NOTE: Do not use double or single quotes in passwords.
4. Click **Next**, and then click **Finish**.
5. Double-click the icon representing the user you just created.
6. Click the **Member of** tab.
7. Click **Add**.
8. Select the appropriate group and click **Add**.
9. Click **OK**, and then click **OK** again.

   New users can log in to IT Assistant with the user privileges for their assigned group and domain.

Disabling Guest and Anonymous Accounts

NOTE: You must be logged in with Administrator privileges to perform this procedure.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer,** and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.
2. In the console tree, expand **Local Users and Groups** and click **Users**.
3. Click the **Guest** or **IUSR_*system name*** user account.
4. Click **Action** and point to **Properties**.
5. Select **Account is disabled** and click **OK**.

   A red circle with an X appears over the user name. The account is disabled.

Frequently Asked Questions

Top IT Assistant Questions

The following table lists frequently asked questions and answers.

Question	Answer
What User Datagram Protocol (UDP)/Transmission Control Protocol (TCP) ports does IT Assistant use?	See "Ports Used by IT Assistant and Associated Agent Application" in the *Dell OpenManage Security and Installation Guide*.
I just did a system update; why don't I see the updated version in the IT Assistant inventory?	All the data that IT Assistant displays in the system list is stored in the data repository, which is refreshed during each inventory cycle. If you perform an update, IT Assistant reports that change after the next inventory cycle. To refresh the inventory of the device before the next scheduled inventory cycle, right-click the device with the outdated version in the **Device Tree** view and click **Refresh Inventory**. **NOTE:** It may take several minutes for the inventory to display the updated version, so it is recommended that you wait 5 - 10 minutes before requesting an inventory of the device.
I just shut down a system. Why does IT Assistant still show it as awake?	IT Assistant updates a system's up/down status only during a status poll of the system, during a discovery of the system, or when IT Assistant receives an event from the system.
Why can't I see a status update for a device on the IT Assistant user interface (UI)?	If IT Assistant detects that the global status of a device has NOT changed on a scheduled status poll, then it will not send a message to the UI. Also, IT Assistant will not send a message to the UI when it checks the status after an incoming event for that device. This behavior is to optimally use resources and to increase the processing speed of the other messages that are sent to the user. If you are inspecting the device summary or device details at that very moment, the information about the last status time or the individual agent status will not be automatically refreshed. Refresh the view or click another device to automatically load the latest information from the database.

Question	Answer
How do I know when IT Assistant is finished discovering systems?	IT Assistant provides discovery cycle progress information. In the IT Assistant UI, go to **Discovery and Monitoring→ Logs**. See also "Discovery and Monitoring Logs—Resolving Discovery Issues" in the *Dell OpenManage IT Assistant Online Help*.
I received a message stating that IT Assistant can't communicate with the remote device. What caused this problem?	IT Assistant was unable to connect to the remote agent or device. Use the Troubleshooting Tool to resolve the issue by running Ping, CIM, and SNMP Connectivity tests and the Name Resolution test. In the IT Assistant UI, go to **Tools→Troubleshooting Tool**. See "Troubleshooting Tools—Finding and Resolving Discovery Issues" in the *Dell OpenManage IT Assistant Online Help*.
Why do I get an error message when launching applications from the right-click **Device Tree**?	Certain applications (for example, Dell OpenManage Server Administrator Storage Management Services and Digital KVM Console) must be installed on the system running the IT Assistant UI before they can be launched from IT Assistant.
Why do I get a Java out of memory exception?	When managing an environment with more than 2000 devices, increase the amount of memory allocated to the Java Runtime Environment (JRE) heap. **NOTE:** The memory should be increased on the system from where you access the IT Assistant Management Station. To do so, close the IT Assistant browser session and go to the Java **Control Panel**. The panel is located under the Microsoft® Windows® **Control Panel** or the **ControlPanel** executable in the **bin** folder of the JRE installation on the Linux system. Click the **Java** tab and in the Java Applet Runtime section, click **View...**. Click in the Java Runtime Parameters area and type: `-Xmx256M`
Why do I get a host name mismatch warning when I try to access the IT Assistant user interface?	This warning appears if the web address that you use to connect to IT Assistant contains a different host name than the one that was used to install IT Assistant. For example, if you installed IT Assistant using the host name **sysadmin3** with an IP address of **133.143.157.30**, the warning appears if you log in to IT Assistant using the IP address. However, if you log in to the remote device using the system name, **sysadmin3**, the warning does not appear.

Question	Answer
Why don’t I get a Login prompt when I login to IT Assistant from a desktop?	IT Assistant uses the operating-system credentials of the currently logged-in user and automatically logs you in to IT Assistant. See the section about Single Sign-On in the *IT Assistant User's Guide* for additional information.
Why does the Windows NT® LAN Manager (NTLM) authentication fail when I attempt to log in to IT Assistant?	Ensure that your Single Sign-On is enabled in your Internet Explorer browser. To enable Single Sign-On, launch Internet Explorer. Click **Tools→Internet Options→Security** tab. Select **Trusted sites**. (The IT Assistant system is covered within this security zone.) Click **Custom Level**. Scroll down to **User Authentication** and select **Automatic logon with current username and password**.
How do I disable Java caching?	To disable Java caching on a Windows system, go to the Windows **Control Panel**, click the **Java** icon to display the **Java Control Panel**, and ensure that the **Enable Caching** check box in the **Java Applet Cache Viewer** dialog box is not selected. To disable caching on a Linux system, run the **ControlPanel** executable in the **bin** folder of the JRE installation on the Linux system, and ensure that the **Enable Caching** check box in the **Java Applet Cache Viewer** dialog box is not selected.
What precautions do I need to take when I revert to an older version of IT Assistant?	If you have Java applet caching enabled on any of the systems where you have accessed the IT Assistant UI, then delete the jar files used by IT Assistant, from the cache of each of those systems. Go to **Java Control Panel** and click **Settings** under **Temporary Internet Files**. The panel is located under Microsoft Windows Control Panel or Linux **ControlPanel** in the **bin** folder. Click **View Applets**. Select the cached files and click **Delete**. **NOTE:** Failure to delete the Java applet cache may result in inconsistent behavior of the older version of IT Assistant.

Scope and Capabilities of IT Assistant

These frequently asked questions cover the general capabilities of IT Assistant, optimizing the UI environment, and discovery configuration.

