HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

Getting Started Guide

FastFind Links

Hitachi Data Systems

MK-98IOS001-15

Contents

Preface

Congratulations on acquiring Hitachi IT Operations Analyzer, a component of Hitachi IT Operations. Your organization has a powerful and flexible network monitoring and proactive status reporting tool.

This guide will assist you with the pre-installation process, and the installation through the initial discovery of your environment. It provides information about post-discovery tasks and the documentation that you can reference to complete them.

This preface includes the following information:

Intended audience

This document is intended for system administrators and other users who are responsible for installing, configuring, and operating IT Operations Analyzer.

Product version

This document revision applies to IT Operations Analyzer version 3.3.1.

Document revision level

This section provides a history of the revisions to this document.

Revision	Date	Description
MK-98IOS001-00	April 2009	Initial Release
MK-98IOS001-01	June 2009	Revision 1, supersedes and replaces MK-98IOS001-00
MK-98IOS001-02	August 2009	Revision 2, supersedes and replaces MK-98IOS001-01
MK-98IOS001-03	August 2009	Revision 3, supersedes and replaces MK-98IOS001-02
MK-98IOS001-04	March 2010	Revision 4, supersedes and replaces MK-98IOS001-03
MK-98IOS001-05	March 2010	Revision 5, supersedes and replaces MK-98IOS001-04
MK-98IOS001-06	October 2010	Revision 6, supersedes and replaces MK-98IOS001-05
MK-98IOS001-07	January 2011	Revision 7, supersedes and replaces MK-98IOS001-06
MK-98IOS001-08	April 2011	Revision 8, supersedes and replaces MK-98IOS001-07
MK-98IOS001-09	October 2011	Revision 9, supersedes and replaces MK-98IOS001-08
MK-98IOS001-10	February 2012	Revision 10, supersedes and replaces MK-98IOS001-09
MK-98IOS001-11	July 2012	Revision 11, supersedes and replaces MK-98IOS001-10
MK-98IOS001-12	November 2012	Revision 12, supersedes and replaces MK-98IOS001-11
MK-98IOS001-13	March 2013	Revision 13, supersedes and replaces MK-98IOS001-12
MK-98IOS001-14	June 2013	Revision 14, supersedes and replaces MK-98IOS001-13
MK-98IOS001-15	July 2013	Revision 15 supersedes and replaces MK-98IOS001-14

Related documents

- *Hitachi IT Operations Analyzer Getting Started Guide: Device Configuration Supplement*, MK-90IOS006
- *Hitachi IT Operations Analyzer Help*
- *Hitachi IT Operations Analyzer Release Notes,* RN-99IOS004
- *Hitachi IT Operations Repository Getting Started Guide,* MK-90IOS034

Document conventions

The following symbols are used to alert you to important information.

Symbol	Meaning	Description
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Note	Notes emphasize or supplement important points of the main text.
	CAUTION	Cautions indicate that failure to take a specified action could result in damage to the software or hardware.

The following typographic conventions are used in this document.

Convention	Description
Bold	Indicates text in a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. In the case of version information, the italic x represents all subsequent versions. Examples: • Copy *source-file target-file*. • Kernel version 2.6.*x*. **Note**: Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or is entered by the user. Example: `# pairdisplay -g oradb`
angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` **Note**: Italic font is also used to indicate variables.

Product references

In this manual, there are references to VMware® products. Those references are handled as follows:

- Reference to the product when the type/version is specific; for example: VMware ESX 3, VMware ESX 3i, VMware ESX 4.0, etc.
- Reference to the product server when the server type/version is non-specific: ESX Server

IT Operations Software Portal

Your site has online access to product-related and other information and resources, through the IT Operations Software Portal:

http://www.itoperations.com

The IT Operations Software Portal provides a knowledge base that includes technical and configuration resources, and it includes product-related downloads and updates:

- By registering on the IT Operations Software Portal, you can access the knowledge base, FAQs, forums and videos.
- If your organization has a valid Software Maintenance, then it can download updates.

