



Dell OpenManage™ IT Assistant

Version 7.2

User's Guide

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.

Information in this document is subject to change without notice.
© 2005 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *Dell OpenManage*, *OptiPlex*, *PowerEdge*, and *PowerConnect* are trademarks of Dell Inc.; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation; *Novell* and *NetWare* are registered trademarks of Novell, Inc.; *Red Hat* is a registered trademark of Red Hat, Inc.; *Intel* is a registered trademark of Intel Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

December 2005

Contents

1	Introducing IT Assistant	9
	Simplifying System Administration	9
	Identifying the Groups of Systems for Remote Management	9
	Consolidating a View of All Your Systems	9
	Creating Alert Filters and Actions	10
	Creating Customized Discovery and Inventory Reports	10
	Creating Tasks That Enable Configuration Management From a Central Console	10
	Understanding IT Assistant's Components	10
	User Interface.	11
	IT Assistant Services	11
	Terminology: Managed System and IT Assistant System	12
	Integrated Features	12
	Native Install	12
	User Interface Design and Online Help.	12
	DMI Support	12
	New Topology View.	12
	Dynamic Groups	13
	Application Launch	13
	Reporting	13
	Software Updates.	14
	Manage Tasks.	14
	Troubleshooting Tool	14
	User Authentication.	14
	Enhanced Inventory Cycle	14
	Single Sign-On	15
	User Preferences	15
	Other Information You May Need	15

2	Planning Your IT Assistant Installation	17
	Decisions That You Make Before Installation.	17
	Primary Planning Questions.	18
	Selecting the Operating System.	18
	Selecting a Hardware Configuration	19
	Selecting the MSDE Default Database or SQL 2000 Server.	19
	E-mail Notification Features.	20
	Determining Systems Management Protocols	20
	Supported Protocols	20
	SNMP	20
	CIM	20
	Factors That Affect Protocol Choice	21
	Summary of Pre-Installation Decisions	23
3	Installing, Uninstalling, and Upgrading IT Assistant.	25
	Installation Requirements	25
	TCP/IP Protocol Support	25
	Setting Up or Enabling Protocols for Agent Communication	25
	Installing SNMP on the IT Assistant System	25
	Enabling CIM	26
	Setting Up RBAC User Information	26
	Installing IT Assistant	27
	Upgrading from a Previous Version of IT Assistant.	28
	Uninstalling IT Assistant.	29
	Remote Microsoft SQL Server and IT Assistant	29

4	Configuring IT Assistant to Monitor Your Systems	31
	IT Assistant in Real-World User Scenarios	31
	Ensure That Agents and Instrumentation Are Installed and Running.	31
	Start IT Assistant.	32
	Configuring SNMP for System Manageability.	33
	Details on Configuring the SNMP Service	33
	Configuring SNMP on Systems You Want to Manage	33
	Configuring CIM for Manageability	34
	Configuring CIM in the Operating System	34
	Best Practices for Setting Up Discovery Targets	35
	Discovery in Jane’s Small-to-Medium Size Business	36
	Determining Requirements for a Mixed Server-Client System.	36
	Initial Tasks for Finding Systems on Jane’s Network.	37
	Using IT Assistant to Find and Manage Jane’s Networked Systems	37
	Configuring Discovery Settings.	38
	Configuring Inventory Settings	39
	Configuring Status Polling Settings.	39
	Configuring Discovery Ranges	40
	Changing Discovery, Inventory, and Status Polling Settings After Original Setup.	41
	Creating Alert Action Filters and Alert Actions for Jane’s Small-to-Medium Size Business	42
	Creating an Alert Action Filter	42
	Creating an Alert Action	43
	Discovery in Tom’s Enterprise-Size Business.	44
	Configuring the Discovery Cycle	44
	IP Subnet Ranges for Servers	45
	Configuring SNMP on Each Managed System	45
	Selecting An Appropriate Discovery Time-Out Value for the Network	46
	Configuring Discovery Settings.	47
	Configuring Inventory Settings	48
	Configuring Status Polling Settings.	48
	Configuring Discovery Ranges	49
	Changing Discovery, Inventory, and Status Polling Settings After Original Setup.	51

	Creating Alert Action Filters and Alert Actions for Tom's Large Enterprise	51
	Tom's Administrators	52
	Creating Custom Groups	52
	Creating an Alert Action Filter	53
	Notification Alert Actions in the Enterprise Environment	54
	Creating an Alert Action	54
	Summary	55
5	Reporting and Task Management	57
	Custom Reporting	57
	Creating a New Report	59
	Editing, Deleting, or Running Reports.	60
	Pre-defined Reports	60
	IT Assistant Database Schema Information	61
	Software Updates	77
	Using Software Updates in IT Assistant	77
	Managing Tasks	78
	Creating a Device Control Task.	78
	Other Tasks Available in IT Assistant.	79
6	Ensuring a Secure Dell OpenManage IT Assistant Installation	81
	TCP/IP Packet Port Security	81
	Securing Managed Desktops, Laptops, and Workstations	81
	Securing the Managed System's Operating System	81
	Session Time-out	81
	ASF and the SNMP Protocol	82
	Securing Managed Server Systems	82
	Securing the Managed System's Operating System	82
	Choosing the Most Secure Managed System Server Protocol	82
	CIM Monitoring, DCOM, and Windows Authentication	82
	Security and the SNMP Protocol.	83
	Ensuring Database Security When Using IT Assistant.	84