Question	Answer
Why does IT Assistant show that my discovered system is down during a status poll when it is up?	For networks where Dynamic Host Configuration Protocol (DHCP) is prevalent, IT Assistant may show a system as down when it is actually up due to another system obtaining its IP Address. During a discovery round, when IT Assistant discovers a particular managed system, it looks for other systems in its database with the same IP address as the one under discovery. If any other system shares that address, its IP address is marked as invalid. When the system whose IP address was marked as invalid is eventually rediscovered, its IP address entries are updated and marked as valid again. Until these IP address entries are updated, any status poll that runs will mark that system as down due to not having any valid IP address entries to check against.
Why doesn't IT Assistant show my system as up after I changed the name?	When IT Assistant discovers a particular managed system through its IP address during a discovery round, IT Assistant attempts to resolve the managed system's address to a name, either through instrumentation or DNS. If DNS is the preferred name resolution method and the name of the managed system under discovery has recently changed, it may take several discovery rounds for the name to update in IT Assistant due to Windows caching DNS entries on the local system. For more information on how to clear the cache faster, see the Microsoft documentation for your operating system.
Why can't I discover my desktop system?	Use the IT Assistant Troubleshooting Tool to help resolve this issue. In the UI, go to **Tools→Troubleshooting Tool**. See "Troubleshooting Tool—Finding and Resolving Discovery Issues" in the *Dell OpenManage IT Assistant Online Help*.
Does IT Assistant manage only Dell systems?	Yes. IT Assistant only manages Dell systems that have Dell instrumentation installed and running. However, starting with IT Assistant 8.0, devices that are configured with IPMI 1.5 or later can also be discovered with IT Assistant.

Question	Answer
Do I have to install IT Assistant on a Dell system?	No. Although IT Assistant is tested for installation on Dell systems, the IT Assistant UI is designed to operate on a system running the supported operating systems. Therefore, IT Assistant should work without incident on non-Dell systems that run these operating systems and that meet the minimum hardware specifications. See "Planning Your Dell OpenManage™ IT Assistant Installation" for more details. However, Dell does not provide warranty or free support for non-Dell systems.
How many users can run IT Assistant at the same time?	Multiple users can run IT Assistant to connect to IT Assistant services. The number of users is limited by the resources available on the management station.
Can I install IT Assistant on top of Client Administrator?	Client Administrator is not currently a supported configuration on the same system as IT Assistant.
How many systems can I manage?	IT Assistant is designed and tested to *manage* up to several thousand systems on a suitably configured system. **NOTE:** CPU-intensive tasks like the performance monitoring can, however, be performed only on a hundred systems and software deployment can be attempted only on about 20 systems at a time.
Can I use IT Assistant over the Internet?	IT Assistant is a local area network (LAN)-oriented tool for monitoring and managing systems in an IP network. You can monitor and manage systems over the Internet using IT Assistant, but Dell does not recommend it unless you have a way of securing your data, which you must provide. IT Assistant does provide security suitable for use over a corporate intranet.

IT Assistant User Interface

Question	Answer
I know that the IT Assistant UI is set to automatically log me out after 30 minutes of being idle. So, why am I able to continue to change menus and views after being logged into IT Assistant after 30 minutes?	IT Assistant caches some data and validates the time-out only when gathering new data is required.
Why don't I see all the alerts on the **Alerts** tab?	The IT Assistant UI displays alerts in the **Alert Logs** view. You can specify that you want to view all alerts by selecting **All Alerts** in the **Filter** drop-down menu. See "Alert Logs—Working With Alerts" in the *Dell OpenManage IT Assistant Online Help*.

Question	Answer
Why is the power state for a system that I shut down not shown as shut down in IT Assistant?	The power state is dependent on the most recent status poll, which is dependent on the status polling interval. The power state will be updated when the next status poll occurs.
What do I do if a system does not wake up?	To wake up a device, IT Assistant uses the MAC addresses and subnet mask that were discovered for that device. If NIC teaming is configured on the device, only one MAC is advertised by the operating system. For Wake-on-LAN (WOL) to work, WOL must be enabled for all NICs in that team. For a WOL packet to reach its intended destination, directed broadcasting (also known as subnet broadcasting) must be enabled on the intermediate routers. Directed broadcasting is typically disabled on the routers, so you must configure this feature on the routers to enable it.
Why don't I see new alerts displayed in the **Alert Logs** view?	To see new alerts, click **Show New Alerts** in the **Alert Logs** window.
Why don't I see a detailed description of my network adapter manufacturer on the IT Assistant **Device Details Summary** page?	Due to the implementation of MIB2 on Red Hat Linux, the **Network** section of the IT Assistant **Device Details Summary** page does not have a detailed description of the network adapter manufacturer. For example, "eth0" or a similar string appears under **Product Name**.
Why is the IP address on the NIC information page displayed in a wrong row.	This issue has been fixed by a Red Hat patch to the net-snmp package.
When I export my report to CSV format, Excel doesn’t display the report in a correct view. How can I fix this problem?	The reporting system generates all of its output in Unicode format (**www.unicode.org**). To open the CSV reports, start Microsoft Excel and run the **File | Open** command, which displays the Import Wizard. Select the **comma delimited** option to open the report with the data in the correct columns.
Why do I get a registry error when I attempt to open the IT Assistant UI?	A registry editor error occurs while opening the IT Assistant UI on a system with less than the required space. The IT Assistant client requires 25 MB of available hard-drive space.

Alert Management

Question	Answer
Why is the Alert Log for a managed system empty when I receive alerts and see them displayed in the **Alert Logs** view?	When IT Assistant receives an event with an IP address stored in the event, IT Assistant resolves the event to a name accordingly by using its database of discovered systems (if instrumentation name resolution is preferred) or by using DNS (if DNS resolution is preferred). SNMP traps and CIM indications will always have an IP address to resolve from. If the IP address is already resolved to a name, IT Assistant does not attempt to resolve it again because this action could lead to differences in the name stored in the event versus the name under which IT Assistant discovered the system and sent the event, if instrumentation name resolution is preferred in IT Assistant. This issue may result in event actions not being performed due to the selection of system names in the **Event Filters** creation dialog that do not match the name contained in the event. In addition, all of the events received from that system may not be displayed in that system's **Alerts** view in IT Assistant. To avoid this behavior, it is recommended to choose DNS resolution as the preferred resolution in IT Assistant if DNS or WINS exist in the network environment in which IT Assistant is performing discovery.