Getting help

If you encounter any problems with the software installation or discovery notification, please refer to the Troubleshooting chapter of this guide.

If the issue you are experiencing is not addressed by the troubleshooting procedures, and if you purchased this product and have a current product support agreement, then please collect the following information:

- The product name and version number
- The operating system name and revision or service pack number
- The serial number of the license for which you are requesting help
- The content of any error messages that are displayed
- The circumstances surrounding the error or failure
- A description of the problem and what has been done to try to solve it

After you collect this data, contact the Hitachi Data Systems Support Center.

Following is a link to the Hitachi Data Systems Web site, where you can obtain current telephone numbers and other contact information for the Hitachi Data Systems Support Center:

https://portal.hds.com

NOTE: If you are working with a trial version of the product, then please refer to the self-service materials that are located on the IT Operations Software Portal.

Comments

Please send us your comments about this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

1

Overview

This chapter provides an outline of the basic steps that you will complete to prepare your environment for the installation, install the software, and begin working with IT Operations Analyzer.

- Reviewing the getting started process
- Referring to the IT Operations Software Portal

Reviewing the getting started process

There are five basic steps that you will complete to set up your environment and begin monitoring. Chapter 2 and subsequent chapters in this guide provides task details, in the recommended order of completion:

1. **Prepare your environment for the installation**.

   Verify the settings that are used in your environment, and collect information that will be necessary later on, during the setup procedures.

   If you need to make adjustments, such as preparing SNMP for IP switches, then refer to the *Hitachi IT Operations Analyzer Getting Started Guide: Device Configuration Supplement* for guidance.

2. **Install IT Operations Analyzer**.

   You will install the software on a Microsoft Windows® server. (In this manual, it is referred to as the management server.) You will use an Installation Wizard to specify the URL of your management server and other data, such as the location of installation files.

3. **Activate your license**.

   Depending on the type of license, your site can experience the benefits of monitoring with the IT Operations Analyzer for a limited time, or it will be able to continuously monitor nodes. In either case, no monitoring or other activities can begin without activating the license. You will use the License Activation wizard to complete the process.

4. **Log in and complete initial setup tasks**.

   For security, you will change the built-in account password, and you will add accounts for other administrators who will be working with the software.

5. **Discover and Monitor your environment**.

   Use the Interactive Discovery Wizard to point IT Operations Analyzer to the location of the servers, storage, and switches that you want to monitor. When all discovery steps are complete, you can view the status of monitored nodes in the Monitoring module.

NOTE: Additional device support is available by installing and using plug-ins. If your site intends to use plug-ins, additional steps in the getting started process are necessary. For more information, refer to the IT Operations Software Portal.

Referring to the IT Operations Software Portal

The IT Operations Software Portal provides you with online access to product-related and other information, such as product literature and support and technical references: http://www.itoperations.com

2

Setup and installation

This chapter describes the environment and data collection preparations that are necessary before completing the product installation. It also provides installation information.

- Overview
- Preparing your environment
- Obtaining environment information
- Installing the software
- Migrating from an IT Operations Analyzer 32-bit version to a 64-bit version

Overview

Before installing IT Operations Analyzer or using the Discovery Wizard, it is important to check your environment and gather the information that you will be prompted to provide. This involves:

Preparing your environment:

- Preparing the server on which the software will be installed (the management server).
- Preparing the servers, storage, and switches that you intend to monitor (your monitoring targets).
- Completing any additional tasks, based on environment-specific components and attributes, such as your current firewall settings and VMware® usage.
- Gathering the access protocol credentials for each monitoring target (IP addresses, ports, namespace, and so on).
- Gathering credentials information for each monitoring target (NT user ID and password).

Obtaining information about your environment, such as:

- Mail server access information; for example, the SMTP server name and port. This information is required in order for IT Operations Analyzer to send e-mail notifications when the discovery of your environment is finished.
- User information; for example, the names, job functions, and e-mail addresses of the administrators at your site who will be working with the software.