Running IT Assistant Behind a Firewall	84
Setting Up Additional Security for IT Assistant Access	85
Securing Ports for IT Assistant and Other Supported Dell OpenManage Applications	87
Single Sign-On	87
Role-Based Access Security Management	88
Role-Based Access Control	88
Assigning User Privileges	89
Creating IT Assistant Users for Supported Windows Operating Systems	89
Disabling Guest and Anonymous Accounts	91
A Configuring Protocols to Send Information to IT Assistant	93
Configuring the SNMP Service	93
SNMP Community Names in IT Assistant and Server Administrator	94
Configuring the SNMP Service on a System Running a Supported Windows Operating System	94
Configuring the SNMP Service on an IT Assistant Managed System Running a Supported Windows Operating System	95
Enabling SNMP Set Operations	96
Configuring Your System to Send SNMP Traps	96
Configuring the SNMP Agent on Systems Running Supported Red Hat Linux Operating Systems	97
Change the SNMP Community Name	97
Enabling SNMP Set Operations	98
Configuring Your Managed Systems to Send Traps to IT Assistant	98
Configuring the SNMP Agent on Systems Running Supported NetWare Operating Systems	99
Changing the SNMP Community Name	99
Setting Up CIM	101
Setting Up CIM on Your Managed Systems	101
Index	105

Introducing 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.

Identifying the Groups of Systems for Remote Management

IT Assistant performs basic 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 is the Microsoft® Database Engine (MSDE) 2000. Users who require a more powerful database can use Microsoft SQL Server.

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 the 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 PowerConnect™, and Digital Keyboard/Video/Mouse (KVM).

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 is 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 device card in all servers 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, or run command line tasks on any systems in your managed group. IT Assistant allows you to load Dell Update Packages and System Update Sets into a central repository, and then run a compliance check against servers 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."

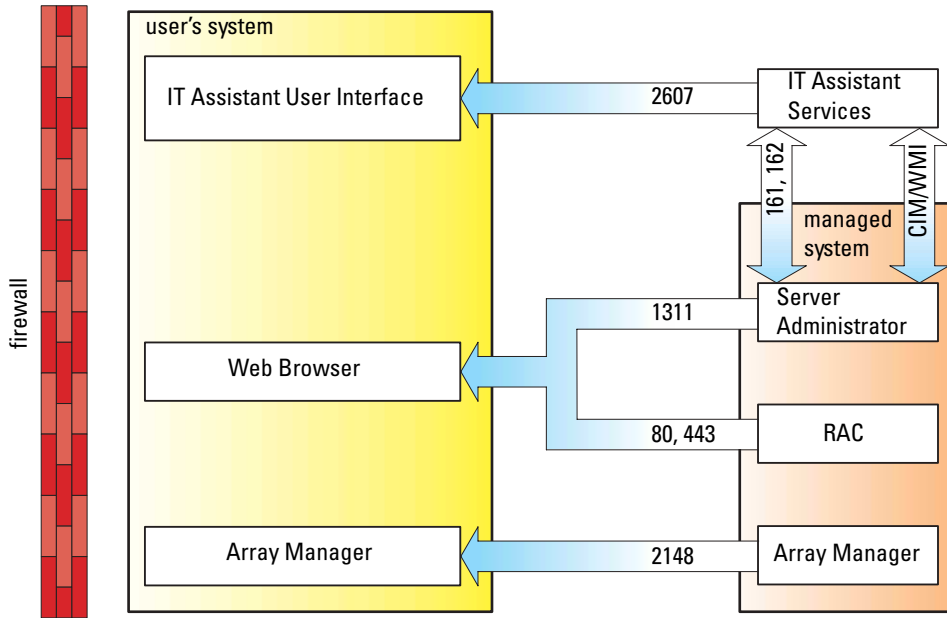
Understanding IT Assistant's Components

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

- IT Assistant 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.

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 Java technology. Remote access is through either a Web browser (Internet Explorer on Microsoft Windows®, and Mozilla or Firefox on Red Hat® Enterprise Linux systems) 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 SNMP agent on a managed system, trap destinations for the SNMP service must point to the host name or IP address 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.

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 menu bar options have changed, so previous users should take some time to familiarize themselves 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 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 below) and Dell OpenManage Client Instrumentation 6.0 (and below) will not be discovered by IT Assistant.

New 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 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, PowerConnect, and Digital KVM (keyboard/video/mouse). 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 Microsoft Data Engine (MSDE) or 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
- 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 tasking 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, and command line execution.

To use the tasking 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 Simple Network Management Protocol (SNMP) and Common Information Model (CIM) 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 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 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 logon 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.

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 on 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 SNMP management information base (MIB). The SNMP 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 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.

Planning Your 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 only 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 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 2-4 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 (MSDE) 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 2-1.

Table 2-1. 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	Windows 2000 with SP4



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™ servers running Red Hat® Enterprise Linux operating systems. These servers can, however, launch IT Assistant through supported browsers (Mozilla version 1.7.3 and later, and Firefox version 1.0.1 or later).

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, and status polls
- Are running Microsoft SQL Server tuned to maximum performance

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


Table 2-2. 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	as much as 5 GB

 **NOTE:** The amount of disk space needed may increase if you import numerous Update Packages.

Selecting the MSDE Default Database or SQL 2000 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 you use with IT Assistant. If you will be managing fewer than 500 systems, the SQL Server-compliant default database that ships with IT Assistant, Microsoft Data Engine (MSDE) 2000, 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. In addition, if you are performing frequent discoveries or status polls, you may benefit by the increased performance offered by SQL Server 2000 over MSDE 2000.

 **NOTE:** You can configure IT Assistant version 6.3 and later to use Microsoft SQL Server running on a remote, dedicated server instead of on the IT Assistant system. See the corresponding Dell white paper titled "Remote Microsoft SQL Server Use with IT Assistant Step-by-Step" at www.dell.com/openmanage.