IT Assistant Services

Question	Answer
How does IT Assistant resolve the names of discovered systems?	See "Name Resolution" in the *Dell OpenManage IT Assistant Online Help*.
Why am I experiencing a slow logon process after rebooting my system? Are IT Assistant Services causing these performance issues?	Ensure that your system meets the minimum system requirements as described in the "Planning Your Dell OpenManage™ IT Assistant Installation."
Why does the SQL server process appear to consume a large amount of the management station's memory when viewing memory consumption from the Task Manager?	The Task Manager may not be reporting the actual amount of memory that is being consumed. To better gauge the SQL server's memory usage, go to **www.microsoft.com** and search for the knowledge base article KB321363, which describes how SQL Server consumes and releases memory.

IT Assistant Discovery

Question	Answer
I have discovered a system that supports CIM indications. In the past I was able to receive indications from the system, but am now no longer receiving them through IT Assistant. I am seeing the indications locally on the managed system.	In order for CIM indications to be sent to the management station, the management station must register with the managed system. The registration is broken every time the management station or the managed system is restarted. When IT Assistant discovers a system, it registers that system with the CIM indication provider. If the managed system is restarted, IT Assistant does not reregister it until the next discovery cycle. To force a reregistration with the indication provider, force discovery of the managed system in IT Assistant by right-clicking the system in the **Device Tree** view and clicking **Refresh Status**.
How do I qualify CIM user names?	CIM is enabled/disabled only by discovery range and requires each CIM user to be qualified with a domain or local host if no trusted domain is configured. It is critical to provide this qualification when configuring CIM through a discovery range (for example: <*domain*>\<*user name*> or *localhost*\<*user name*>) to authenticate and use the CIM protocol. To upgrade from IT Assistant version 6.*x* to version 7.*x*, qualify your user name correctly by editing the discovery ranges.
How does the IT Assistant UI determine the times that it displays?	Dates and times are reported according to the time zone configured on the management station.
Why can't IT Assistant discover systems on the configured discovery range?	Use the IT Assistant Troubleshooting Tool to help resolve this issue. In the UI, go to **Tools→Troubleshooting Tool**. See also "Troubleshooting Tool—Finding and Resolving Discovery Issues" in the *Dell OpenManage IT Assistant Online Help*.
Why does IT Assistant report some attribute values as blank or empty values?	IT Assistant will show blank or empty data values for those attributes which are queried from, but are not returned by, the agent. These blank fields may indicate that the feature is not supported by the device or reported by the device's agent(s), or that the device's current configuration disables the feature. In addition, blank values can also indicate empty fields that are returned by the agent.

Question	Answer
What ports do the IT Assistant services use to communicate? How can I change the port assignments?	Port 2607 enables the IT Assistant UI to communicate with the IT Assistant Connection Service. Port 2606 enables the IT Assistant Connection Service to communicate with the IT Assistant Network Monitoring Service. You can change these port assignments when installing IT Assistant using customized settings. If you do not change the port assignments during customized installation, you must use the registry to reassign port numbers. See also "Ports Used by IT Assistant and Associated Agent Application" in the *Dell OpenManage Security and Installation Guide*.
If I have multiple protocols bound to one network card, IT Assistant displays multiple entries for that network card under Network Data on the Summary tab of the systems window. This leads me to believe that I have more network cards installed on the system than are actually there. Why does IT Assistant display these multiple entries?	This situation is most likely to occur when using pure SNMP to communicate with the managed system. Most of the summary information shown is taken out of tables across the appropriate MIB file. In this case, network information is taken from the MIB2|Interfaces table. Binding multiple protocols to a single network card adds a row to the MIB file interfaces table for each protocol. IT Assistant then pulls all rows from this table. Because there is only one physical address per network card, you can use the physical media access control (MAC) address to ascertain how many network cards are actually installed.
Why does DCOM generate event log messages when it fails to establish communication with managed systems?	This problem is a known issue with the Microsoft WBEM implementation. DCOM logs an error every time a remote connection fails. If CIM is enabled, IT Assistant tries to connect to every CIM agent that resides at an address that can be contacted using the **ping** command. If the user name and password do not work or if there is no CIM agent, DCOM adds an error message to the event log.
Why are IT Assistant services unstable on my system running Windows 2000?	IT Assistant services may exhibit instability on Windows 2000 SP3. See the Microsoft Knowledge Base Article 813648: "Random Access Violations When Multithreaded Applications Call the setlocale Function."
Why is there a delay in the display of discovery feedback in the **Discovery and Monitoring Logs** window?	If a discovery task is already running and another discovery range is entered, the new range may not immediately show in the **Discovery and Monitoring Logs** window. This behavior is also dependent on the number of systems that are being discovered.

Question	Answer
Why does discovery hang on my CIM-enabled IT Assistant installation?	If IT Assistant has CIM enabled and is discovering managed systems with Dell OpenManage Server Agent version 4.4 or earlier that are configured for CIM, discovery may hang. You must upgrade the instrumentation for these systems. In the IT Assistant UI, go to **Discovery and Monitoring→Discovery Configuration** to resolve this issue. See "Discovery Configuration—Configuring IT Assistant to Discover New Devices" in the *Dell OpenManage IT Assistant Online Help*.
A memory leak has occurred in the IT Assistant Network Monitoring Service. What caused the problem?	If IT Assistant is installed on a device that is running Windows 2000 SP4, a known issue with the Microsoft WMI API results in a memory leak in the IT Assistant Network Monitoring Service when using the CIM protocol. The leak occurs when the remote device is passed incorrect authentication credentials during a discovery cycle or status poll.
Why can't I discover my ERA/MC device?	Before you can discover your ERA/MC you must have it properly configured. (For configuration information, see your ERA/MC documentation.) After you configure your ERA/MC, ensure that the IP address assigned to the device is included in the IT Assistant discovery range.
Why does the device status display **Unknown** when I attempt to discover it using the SNMP and CIM protocol combinations?	IT Assistant discovers various ranges asynchronously and one range will be overwritten by the other. Provide consistent credentials for discovering the device. For example, if you have enabled SNMP and CIM with particular credentials for the first range, enter the same SNMP and CIM credentials for the second range for the device to be discovered.
I have discovered a device by specifying the IP address in the range. The system rebooted and received a new IP address. Though the IP address is in the range, why is the **Status** displaying the system as down?	IT Assistant uses the IP address supplied only during discovery for all operations, such as, **Status**, **Troubleshooting**, **Tasks**, and so on. If the IP addresses used for discovery is unavailable or changed (due to **Dynamic Host Configuration Protocol** re-allocation), the **Status** will display the system as down. Discover the device again from the range that contains the updated IP address for the device.