Verifying information about your environment, such as the:

- Windows Installer service. For the Windows Installer service, confirm that the [Startup type] is not [Disabled].
- Processing load. In frequently-accessed environments, such as a domain controller, the processing load is already very high, which may impact the ability to process other tasks. Therefore, we do not recommend installing IT Operations Analyzer to environments such a domain controller.
- Available disk space. The disk space that is required for the software installation is related to the number of nodes that your site plans to monitor. Check that you have sufficient space for your monitoring needs.
- Host names. The identity of Microsoft Windows, Microsoft Hyper-V, Linux, and Solaris nodes is determined by the host name. As a result, IT Operations Analyzer cannot simultaneously monitor multiple servers that have the same host name. In preparation for the Discovery process, identify only the server you intend to monitor.
- Port number settings. If a network firewall separates the management server from the mail server or from the nodes you intend to monitor, then it must be configured to allow communication at designated ports.

By completing the tasks in this chapter, you help to ensure that the software installation is successful, and that the discovery process fully captures information about all of your monitoring targets. These checks also prevent discovery problems from occurring, which can originate from communication, credential, or port setting errors.

Preparing your environment

Table 2-1 describes required tasks (and some optional tasks based on your environment and monitoring objectives). Except for some references later in this chapter, the procedure details of each task are described in the *Hitachi IT Operations Analyzer Getting Started Guide: Device Configuration Supplement.*

NOTE: IT Operations Analyzer cannot be installed on the same server on which:

- IT Operations Repository is installed.
- IT Operations Integrator is installed.

Table 2-1: Environment Preparations

Required Tasks	
Task	**Details**
Setting up the management server:	The management server is the machine on which IT Operations Analyzer is installed. It must meet certain operating system and disk space requirements.
• Verify the installed operating system	• Microsoft Windows Server 2003 (Service Pack 1 or later) • Microsoft Windows Server 2003 R2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 Microsoft Windows Server (x86 and x64 editions) are supported. IPF is not supported. Also, Service Pack 2 (SP2) is recommended for use with Windows Server 2003 and Windows Server 2003 R2. There is no requirement for applying SP2 to Windows Server 2008 and Windows Server 2008 R2.
• Check for sufficient space	• Memory: 2 GB (minimum) • Processor: 2 GHz (minimum) • Available disk space: 20 GB These requirements apply to monitoring up to 250 nodes. The requirements change, however, based on whether fewer or more nodes are monitored. The processing speed depends on the type of CPU, such as Intel® Core™ Duo, AMD Athlon™, and so on. For details, see Planning for the required disk space.
• Check DCOM settings for WMI	Prevent WMI remote connection errors from occurring because remote execution of DCOM is not permitted.

Prepare the client machines:
• Verify the supported browser
	Client machines are used to connect to the management server using a browser.
	• Use either of the following browsers:
	  • Microsoft Internet Explorer 7, 8, 9 or 10 is recommended. Although version 6 is supported, there are known issues when printing reports. Refer to the product release notes for information. Because IT Operations Analyzer does not support Internet Explorer 10 for the new Windows Store interface, please use Internet Explorer 10 for the Desktop interface.
	  • Mozilla Firefox 3.5 or later