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 by IT Assistant becomes unnecessary because e-mail notification is set up to occur whenever the event criteria are met.

Determining Systems Management Protocols

One of the most important decisions you will make in planning your IT Assistant installation is determining the protocols you will 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) or Common Information Model (CIM) protocols, these must also be configured in IT Assistant.

Supported Protocols

IT Assistant supports two systems management protocols: SNMP and CIM. 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 server management, it is strongly recommended that you enable and configure both 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.

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.

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, including portable computers, desktops, workstations, and standalone servers such as print and file servers, server modules (or blades), clustered servers, or hundreds of servers in densely populated racks. 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 2-3 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 below) and OMCI 6.0 (and below) will not be discovered by IT Assistant.

Table 2-3. Agents Supported by IT Assistant

Device	Version(s) Supported	Auto Discoverable	Alerting
Dell PowerEdge™ Agents*			
Server Administrator	1.0-2.2	Yes	Yes
Server Agent	4.2-4.5	Yes	Yes
Array Manager	2.5-3.7	Yes	Yes

Table 2-3. Agents Supported by IT Assistant (continued)

Device	Version(s) Supported	Auto Discoverable	Alerting
DRAC 4	1.0-1.30	Yes	Yes
DRAC III, DRAC III/XT	1.0-3.50	Yes	Yes
ERA, ERA/O	1.0-3.50	Yes	Yes
ERA/MC	1.0-3.50	Yes	Yes
PowerEdge 1655MC/1855MC Integrated Switch	N/A	Yes	Yes
* IT Assistant requires Server Administrator 2.0 or later for remote software updates.			
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
PowerVault 775N	N/A	Yes	Yes
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 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	Yes	Yes
PowerConnect 5316M	1.0.0.x	Yes	Yes
PowerConnect 5324	1.0.1.x	Yes	Yes
PowerConnect 6024	1.0.2.x	Yes	Yes
PowerConnect 6024F	1.0.2.x	Yes	Yes

Table 2-3. Agents Supported by IT Assistant (continued)

Device	Version(s) Supported	Auto Discoverable	Alerting
Digital KVM Agents			
2161 DS	N/A	Yes	Yes
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.x	Yes	Yes

Summary of Pre-Installation Decisions

This section has listed the major factors you must consider before installing and using IT Assistant to manage systems on your network. Table 2-4 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 2-4. 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 component of IT Assistant you are installing.	For a large network, install IT Assistant on a server-based operating system.	See the latest IT Assistant <code>readme.txt</code> either on the Dell Support website at support.dell.com or on the <i>Dell Systems Management Consoles</i> 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 IT Assistant components that will be installed on the system.		

Table 2-4. Pre-Installation Questions, Options, and Actions (continued)

Question	Option/Action	Option/Action	Next Step
Do I want to use the default installed database (MSDE) or should I install the Microsoft SQL Server database?	Generally, MSDE is adequate if you are managing fewer than 500 systems. However, heavy event traffic or other performance concerns may lead you to select SQL 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 IT Assistant" and "Configuring 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"

Installing, Uninstalling, and Upgrading 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 IT Assistant Installation" for more information.

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) 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/Remove Programs** icon.
This launches the **Add/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 and check **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/Remove Programs** window.
SNMP is now installed on your system.

IT Assistant is installable 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 Novell® NetWare® operating systems, see "Configuring Protocols to Send Information to 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 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 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 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 dependency is found, an information window is displayed and you may be prompted to install the required package.

- 2 If no 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 **Express** 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 **Express** 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 **Express**, skip to the last step.


- 5 Ensure that **IT Assistant** is checked from 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 **Express** 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.


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 dependencies, such as whether you have SNMP installed or have a supported database application. If a dependency is found, an information window is displayed and you may be prompted to install the required packages.

 **NOTE:** If you have IT Assistant version 6.x, install IT Assistant 7.0 before installing version 7.1 or later. The 7.0 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 7.0 or later, the installer installs IT Assistant 7.2 as a service pack.

- 3 If no 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 **Express** 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 **Express** installs all Dell OpenManage applications (including IT Assistant) with pre-selected default settings for location and port.


- 6 Ensure that **IT Assistant** is checked from 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 **Express** install option, this dialog does not appear.

- 8 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


- 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.

Uninstalling IT Assistant

To uninstall IT Assistant:

- 1 Click the **Start** button, point to **Settings**, and double-click **Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Select **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, make sure 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.

Remote Microsoft SQL Server and IT Assistant

See the white paper "Remote Microsoft SQL Server Use With IT Assistant Step-by-Step" at www.dell.com/openmanage, which describes how to configure IT Assistant version 6.3 and later to use Microsoft SQL Server running on a remote server as the IT Assistant database.

Configuring 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, portables, and workstations), servers, 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.

Ensure That Agents and Instrumentation Are Installed and Running

Whether large or small, all networks managed by IT Assistant share a basic requirement: all of the managed systems in the network must have Dell systems management agents (instrumentation) 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 portables) are contained in Dell OpenManage Client Instrumentation (OMCI).

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 these two agents are not installed, see the *Dell OpenManage Server Administrator* and *Dell OpenManage Client Instrumentation* documentation before continuing with IT Assistant configuration. If both are installed and running correctly, start IT Assistant and read on.


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 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 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 DNS 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 to be discovered and managed using SNMP protocol, ensure that:

- SNMP is installed.
- The name or IP address for the IT Assistant system is in the list under the **SNMP Service Properties** window → **Security** tab → **Accept SNMP packets from these hosts** radio button. This value needs to be configured on the managed system.
- If managed systems are going to send traps to IT Assistant, the host name or IP address of the IT Assistant system must be listed as the **Trap destination** on the **Traps** tab of the **SNMP Service Properties** window.
- Valid community names must be assigned on the **Traps** and **Security** tabs as appropriate in the **SNMP Service Properties** window.