Performance Monitoring

Question	Answer
I have scheduled my performance monitoring tasks with an interval of 2 minutes. The task, however, does not fetch all samples at equal intervals.	The delay in fetching samples can be caused due to various reasons, such as, low memory or high processor utilization on the IT Assistant management station.
I am unable to see the information about the memory attribute in Execution Results pane of the task.	If an attribute is not supported on the remote device (managed system), information about the attribute will not display in the **Execution Results** pane of the task and the **Performance** tab on the **Device** view. Also, this attribute is not considered for status calculations.
I stopped the Windows Management Interface (WMI) service. When I restart this service, why do I see the "Unable to connect to device using CIM/SSH" message?	This is a normal situation. Data collection will start after fifteen to thirty minutes, as the connections are released once every fifteen minutes.

IPMI Discovery Support

Question	Answer
I have given my system IP address and credentials for Intelligent Platform Management Interface (IPMI) discovery, but the discovery still fails.	Provide the managed system's BMC IP address and the BMC credentials (user name, password, and KG Key) **NOTE:** KG Key is available only on PowerEdge *x9xx* systems.
I have configured BMC on my managed systems. However, I am still unable to discover these systems.	Ensure that you have a LAN connection to the BMC.
I am using the IPMI discovery feature to discover my *x9xx* systems. However, I am unable to get the software and hardware inventory of these systems.	IPMI discovery feature communicates with the BMC of the managed systems to get the status of the systems. The BMC provides data such as: • power and chassis status • hardware log • service tag • host name • operating system • system type BMC does not provide any other information about the managed systems. **NOTE:** If you want more information about your managed systems, you can use the Software Deployment feature of IT Assistant to deploy Dell agent (Server Administrator) on your managed systems. For more information, see "Using Server Software Deployment."

Miscellaneous

Question	Answer
I want to run another application on the port on which the IT Assistant Netmon Service is installed. Do I have to uninstall and reinstall IT Assistant?	The port number for the DSM IT Assistant Network Monitor service is defined using the Microsoft Windows registry key `HKLM\Dell Computer Corporation\Dell OpenManage IT Assistant\Network Monitoring Service\PortNumber`. Change the value of this key and restart the DSM IT Assistant Connection Service and the DSM IT Assistant Network Monitor services.
What are the names of the various IT Assistant services?	The names of the IT Assistant services are: • DSM IT Assistant Network Monitor • DSM IT Assistant Connection Service
I have redundant entries for Dell™ PowerConnect™ switches—one under the **Unknown** category and the other under **Network Devices** as **Switch Object**.	When IT Assistant discovers the PowerConnect switch with its IP address configured, but SNMP not configured, it classifies this object under the **Unknown** group as an **Unknown** device. However, when you configure SNMP on the switch, and click **Refresh Inventory**, IT Assistant reclassifies the switch as a **Switch Object** under the **Network Devices** category, but does not delete the **Unknown** entry. You must delete the redundant **Unknown** entry manually.
The RAC Console Application Launch is not available for my systems.	If you have discovered your systems using CIM instead of SNMP, then the RAC Console Application Launch will not be available.
I am unable to receive traps from the Dell OpenManage Server Administrator Storage Management Service from my Linux systems.	Ensure that the **snmpd.conf** file is *not* set to send SNMP traps in version 2 format. IT Assistant does not recognize the SNMP version 2 format. Ensure that the trap format is set to `trapsink hostname <community string>`. **NOTE:** `trapsink` sends SNMP version 1 traps `trap2sink` sends SNMP version 2 traps.
I am not able to receive Array Manager and Storage Management Service events.	Storage Management Services and Array Manager do not support CIM. Therefore, IT Assistant does not receive events from storage devices using CIM. To receive storage events, configure Array Manager and Storage Management Service to send SNMP-based events.
I am unable to see the latest data on the **Tasks** tree.	If you are seeing outdated data or if the data is missing, press F5 to manually refresh the IT Assistant user interface.

Configuring Protocols to Send Information to Dell OpenManage™ IT Assistant

Dell OpenManage IT Assistant uses two systems management protocols — Simple Network Management Protocol (SNMP) and Common Information Model (CIM). This appendix provides configuration information for SNMP and CIM. These systems management protocols allow IT Assistant to get status for Dell™ PowerEdge™ systems using server agents or Dell OpenManage Client Instrumentation (OMCI). This appendix includes procedures for configuring SNMP and CIM that support the discovery, status, and trap information. The following table summarizes the availability of supported operating systems and corresponding SNMP and CIM protocols for systems that can be managed by IT Assistant.

Table A-1. Supported Operating Systems and Systems Management Protocols on Managed Systems

Operating System	SNMP	CIM
Microsoft® Windows® operating system	Available from the operating system installation media.	Available from the operating system installation media
Red Hat® Linux operating system	You must install the SNMP package provided with the operating system.	Unavailable
SUSE® Linux Enterprise Server operating system	You must install the SNMP package provided with the operating system.	Unavailable

Configuring the SNMP Service

In order for IT Assistant to install and function properly, it must be installed on a supported Microsoft operating system that has the SNMP service installed and running. Unless it has been modified after installation, the Microsoft operating system SNMP service should require no additional configuration. Although the SNMP service on IT Assistant system does not require special configuration, the SNMP service on the systems that it will be managing does. Furthermore, whereas IT Assistant can be installed only on supported Microsoft operating systems, it can manage systems that are running supported Microsoft, SUSE® Linux Enterprise Server, and Red Hat Enterprise Linux operating systems. This section explains how to configure SNMP on these managed systems.

Each of the managed systems that use the SNMP protocol to communicate with IT Assistant must have read/write and read-only community names assigned. If you want IT Assistant to be able to receive traps from these managed systems, you must also configure an SNMP trap destination, defined either by host name or by IP address.

SNMP Community Names in IT Assistant and Server Administrator

For IT Assistant to successfully read information, modify information, and perform actions on a system running Dell OpenManage Server Administrator (the Dell recommended server agent) and/or other supported agents, the community names used by IT Assistant must match the corresponding community read-only (Get) and read/write (Set) community names on the managed system. Also, for IT Assistant to receive traps (asynchronous event notifications) from a system running Server Administrator, the system must be configured to send traps to the system running IT Assistant. For more information, see "Configuring SNMP for System Manageability."

Community Names Must Be Secure

There are operating system default names for both Get and Set community names. For security reasons, these names should be changed. When selecting community names for your network, use the following guidelines:

- Change both the Get and Set names to passwords that are hard to guess.
- Avoid using strings such as your company's name or phone number or any well known personal information about yourself.
- Use an alphanumeric string that includes both letters and numbers, mixing uppercase and lowercase letters; community names are case-sensitive.
- Use strings that are at least six characters long.

Configuring the SNMP Service on a System Running a Supported Windows Operating System

Running IT Assistant

IT Assistant may be installed on a system with any of following operating systems: Windows 2000, Windows XP Professional, or Windows Server® 2003. See the readme for the latest information on supported operating systems details and hardware configuration.

To install SNMP on the IT Assistant system, perform the following steps:

1. Click the **Start** button, point to **Settings**, and choose **Control Panel**.
2. Double-click the **Add or Remove Programs** icon.
3. In the left-hand pane, click **Add/Remove Windows Components**.
4. Select **Management and Monitoring Tools**, click **Details**, select **Simple Network Management Protocol**, and click **OK**.
5. Click **Next**.

   The **Windows Optional Networking Components Wizard** installs SNMP.

Configuring the SNMP Service on an IT Assistant Managed System Running a Supported Windows Operating System

Server Administrator and certain other managed system agents, such as Dell PowerConnect™ switches, use the SNMP protocol to communicate with IT Assistant. To enable this communication, the Windows SNMP service must be properly configured to enable Get and Set operations and to send traps to a services system.

NOTE: See your operating system documentation for additional details on SNMP configuration.

NOTE: For systems running Windows Server 2003 to be discovered, Microsoft's standard SNMP configuration on Windows Server 2003 requires SNMP to be configured to accept packages from the IT Assistant host.

Change the SNMP Community Name

Configuring the SNMP community names determines which systems are able to manage your system through SNMP.

1 If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, right-click **My Computer**, and point to **Manage**.

   The **Computer Management** window appears.

2 Expand the **Computer Management** icon in the window, if necessary.

3 Expand the **Services and Applications** icon and click **Services**.

4 Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service**, and then click **Properties**.

   The **SNMP Service Properties** window appears.

5 Click the **Security** tab to add or edit a community name.

   a To add a community name, click **Add** under the **Accepted Community Names** list.

      The **SNMP Service Configuration** window appears.

   b Type the community name of a system that is able to manage your system (the default is `public`) in the **Community Name** text box and click **Add**.

      The **SNMP Service Properties** window appears.

   c To change a community name, select a community name in the **Accepted Community Names** list and click **Edit**.

      The **SNMP Service Configuration** window appears.

   d Make all necessary edits to the community name of the system that is able to manage your system in the **Community Name** text box, and then click **OK**.

      The **SNMP Service Properties** window appears.

6 Click **OK** to save the changes.

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the managed system to change Server Administrator attributes using IT Assistant.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, right-click **My Computer**, and point to **Manage**.

   The **Computer Management** window appears.

2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon, and then click **Services**.
4. Scroll down the list of services until you find **SNMP Service,** right-click **SNMP Service**, and click **Properties**.

   The **SNMP Service Properties** window appears.

5. Click the **Security** tab to change the access rights for a community.
6. Select a community name in the **Accepted Community Name**s list, and then click **Edit**.

   The **SNMP Service Configuration** window appears.

7. Set the **Community Rights** to **READ WRITE** or **READ CREATE**, and click **OK**.

   The **SNMP Service Properties** window appears.

8. Click **OK** to save the changes.

Configuring Your System to Send SNMP Traps

Managed system agents such as Server Administrator generate SNMP traps in response to changes in the status of sensors and other monitored parameters. You must configure one or more trap destinations on the managed system for these traps to be sent to an IT Assistant system.

1. If your system is running Windows Server 2003, click the **Start** button, right-click **My Computer**, and point to **Manage**. If your system is running Windows 2000, right-click **My Computer** and point to **Manage**.

   The **Computer Management** window appears.

2. Expand the **Computer Management** icon in the window, if necessary.
3. Expand the **Services and Applications** icon and click **Services**.
4. Scroll down the list of services until you find **SNMP Service**, right-click **SNMP Service,** and click **Properties**.

   The **SNMP Service Properties** window appears.

5. Click the **Traps** tab to add a community for traps or to add a trap destination for a trap community.
6. To add a community for traps, type the community name in the **Community Name** box and click **Add to list**.

7 To add a trap destination for a trap community, select the community name from the **Community Name** drop-down menu and click **Add**.

The **SNMP Service Configuration** window appears.

8 Type the trap destination and click **Add**.

The **SNMP Service Properties** window appears.

9 Click **OK** to save the changes.

Configuring the SNMP Agent on Systems Running Supported Linux Operating Systems

This section describes the configuration of SNMP agents on systems running Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems.

Managed system agents such as Server Administrator use the SNMP services provided by the ucd-snmp or net-snmp SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to an IT Assistant system. To configure your SNMP agent for proper interaction with IT Assistant, perform the procedures described in the following sections.

NOTE: See your operating system documentation for additional details on SNMP configuration.

Changing the SNMP Community Name

Correctly configuring SNMP community names determines which IT Assistant services systems are able to communicate with managed systems in your network. The SNMP community name used by IT Assistant must match an SNMP community name configured on a managed system so that IT Assistant can successfully read from, write to, and perform actions on managed systems in your network.

To change the SNMP community name, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf**, by performing the following steps:

1 Find the line that reads:

```
com2sec publicsec default public
```

or

```
com2sec notConfigUser default public
```

2 Edit this line by replacing `public` with the new SNMP community name. When edited, the line should read:

```
com2sec publicsec default community_name
```

or

```
com2sec notConfigUser default community_name
```

To change the SNMP community name in SUSE Linux Enterprise Server, edit the SNMP agent configuration file, **/etc/snmpd.conf** by performing the following steps:

1 Find the line that reads:

```
rocommunity public 127.0.0.1
```

2 Edit this line by replacing `rocommunity` with the new SNMP community name. When edited, the line should read:

```
rwcommunity public <ITA system IP address>
```

Enabling SNMP Set Operations

SNMP Set operations must be enabled on the system running Server Administrator in order to change Server Administrator attributes using IT Assistant. To enable SNMP Set operations on the system running Server Administrator, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf** (**/etc/snmpd.conf** in SUSE Linux Enterprise Server), and perform the following steps:

1 Find the line that reads:

```
access publicgroup "" any noauth exact all none none
```

or

```
access notConfigGroup "" any noauth exact all none none
```

2 Edit this line, replacing the first `none` with `all`. When edited, the line should read:

```
access publicgroup "" any noauth exact all all none
```

or

```
access notConfigGroup "" any noauth exact all all none
```

For Red Hat Enterprise Linux (version 7.3 or later) and Red Hat Enterprise Linux AS (version 2.1 or later) operating systems, the default SNMP access for the `sysLocation` and `sysContact` variables has been changed to read-only access. IT Assistant uses the access rights for these variables to determine whether or not certain actions can be performed through SNMP. These variables must be configured with read/write access to enable "sets" or system configuration setting changes in IT Assistant. To configure the variables, it is recommended that you comment out the `sysContact` and `sysLocation` values in the Red Hat Enterprise Linux and SUSE Linux Enterprise Server SNMP configuration file.