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.

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 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 4-1. 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

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 credentials for authentication
- 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 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 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:

- 1 Select **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**, select when you want IT Assistant to perform discovery.

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

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

- 3 Under **Discovery Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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**, choose whether to discover **All Devices** or **Only Instrumented Devices**.

Jane 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**, select **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 Click **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:

- 1 Select **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**, select when you want IT Assistant to perform inventory.
Jane selects all seven days per week at 6:00:00 AM, a non-peak period for network traffic.
- 3 Under **Inventory Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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 Click OK.

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:

- 1 Select **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 Inventory**, select the interval that you want IT Assistant to use to perform status polling.
- 3 Under **Status Polling Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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 Click 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.

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

To identify an *include* range:

- 1 Select **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 Expand **Discovery Ranges**, right-click **Include Ranges** and select **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, enter an IP address (or range) or host name and click **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.

- 4 In Step 2 of the wizard, use the default values for Internet Control Message Protocol (ICMP) time-out and retry for the range. Use the **Troubleshooting Tool** to determine these values.

- 5 In Step 3 of the wizard, configure the **SNMP** parameters to be used during discovery:

- Make sure the **Enable SNMP Discovery** option is selected.
- Enter 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** 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 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, 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.


- Enter 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, including shutting down, configuring alert actions, 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.

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.

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

6 In Step 4 of the wizard, configure the CIM parameters to be used during discovery.

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

- Make sure **Enable CIM Discovery** is selected.
- In **Domain\User Name**, enter the same name you used to configure CIM on the managed system.
- Enter the same **Password** you used for the CIM password on the managed system.

7 In Step 5 of the wizard, choose what action IT Assistant will take upon completion of the wizard.

8 In Step 6 of the wizard, review your selections and choose **Finish** to complete the wizard or **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 setting 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 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 Action Alert 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 check **Select All**, or select the categories of events to include in the alert filter.

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

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




Jane checks **Servers and Network Devices**.

- 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.
- 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 Select **Alerts**→**Actions** from the menu bar.
- 2 Right-click **Alert Actions** in the navigation and select **New Alert Action**.
The **Add Alert Action Wizard** appears.
- 3 Give the action a logical name in the **Name** field.
- 4 From the **Type** pull-down menu, choose **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 and 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, specify 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.
- 6 In **Alert Filter Associations**, identify the Action Alert filter that will trigger this e-mail.
In Jane's case, 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 your selections. Click **Finish** to accept, or **Back** to make changes.
Verify that the name of the Alert Action you assigned in step 3 appears in the **Summary of Alert Actions** window.

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 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 systems, 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 business, 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 Cycle


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'll also enable CIM (like Jane).

To configure the discovery cycle 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 public (Get) and private (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 4-2. 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 public and private 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 private 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 4-2 provides information about the remote systems that Tom is monitoring.

Table 4-2. 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	Public/Private Community Names	Number of Servers on Subnet	Longest Ping Response Time Observed on Subnet
Data Center Servers 1	192.166.153.*	192.166.153.2	dcp123/dcsecure01	100	64
Data Center Servers 2	192.166.154.*	examplehost	dcp123/dcsecure02	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

Table 4-2. Example Subnet Ranges, IP Addresses, or Host Names and Corresponding Information for Data Center and Remote Servers (continued)

System Group Name	Include Subnet Range	Exclude Hosts or Subnet Range	Public/Private Community Names	Number of Servers on Subnet	Longest Ping Response Time Observed on Subnet
Data Center Servers 8	192.166.160.*		dcp123/dcexprivall	100	59
Data Center Servers 9	192.166.161.*		dcp123/dcexprivall	50	128
Remote Servers 1	10.9.72.*		dcp123/dcexprivrem	50	5600
Remote Servers 2	10.9.73.*		dcp123/dcexprivrem	100	2400

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 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 the corresponding 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:

- 1** Select **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**, select when you want 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. Network traffic is the lightest at this time.
- 3** Under **Discovery Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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 system performance while he is attempting to perform other tasks on the system, he can change the **Discovery Speed** to consume fewer network resources.
- 4** Under **Discover**, choose whether to discover all devices or only instrumented devices.
- 5** Under **Name Resolution**, 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** Click **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:

- 1 Select **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**, select when you want IT Assistant to perform inventory.
Tom sets inventory for weekly on Saturday at 3:00 a.m.
- 3 Under **Inventory Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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 Click OK.

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:

- 1 Select **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 Inventory**, select the interval you want IT Assistant to use to perform status polling.
- 3 Under **Status Polling Speed**, use the sliding bar to indicate how much network bandwidth and system resources you want 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 Click 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 4-2).

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:

- 1 Select **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 Expand **Discovery Ranges**, right-click **Include Ranges** and select **New Include Range**.

The **New Discovery Wizard** starts.


- 3 In Step 1 of the wizard, enter an IP address (or range) or host name and click **Next** to go to the next step.

Based on the info about Tom's systems in Table 4-2, he must complete this wizard twice to include all this systems. The first time, he enters:

192.166.153-161.*

The second time, he enters:

10.9.72-73.*

 **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, enter Internet Control Message Protocol (ICMP) time-out and retry values for the range.
- 5 In Step 3 of the wizard, configure the SNMP parameters to be used during discovery:
 - Make sure the **Enable SNMP Discovery** option is selected.
 - Enter 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.


- Enter 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.

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

6 In Step 4 of the wizard, configure the CIM parameters to be used during discovery.

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

- Make sure **Enable CIM Discovery** is selected.
- In **Domain/User Name**, enter the same name that you used to configure CIM on the managed system.
- Enter the same **Password** that you used for the CIM password on the managed system.