1 Find the line that starts with `sysContact`.

2 Change the line to `#sysContact`.

3 Find the line that start with `sysLocation`.

4 Change the line to `#sysLocation`.

Configuring Your Managed Systems to Send Traps to IT Assistant

Managed system agents such as Server Administrator generate SNMP traps in response to changes in the status of sensors and other monitored parameters on a managed system. For IT Assistant to receive these traps, one or more trap destinations must be configured on the managed system.

To configure your system running Server Administrator to send traps to a Services system, edit the SNMP agent configuration file, **/etc/snmp/snmpd.conf** (**/etc/snmpd.conf** in SUSE Linux Enterprise Server), by performing the following steps:

1. Add the following line to the file:

   ```
   trapsink IP_address community_name
   ```

   where *`IP_address`* is the IP address of the services system and *`community_name`* is the SNMP community name.

2. Save the **snmpd.conf** file and restart the snmpd service.

Setting Up CIM

CIM is available only on supported Microsoft Windows operating systems.

Setting Up CIM on Your Managed Systems

This subsection provides steps for setting up CIM on managed systems running supported Windows operating systems. For more information, see "Configuring CIM for Manageability."

Recommendation for Creating a Domain Administrator

Although the following procedure describes how to add a local administrator to a supported Windows operating system, Dell recommends that you create a domain administrator instead of create a user on every system managed by IT Assistant. Creating a domain user account will also aid in preventing account lockouts due to failed IT Assistant logons to systems found in the entered discovery range. By example, a discovery range of 192.168.0.* would result in an attempt to log on to all 253 systems. If the credentials passed to any one of these managed systems did not authenticate, the account would become locked out. In addition, the improved security in Windows XP mandates that the client be in the same domain as the IT Assistant system. Windows XP also requires a user name with a nonblank password. For more information on creating a Windows domain user account, see your Microsoft documentation.

NOTE: IT Assistant requires the CIM user name and password with administrator rights that you established on the managed systems. If you are using a domain user, be sure to specify the correct domain in the user name field. A user name must always be qualified with a domain, or **localhost** if a domain is not present. The format is either **domain\user** or **localhost\user**.

NOTE: CIM discovery requires proper user ID and password credentials. Failure to supply proper credentials on a subnet configured for CIM discovery can result in account lockout.

For Managed Systems Running Windows 2000

NOTE: The WMI core is installed with Windows 2000 by default.

1 Click **Start→Settings→Control Panel→Administrative Tools→Computer Management**.

2 In the **Computer Management (Local)** tree, expand the **Local Users and Groups** branch and click the **Users** folder.

3 On the menu bar, click **Action** and then click **New User**.

   a In the **New User** dialog box, fill in the required information fields with the user name and password – for example, `CIMUser` and `DELL`. (These are only examples for illustration; you should set user names and passwords as appropriate for your enterprise.)

   b Ensure that you deselect the **User must change password at next logon** check box.

   c Click **Create**.

4 In the right pane of the **Computer Management** dialog box, double-click **CIMUser**.

   You may have to scroll through the list to locate **CIMUser**.

5 In the **CIMUser Properties** dialog box, click the **Member Of** tab.

6 Click **Add**.

7 Click **Administrators**, click **Add**, and then click **OK**.

8 Click **OK** again, and then close the **Computer Management** dialog box.

9 Install Client Instrumentation 7.*x* or Server Administrator, depending on whether the system is a client or a server.

10 Restart the system.

For Managed Systems Running Windows XP Professional

As mentioned previously, the improved security in Windows XP mandates that the client be in the same domain as the IT Assistant system. Also, when implementing your own user name and password, do not specify a blank password.

The following steps detail how to create a local user. Dell highly recommends that you create a domain user with administrative rights so that you do not have to manually add a user to every client. This will simplify the creation of discovery ranges in IT Assistant.

1 Click **Start→Settings→Control Panel→Administrative Tools→Computer Management**.

2 In the **Computer Management (Local)** tree, expand the **Local Users and Groups** branch and click the **Users** folder.

3 On the menu bar, click **Action** and then click **New User**.

   a In the **New User** dialog box, fill in the required information fields with the user name `CIMUser` and password `DELL`.

   b Ensure that you clear (deselect) the **User must change password at next logon** check box.

   c Click **Create**.

4. In the right pane of the **Computer Management** dialog box, double-click **CIMUser**.

   You may have to scroll through the list to locate **CIMUser**.

5. In the **CIMUser Properties** dialog box, click the **Member Of** tab.
6. Click **Add**.
7. Click **Administrators**, click **Add**, and then click **OK**.
8. Click **OK** again, and then close the **Computer Management** dialog box.

   NOTE: Windows XP Professional is supported for use on IT Assistant client systems only.

9. Install Client Instrumentation 7.*x* or Server Administrator, depending on whether the system is a client or a server.
10. Restart the system.

For Managed Systems Running Windows Server 2003

1. Click **Start→Settings→Control Panel→Administrative Tools→Computer Management**.
2. In the **Computer Management (Local)** tree, expand the **Local Users and Groups** branch and click the **Users** folder.
3. On the menu bar, click **Action** and then click **New User**.
   a. In the **New User** dialog box, fill in the required information fields with the user name `CIMUser` and password `DELL`.
   b. Ensure that you clear (deselect) the **User must change password at next logon** check box.
   c. Click **Create**.
4. In the right pane of the **Computer Management** dialog box, double-click **CIMUser**.

   You may have to scroll through the list to locate **CIMUser**.

5. In the **CIMUser Properties** dialog box, click the **Member Of** tab.
6. Click **Add**.
7. Click **Administrators**, click **Add**, and then click **OK**.
8. Click **OK** again, and then close the **Computer Management** dialog box.
9. Install Client Instrumentation 7.*x* or Server Administrator, depending on whether the system is a client or a server.
10. Restart the system.

B

Utilities in Dell OpenManage™ IT Assistant

IT Assistant has three utilities:

- Import Node List Utility
- Database Management Utility
- Simple Network Management Protocol (SNMP) Event Source Import Utility

IT Assistant Import Node List Utility

The **Import Node List** utility allows you to create a file that defines a discovery list comprised of managed devices, IP addresses, or IP address ranges. This utility supports any type of address that you can enter through the IT Assistant user interface. The IT Assistant import node utility uses the file to quickly import the list into IT Assistant. Using this utility provides:

- A convenient method for those users who have their network configuration already mapped-out in files and want to quickly import this configuration into IT Assistant
- A very targeted discovery, rather than specifying a general subnet for discovery, such as 10.34.56.*

To use the **Import Node List** utility, follow these general steps:

1. Create a file containing the list of discovery addresses and/or system names that you want to import.

   For each entry in the file, you must specify the protocol settings (such as the SNMP protocol's community name). To provide this information to IT Assistant, you must use a template. A template allows you to assign protocol settings to each entry in the file.

2. Define a template that will be applied to one or more discovery ranges. You define the template by entering a discovery range with the host name of `default_template`. The import node list utility applies the protocol settings defined in this template to each discovery item in the file.

3 Run the utility from the command line. (The import node utility is located in the IT Assistant **/bin** directory.) Specify the filename for the file you created and, optionally, the template name. You can also specify the template name in the file. For example:

```
importnodelist nodelist.txt
```

The following options are available and may be specified in any order after the filename:

-delete — This option causes the template(s) used to be automatically deleted after the utility successfully imports the node list.

-default <templatename> — Allows for a different default template name to be used. The default name is **default_template**.

See sample commands for more information.

4 Restart IT Assistant Services.

You can use a default template to import a discovery list into IT Assistant. To import a list of nodes, perform the following steps:

1 Create a file by using the following format (do not include the <begin_file> or <end_file> specifiers):

```
<begin_file>

#This is a comment (a "#" sign at the beginning of the line means to
#ignore the line).

23.45.65.34

23.45.65.35

hostname1

hostname2

23.34.55.*

12.34.56.20-30

<end_file>
```

The last line of the file must have a line feed in it. You can also use any combination of the subnet formats supported by the IT Assistant user interface. It is important to make sure that each entry is the correct format because the import node list utility does not check and validate the format for you.

2 Save the file and specify a filename, for example, **nodelist.txt**.

Sample Import Node List Utility Commands

Import the nodes from the file **nodelist.txt**:

```
importnodelist nodelist.txt
```

Delete the templates used after a successful import:

```
importnodelist -delete
```

Import the nodes from the file **nodelist.txt**, delete the templates used after a successful import, and use "my_template" as the default template name:

```
importnodelist nodelist.txt -delete -default my_template
```

Creating Templates

To create a template for import node list utility, follow these general steps:

1. In **Discovery and Monitoring**, select **Ranges**.
2. Right-click **Include Ranges** in the **Discovery Ranges** tree and select **New Include Range...**.
3. In the **New Discovery Wizard-Step 1 of 6**, select **Host Name**.
4. Enter the template name in **Host Name** (for example, template_1).
5. Complete the wizard by entering the required protocol configurations.

Template_1 can be used in import node list utility.

Using Multiple Templates

The import node list utility supports the use of multiple templates, where different entries in the file may each use different protocol settings and require different templates. The following import file provides an example for using multiple templates:

```
<begin_file>

#This is a comment (a "#" sign at the beginning of the line means to ignore
#the line).

23.45.65.34,template1

23.45.65.35,template1

hostname1

hostname2,template2

23.34.55.*,template2

12.34.56.20-30

<end_file>
```

In this example, the first two entries use a template named **template1**, while entries four and five use a template named **template2**. The rest of the entries use the default template. In this example, you must enter the discovery configuration ranges (from the IT Assistant user interface) of "default_template", "template1", and "template2" and configure their protocol settings appropriately (perhaps they have different SNMP community names). Note that any name may be used for a template name, even an IP address or subnet range. However, Dell recommends that you use names that allow for easy identification as templates.

Saving Templates

If multiple templates are needed to correctly configure a file of node entries, it is possible to set up the templates in IT Assistant, then export the settings for backup or some other purpose. The database management utility, **dcdbmng.exe**, is located in IT Assistant's **/bin** directory. This utility allows you to import, export, and clear IT Assistant database tables. To export templates, perform the following steps:

1. Configure all required templates in IT Assistant.
2. Export the table that contains all entered templates. Navigate to IT Assistant's /bin directory and double-click **dcdbmng.exe**. The database management utility interface starts. On the left tree, navigate to the Discovery Configuration table. Right-click this tree node and select **Export Table**. Enter a name for the file to export to.

   The file containing the templates can now be imported to another IT Assistant installation. You can also restore the file to a new IT Assistant installation by using the Import Table option (right click the table name in the database management utility). When the templates are imported, you can run the import node list utility on the accompanying file of node entries.

Leaving Templates in IT Assistant

If template names are addresses that are not discoverable (for example, it is unlikely that a host name such as "default_template" exists), the templates may remain in IT Assistant. IT Assistant tries to discover the item, but no results occur from the attempted discovery. If many templates are used, it is recommended that you delete the templates to avoid wasting IT Assistant discovery cycles on nondiscoverable addresses.

Database Management Utility

The Dell OpenManage IT Assistant Database Management Utility has two implementations: a graphical user interface (GUI) and a command line interface. Both versions of the utility allow users to perform operations on databases and tables that reside in the IT Assistant data repository.

NOTE: The IT Assistant 6.*x* database schema is not directly compatible with the IT Assistant 7.*x* database schema. Only certain tables in the IT Assistant 6.*x* database schema will be migrated, such as discovery configuration, global configuration, and alert action tables. The database schema can only be migrated during an upgrade of IT Assistant.

NOTE: IT Assistant does not support a direct upgrade from version 6.*x* to version 8.0. You will be required to first upgrade IT Assistant version 6.*x* to 7.0 and then to IT Assistant version 8.0.

You must start the GUI version of the Database Management Utility separately from IT Assistant. When you start the utility, a window opens that contains database and table management functions. The command line application performs the functions of the GUI utility along with a few others.

Using the Command Line Database Management Utility

At a command prompt, change directory to **\Program Files\Dell\SysMgt\IT Assistant\bin**.

Type `dcdbmng` followed by a switch that specifies the command you want. To see a list of valid switches, type:

```
dcdbmng /h
```

OR

```
dcdbmng /H
```

OR

```
dcdbmng /?
```

NOTE: Type a space between the **dcdbmng** command and the / (forward slash).

This command displays a dialog box that lists commands that you can use to do the following:

- Install the appropriate database engine (Microsoft® Data Engine (MSDE) for IT Assistant version 7.x and earlier or SQL Server 2005 Express for IT Assistant version 8.0).
- Start and stop the database engine.
- Attach and detach database files to and from the database engine.
- Import and export tables and databases.