7 In Step 5 of the wizard, choose what action IT Assistant will take upon completion of the wizard.

8 In Step 6 of the wizard, review your selections and choose **Finish** to complete the wizard or **Back** to change your selections.

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 He expands **Discovery Ranges**, right-clicks **Exclude Ranges** and selects **New Exclude Range**.
The **New Exclude Range** dialog box appears.
- 3 He 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 three 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 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 technicians 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, select **Views**→**Devices**.
- 2 Right-click the top-level root in the IT Assistant navigation tree and select **New Group**.
The **Add Group Wizard** appears.
- 3 Enter a name and description for the group you want to add.
Tom names the group **Datacenter Servers**.
- 4 In the **Group Membership** dialog, either select the devices to include in the new group or, if a query-based group, select the query from the pull-down menu.
- 5 Review your selections in the summary screen and choose **Finish** to complete the wizard or **Back** to change your selections.
- 6 Repeat 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:

- 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 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 a filter 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 (Saturday and Sunday, 24 hours)

- 3 Enter 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**, select the severity of the events for which you want to receive alerts and logs.

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

Click **Next**.

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

Tom checks **Select All** because he wants to monitor all of the servers in his enterprise.

- 6 Under **Device/Group Configuration**, select 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.

- 7 Under **Date/Time Range Configuration**, enter 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 enables the time range 12:00:00 A.M. to 12:00:00 P.M. and enables the days Saturday and Sunday.

- 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.

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.

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

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

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 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, 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**.

Creating an Alert Action

To create an alert action:

- 1 Select **Alerts**→ **Actions** from the menu bar.
- 2 Right-click **Alert Actions** in the navigation and select **New Alert Action**.
The **Add Alert Action Wizard** appears.


3 Give 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, choose **Email**.

5 In the **E-mail Configuration** dialog, specify 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.

6 In **Alert Filter Association**, identify 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 your selections. Click **Finish** to accept, or **Back** to make changes.

Verify that the Alert Action you 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.

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.

Reporting and Task Management

Dell OpenManage™ IT Assistant provides the ability to:

- Create customized reports for all systems in your enterprise
- Perform command line execution on managed devices from a central console, including shutdown and wake up
- Perform software compliance checking and updates on an individual managed system

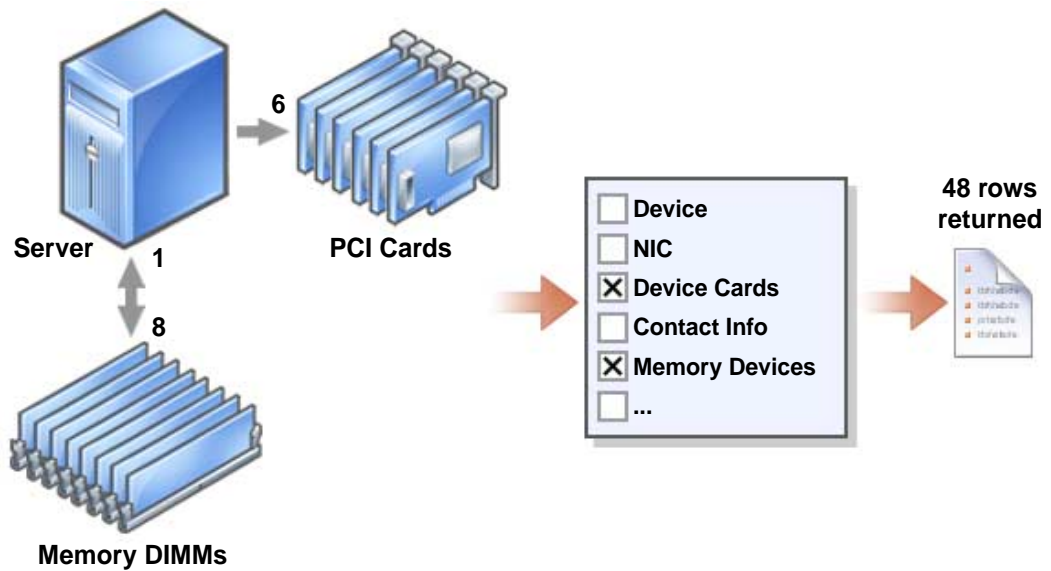
The basics of these capabilities are shown here using the same user scenarios presented in "Configuring IT Assistant to Monitor Your Systems." For more detailed information on these topics, see the IT Assistant online help.

Custom Reporting

IT Assistant uses data from the Microsoft® Data Engine (MSDE) or 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 5-1. 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 on **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**

3 In this case, she will choose **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.

4 Under **Select Attributes**, she chooses **NIC**.

5 Then, she specifies a preferred **Sort by** order.

6 At **Summary**, she either accepts her choices or goes back and changes them.

7 When she 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-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 5-1. Query Report Parameters

Name of the Query	Specifies the name of the query.
Query Criteria	<p>Specifies the query criteria. For example, to create a new query with the query criteria for all devices that correspond to a subnet, specify:</p> <pre>Where: IP Address Starts With 143.166.155</pre> <p>The query operators are:</p> <ul style="list-style-type: none">• 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. <p>You can expand the query with up to 10 subqueries, which together constitute the complete query. You join the subqueries by using AND/OR operators.</p> <p>NOTE: If you make any changes while editing an existing query and save that query, the original query is replaced.</p>
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
- 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