  NOTE: Due to the differences in the way that Microsoft encrypts data between operating system versions, exporting IT Assistant database tables with encrypted passwords from one version of a Microsoft operating system (for example, Windows 2000) and importing into another version (for example, Windows 2003) is not supported.

- Clear tables.
- Restore data for the global IT Assistant configuration or the event management system configuration only.

Help

- Command: **dcdbmng /h** or **dcdbmng /H** or **dcdbmng /?**
- Description: Displays the command line options.

Attach Database

- Command: **dcdbmng /A** *path* or **dcdbmng /a** *path*
- Description: Attaches the single database file specified by *path* to the SQL Server 2005 Express or the Microsoft SQL 2005 Server.

Clear Table

- Command: **dcdbmng /Z** *tablename* or **dcdbmng /z** *tablename*
- Description: Removes all the rows from the specified table, but does not delete the table.

Detach Database

- Command: **dcdbmng /R** or **dcdbmng /r**
- Description: Detaches the attached database file from the SQL Server 2005 Express or the SQL 2005 Server.

NOTE: The detached database file remains in the location from where it was attached to the SQL Server 2005 Express or the SQL 2005 Server.

Export Table

- Command: **dcdbmng /E** *tablename filename* or **dcdbmng /e** *tablename filename*
- Description: Exports the data in the table specified by *tablename* to the flat text file specified by *filename*. If the flat text file does not exist, the utility creates it. If *filename* does not include path information, the utility creates the file in the local directory.

Export Database

Command: **dcdbmng /X** *path* or **dcdbmng /x** *path*

Description: Exports data from all tables in the database to flat text files in the location specified by path.

NOTE: The utility creates the files in the location specified by path in the format of **tablename.txt**.

Import Table

- Command: **dcdbmng /I** *tablename path [migrate]* or **dcdbmng** */i tablename path [migrate]*
- Description: Imports data to the table specified by *tablename* from the flat text file specified in *path*.

Import Database

- Command: **dcdbmng /M** *path* or **dcdbmng /m** *path*
- Description: Imports data to all tables in the database from flat text files in the location specified by *path*.

Install MSDE

- Command: **dcdbmng /N** or **dcdbmng /n**
- Description: Silently installs MSDE.

NOTE: The **MSDEx85.exe** and **iss** files must be placed in the correct location.

Start Server

- Command: **dcdbmng /T** or **dcdbmng /t**
- Description: Starts the **MSSQLServer** service.

Stop Server

- Command: **dcdbmng /P** or **dcdbmng /p**
- Description: Stops the **MSSQLServer** service.

Suppress Messages

When you run the Database Management Utility as a command line application, you receive messages when commands succeed or fail. The command to suppress messages halts these notifications.

- Command: **dcdbmng /S**
- Description: Runs without displaying any messages (whether the action was successful or unsuccessful). This command is useful if you are running the utility from a batch file.

NOTE: Using **/S** with no other option causes the command to be ignored.

Simple Network Management Protocol Event Source Import Utility

You can import multiple event sources, not natively supported in IT Assistant, into the IT Assistant database.

Create a text file containing the appropriate event source information. After creation, this text file will not be available for sharing between multiple users of the product.

Run a Command Line Interface (CLI) utility (you can find the this utility in <*install folder of IT Assistant*>/bin) to import the text file data into the IT Assistant database.

Ensure that the text file format complies with the following formatting rules:

1. The format for the usage of the utility must be:

   ```
   ImportEventSources.exe <fully qualified path\filename>
   ```

2. All values of a particular Event Source must be bar-separated.
3. Each Event Source entry must be on a separate line.

4 The format of entries for each Event Source must be:

```
<EventCategoryName>|<EventSourceName>|<Severity>|<Format
String>|<SNMPEnterpriseOID>|<SNMPGenericTrapID>|<SNMPSpecificTrapID>
|<EventPackageName>
```

5 The format for severity strings by value must be:

```
<ObjectId>,<ObjectValue>,<Severity>;<ObjectId1>,<ObjectValue1>,
<Severity1>
```

6 EventSourceName cannot be NULL or an empty string.

NOTE: If the EventCategoryName is an empty string, the category is defaulted to **Other**. If the category name does not match any of the pre-defined category types in IT Assistant, a new Event Category is created with the category name that you enter.

NOTE: If the severity string entered in the input file does not match the pre-defined severity strings, an appropriate error message is displayed.

NOTE: A combination of EnterpriseOID, Generic TrapID, and SpecificTrapID for each event should be unique. Also, the combination of EventSourceName and EventPackageName is validated to check if the entry is unique.

NOTE: Enter two consecutive bars (" || ") to represent NULL or empty strings.

The following is a sample MIB entry.

```
-- Lower Critical threshold crossed
 asfTrapFanSpeedProblem TRAP-TYPE
 ENTERPRISE asfPetEvts
 DESCRIPTION
 "Generic Critical Fan Failure"
 --#SUMMARY    "Generic Critical Fan Failure"
 --#ARGUMENTS  {}
 --#SEVERITY   CRITICAL
 ::= 262402
```

The conversion process is as follows:

```
EventCategory : Environmental
```

NOTE: IT Assistant has a set of pre-defined categories (Environmental, General Redundancy, Keyboard-Video-Mouse (KVM), Memory, Physical Disk, Power, Printers, Processor, Security, Storage Enclosure, Storage Peripheral, Storage Software, System Events, Tape, Virtual Disk, and Other). The event could fall under any of these categories. However, a new category can also be created.

`EventSourceName : asfTrapFanSpeedProblem`

`Severity : Critical [--#SEVERITY]`

NOTE: IT Assistant categorizes events under the following categories: Ok, Warning, Critical, Information, and Unknown.

`Format String : Generic Critical Fan Failure [--#SUMMARY]`

`EnterpriseOID : .1.3.6.1.4.1.3183.1.1` (To get the EnterpriseOID, compile the MIB, in this case "DcAsfSrv.mib," in MG-Soft or any other MIB browser.)

`GenericTrapId : 6`

`SpecificTrapId : 262402 [::=]`

`EventPackageName : ASF` (You can get this information from the MIB. Open the MIB. The EventPackageName is displayed within `[--Begin Definition]`.)

If there is no package present under which the EventSource falls, you can provide a new category name.

The final entry in the text file will be similar to:

```
Environmental|asfTrapFanSpeedProblem|Critical|Generic Critical Fan
Failure|.1.3.6.1.4.1.3183.1.1|6|262402|ASF
```

NOTE: In case the import file contains a non-existing category, the category will be created.

Index