The rows in the Device table represent the devices in the network. 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 5-2. 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	ComputerSystemName
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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
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 is 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	Foreign Key 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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.
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 DRAC II = 5 Array 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 to the management application (if the agent supports a Web address).
AgentData	ntext	16	Yes	Extended agent data; for internal use only.
ArrayDisk Table				
DeviceId*	int	4	No	Foreign Key to the Device Table.
ArrayDiskNumber*	int	4	No	The instance number of this array disk entry.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
ArrayDiskName	nvarchar	256	Yes	The array disk's name as represented in Storage Management.
ArrayDiskVendorName	nvarchar	64	Yes	The array disk's reseller'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.
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.
ArrayDiskChannel	int	4	Yes	The bus to which this array disk is connected.
ArrayDiskLength	int	4	Yes	The array disk's size in megabytes. If the size is 0, it is smaller than a megabyte.
ArrayDiskBusType	nvarchar	64	Yes	The array disk's bus type. Possible values: SCSI, IDE, Fibre Channel, SSA, USB, 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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
Enclosure Table				
DeviceId*	int	4	No	The foreign key to the Device Table.
EnclosureNumber*	int	4	No	The instance 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.
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.
EnclosureProductId	nvarchar	64	Yes	The enclosure's product identification, which also corresponds to the enclosure type.
EnclosureType	nvarchar	64	Yes	The type 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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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 megabytes.
VirtualDiskWritePolicy	nvarchar	64	Yes	Indicates whether the controller's write cache will be used when writing to a virtual disk.
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.
VirtualDiskTargetId	int	4	Yes	Unique ID for the virtual disk.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
OSRevision	nvarchar	64	Yes	The revision of the operating system (for example, the Microsoft Windows® service pack or the Linux kernel version)
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.
ProcessorCores	int	4	Yes	This attribute defines the number of processor cores detected for the processor device.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.
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 controller is enabled, auto, or read-only.
BuiltinPointingDevice	nvarchar	64	Yes	Defines whether the built-in pointing device (mouse) port is enabled or disabled.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
WakeupOnLAN	nvarchar	64	Yes	Defines whether Wakeup 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 Wakeup 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 (0-23).
BootSequence	nvarchar	64	Yes	Defines the boot sequence for the next system boot.
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
PCISlots	nvarchar	64	Yes	The status of the system's add-in 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.
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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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 5-2. 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 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 name.
BoxAssetTagName	nvarchar	64	Yes	The device's asset tag.
BoxSystemName	nvarchar	64	Yes	The device's operating system 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.

Table 5-2. IT Assistant Database Schema (continued)

Column Name	Data Type	Data Size	Nulls Allowed	Description
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.
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.

Software Updates

IT Assistant provides a centralized software update capability. You can load Dell Update Packages and System Update Sets into a central 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 Update Packages designed to enable package sequencing and minimize system reboots. Dell Update Packages are available from the Dell Support website at support.dell.com or from the *Dell PowerEdge Updates* CD. This CD is available through the Dell OpenManage Subscription Service or as an ISO image downloaded from support.dell.com. You can download the OpenManage Subscription Service can be ordered from www.dell.com.

The *Dell PowerEdge Updates* 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 Navigate to **Manage**→ **Software Updates**.
- 2 Right-click the root node (**Software Update Repositories**) and select **Open Repository (Update CD)....**"
- 3 Insert the *Dell PowerEdge Updates* CD into the CD drive.
- 4 Navigate to the CD location and locate the repository directory.
- 5 Select **catalog.xml** and click **Open**.
The contents of the *Dell PowerEdge Updates* CD will be available within IT Assistant. You can then perform operations like 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 it 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 do it:

- 1 Select **Manage**→ **Software Updates**.
- 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. The package may be a **catalog.xml** file or another filename on a CD. When she highlights the filename and clicks **Open**, IT Assistant adds it 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 a specific group of devices (or a query) to check the package against.

- 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 an iconic representation of the differences found, full version information on the devices she chose, and other information that can help her identify out-of-compliance systems or devices.
- 6 If IT Assistant finds servers or devices that need updating, Jane can select which ones 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.

Managing Tasks

IT Assistant also allows you to 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



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 IT Assistant online help.

Creating a Device Control Task

For instance, Jane wants to reboot a troublesome server that has issued several e-mail alerts through IT Assistant. To perform this task 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 starts.
- 3 Jane enters a **Task Name**, then chooses **Shutdown Device** from the **Task Type** pull-down menu.
- 4 She chooses **Reboot** from the **Select Shutdown Type** window.
- 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 At 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 IT Assistant online help.

IPMI Command Line

Choosing **IPMI Command Line** from the pull-down menu allows you to execute IPM 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.


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>`. The default port number is 2607. 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. The user is 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 to 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. Perform the same 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 on **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.

ASF and the SNMP Protocol

A final security consideration, starting with Dell™ OptiPlex™ GX260 systems, is the integrated Network Interface Controller (NIC) that provides support for Alert Standard Format (ASF). 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 Novell® NetWare®.

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 ID/password) authentication. In addition, communication to managed system is established through the domain/user ID/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 Linux and Novell NetWare 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 address or name of the system running IT Assistant.



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. You can also limit user access using the Server Administrator CLI command `omconfig preferences useraccess enable= admin`. See the *Server Administrator Command Line Interface User's Guide* on 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.
- Use the SNMP and CIM (Server Administrator) protocol.
- 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 SQL Server database is detected when IT Assistant is installed, the process installs a copy of MSDE 2000, 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 or account password was set to either `null` or `de11`. 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.

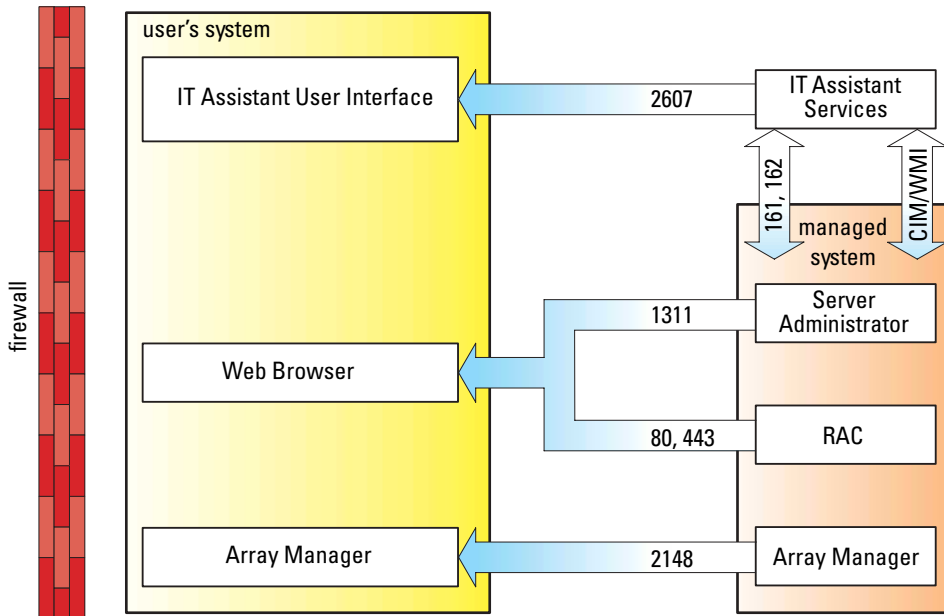
Running IT Assistant Behind a Firewall

Figure 6-1 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.

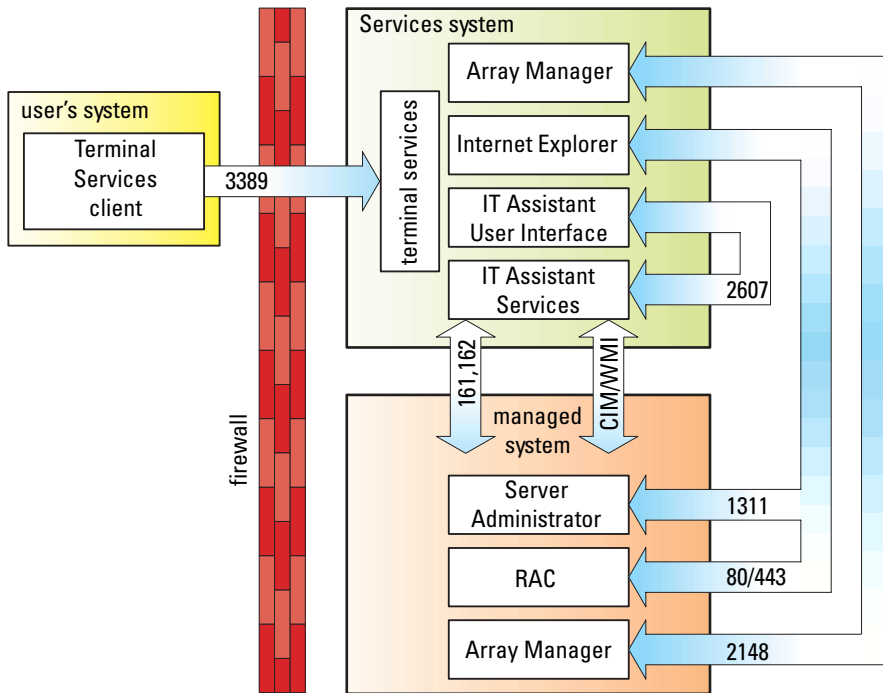
Figure 6-1. Typical Installation Behind a Firewall



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 6-2.

Figure 6-2. Using Terminal Services for Additional Security



In Figure 6-2, 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, 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 logon 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 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 into IT Assistant on a system running Windows Server 2003 due to operating system constraints.

- 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 into IT Assistant with the user privileges for their assigned group.

Creating Users and Assigning User Privileges for Supported Windows 2000 Operating Systems

- 🔧 **NOTE:** For questions about creating users and assigning user group privileges or for more detailed instructions, see your operating system documentation.

- 1 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 into IT Assistant on a system running Windows Server 2003 due to operating system constraints.

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 Click the name of the user you want to add, and then click **Add**.


10 Click **Check Names** to validate the user name that you are adding.

11 Click **OK**.

New users can log into 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.

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 into 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.

Configuring Protocols to Send Information to 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™ 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
Novell® NetWare® operating system	Always installed.	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, Novell NetWare, and Red Hat 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 an assigned read/write and read-only community names. 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.

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/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 Names** 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 Red Hat Linux 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.

Change 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
```

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`, 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, you must comment out the `sysContact` and `sysLocation` values in the Red Hat Enterprise Linux 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`, 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.

Configuring the SNMP Agent on Systems Running Supported NetWare Operating Systems

Managed system agents such as Server Administrator use the SNMP services provided by the NetWare SNMP agent. You can configure the SNMP agent to change the community name, enable Set operations, and send traps to a Services system. To configure your SNMP agent for proper interaction with IT Assistant, perform the tasks in the following sections.

 **NOTE:** See your operating system documentation for additional details on SNMP configuration.

 **NOTE:** All community names are case sensitive.


Changing the SNMP Community Name

The SNMP community name used by IT Assistant must match the SNMP community name configured on all managed systems. This is required for IT Assistant to retrieve management information from Server Administrator and any other supported agents.

To change the SNMP community name on a managed system, perform the following steps:

- 1 At the NetWare command line console, type `inetcfg` and press <Enter>.

The **Internetworking Configuration** menu appears.

 **NOTE:** If this is the first time you are using the `inetcfg` command, you may be prompted with the question: Do you want to transfer LAN drivers, protocol, and remote access commands? Dell recommends that you answer **Yes** to this message. For additional information regarding this prompt, see the Novell website. When you choose **Yes**, the system will force a restart. After the system restarts, return to the console and type the `inetcfg` command again. A screen pop-up will appear with the following prompt: Do you want to use the fast setup method or the standard method? Dell recommends you select the standard method to perform SNMP setup. After selecting the standard method see the next step below.

- 2 Select **Manage Configuration**.

The **Manage Configuration** menu appears.

- 3 Select **Configure SNMP Parameters**.

The **SNMP Parameters** menu appears.

- 4 Select **Monitor State** to configure the read (or Get) community name.

The **Monitor Community Handling** menu appears with the following options:

- Any Community May Read
- Leave as Default Setting
- No Community May Read
- Specified Community May Read

 **NOTE:** Press <F1> for more information about **Monitor State**. Press <Esc> to clear the help window.

5 Select **Specified Community May Read**.

6 Under **Monitor Community**, enter the read community name.

7 Select **Control State** to configure the write (or set) community name.

The **Control Community Handling** menu appears with the following options:

- Any Community May Write
- Leave as Default Setting
- No Community May Write
- Specified Community May Write

 **NOTE:** Press <F1> for more information about **Control State**. Press <Esc> to clear the help window.

8 Select **Specified Community May Write**.

9 Under **Control Community**, enter the write community name.


10 Select **Trap State** to configure trap community handling.

The **Trap Handling** menu choices appears with the following options:

- Do Not Send Traps
- Leave as Default Setting
- Send Traps With Specified Community

11 Select **Send Traps With Specified Community**.

12 Under **Trap Community**, enter the community name you wish the traps to have.

 **NOTE:** : Press <F1> for more information about **Trap State**. Press <Esc> to clear the help window.

13 Press <Esc> to exit the **SNMP Parameters** menu.

A message box appears, prompting you to save changes.

14 Select **Yes**.

The **Manage Configuration** menu appears.

15 Press <Esc> to exit the **Manage Configuration** menu.

The **Internetworking Configuration** menu appears.

16 Select **Protocols**.

The **Protocol Configuration** menu appears.

17 Select the **TCP/IP**.

The **TCP/IP Protocol Configuration** menu appears.

18 Select **SNMP Manager Table**.

The **SNMP Manager Table** menu appears with the following options:

- Press <Ins> to add SNMP trap destinations.
- Press <Enter> to modify SNMP trap destinations.
- Press to delete SNMP trap destinations.

 **NOTE:** Press <F1> for more information about **SNMP Manager Table**. Press <Esc> to clear the help window.

19 Select one of the **SNMP Manager Table** menu options.

20 Press <Esc> to exit the **SNMP Manager Table** menu.

A message box appears, prompting you to update the database.

21 Select **Yes**.

The **TCP/IP Protocol Configuration** menu appears.

22 Press <Esc> twice to exit the **TCP/IP Protocol Configuration** menu.

The **Internetworking Configuration** menu appears.

23 Restart your system to make the configuration changes active.

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.


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 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.

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.

Index

A

- adding users, 90
- agents on systems, 21
- alert filters, 10
- ASF, 82

C

- CIM, 34, 93
- configuring
 - discovery cycle, 44
 - discovery ranges, 40, 49
 - discovery settings, 38, 47
 - inventory settings, 39, 48
 - SNMP, 45, 93
 - status polling settings, 39, 48
 - system to send SNMP traps, 96
- creating
 - alert action, 43, 54
 - alert action filter, 42, 53
 - custom groups, 52
 - device control task, 78
 - reports, 59
 - users, 89
- custom reporting, 57

D

- database schema information, 61
- disabling users, 91
- DMI support, 12

E

- e-mail notification, 20
- enabling SNMP, 96

G

- generic command line, 79

H

- hardware configuration, 19

I

- installation prerequisites, 17
 - database, 19
 - operating system, 18
 - summary, 23
 - systems management protocols, 20

installing

- IT Assistant, 27
- SNMP, 25
- IPMI command line, 79
- IT Assistant components
 - IT Assistant system, 12
 - managed system, 12
 - services, 11
 - user interface, 11
- IT Assistant features, 12
 - application launch, 13
 - dynamic groups, 13
 - enhanced inventory cycle, 14
 - managing tasks, 14
 - native install, 12
 - reporting, 13
 - single sign-on, 15
 - software updates, 14
 - topology view, 12
 - troubleshooting tool, 14
 - user authentication, 14
 - user preferences, 15

M

- managing tasks, 78
- MSDE, 19

N

network management
station, 10, 12, 32

R

RBAC, 26, 32

remote client

instrumentation
command line, 79

remote management
identifying groups, 9

Remote Microsoft SQL Server
and IT Assistant, 29

reports

creating, 59
customized reports, 10
editing, deleting, running, 60
pre-defined, 60

S

securing managed
systems, 81-82

security and IT Assistant, 85

security and SNMP, 83

single sign-on, 87

SNMP, 33, 37, 93

best practices, 33
optimal configuration, 34

software update, 79

software updates, 77

SQL server, 19

starting IT Assistant, 32

systems management
protocol, 20
CIM, 20
SNMP, 20

systems you want to
monitor, 21

T

tasks

enable configuration
management, 10

U

uninstalling IT Assistant, 29

user privileges, 88

users

adding, 90
creating, 89
disabling, 91

using IT Assistant, 37

using software updates, 77

V

views of systems, 9

W

Windows authentication, 88