Table 2-1: Environment Preparations

• Check the installed media player	• Adobe® Flash® Player 10.0.42 or later is supported.
Required Tasks	
Task	**Details**
Set up monitoring targets: (If your site uses any of the monitoring targets listed below, you must set them up to ensure that they are correctly identified during the discovery process.)	Monitoring targets are the servers, storage, and switches that your site intends to monitor.
• Linux® servers	IT Operations Analyzer logs on to a Linux server and runs commands to monitor it, using SSH. Verify the supported OS: • Red Hat® Enterprise version 5.0, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 • Red Hat® Enterprise version 6.0, 6.1, 6.2, 6.3, 6.4 • SUSE® Linux Enterprise server 10 • SUSE® Linux Enterprise server 11 • SUSE® Linux Enterprise server 11 with Service Pack 1 • SUSE® Linux Enterprise server 11 with Service Pack 2 • Cent OS 6.0, 6.1, 6.2, 6.3 • Oracle Linux 6.0, 6.1, 6.2, 6.3 Determine the administrator login method, then complete the associated tasks: • For direct root login, obtain the root password. • For normal user and su root login, obtain the user ID for normal user, password for the user ID and the root password. • For normal user login and sudo, configure the sudo setting, and obtain the user ID for normal user and password for the user ID.
• Solaris® servers	IT Operations Analyzer logs on to a Solaris server and runs commands to monitor it, using SSH. Verify the supported OS: • Solaris 9 (Sun OS 5.9) SPARC 09/05 • Solaris 10 (Sun OS 5.10) SPARC 05/08 Determine the administrator login method, then complete the tasks: • For direct root login, obtain the root password. • For normal user and su root login, obtain the user ID for normal user, password for the user ID and the root password. • For normal user login and sudo, configure the pfexec setting, and obtain the user ID for normal user and password for the user ID.

Table 2-1: Environment Preparations

Required Tasks	
Task	**Details**
• Microsoft Windows servers	These servers are supported. **Note**: In Windows, the x86 and x64 editions do not support IPF. • Windows Server 2003 (x86 and x64 Edition) *1 • Windows Server 2003 R2 (x86 and x64 Edition) • Windows Storage Server 2003 *2 • Windows Storage Server 2003 R2 • Windows Server 2008 (x86 and x64 Edition) • Windows Server 2008 R2 • Windows Server (x86 and x64 Edition) • Windows Server 2012 • Hyper–V version1.0, 2.0, 3.0 *1 x86 is SP1 or later, x64 edition is only SP2 *2 SP1 or later
• IP Switches	IT Operations Analyzer uses SNMP to monitor IP switches. • Enable SNMP • Obtain the SNMP community string • Obtain the IP address
• Hitachi 9500V	IT Operations Analyzer monitors Hitachi 9500V through Device Manager's SMI-S agent. Performance is not monitored. Install Device Manager 5.9 or later and enable SMI-S.
• Hitachi USP VM	IT Operations Analyzer monitors Hitachi USP VM through Device Manager's SMI-S agent. Install Device Manager 6.2 or later and enable SMI-S.
• Hitachi Modular and Unified Storage	Verify the connection credentials: • Obtain the IP Address • Obtain the User ID and Password SSL connection is not supported.

• Other storage, FC switches	IT Operations Analyzer uses SMI-S to discover and monitor other storage and FC switches.
	Install the SMI-S agent, then obtain the following:
	• IP address
	  • SMI-S agent (proxy): Use an IP address of the SMI-S server for the switch.
	  • SMI-S agent (embedded): Use the same IP address for the FC switch.
	• User ID and Password
	• Port number
	• Namespace
	Also, check the SSL status. Specify either **https** or **http**.

Table 2-1: Environment Preparations

Required Tasks	
Task	**Details**
Configure firewall settings: Allow communication between the management server and the components listed on the right:	Communication among components must exist in order to complete the discover process and monitor nodes. • monitoring targets • mail server • client machines See Permitting communications through a firewall.
Gathering IP addresses and credentials:	IT Operations Analyzer requires an IP address range and credentials to discover nodes.
• Gather IP addresses	For each monitoring target, obtain the IP address (and IP address range) that will be scanned during the discovery process. **Note**: IPv6 is not supported.
• Gather credentials	For the monitoring targets that require it, obtain credential information, such as passwords.

Table 2-1: Environment Preparations

Recommended Tasks	
Task	**Details**
Check and configure the default ports for IT Operations Analyzer.	IT Operations Analyzer uses certain ports for client machine access and communications. If there are any conflicts (for example, you are using one of the specified ports), then use a different port number. Port conflicts prevent IT Operations Analyzer from performing correctly.
Check monitoring targets:	Each server type uses a different method for monitoring. Verify that the server type you are monitoring has these additional correct settings.
• Windows servers	IT Operations Analyzer uses WMI to monitor Windows servers. For remote access to WMI, DCOM must be enabled at the Windows server and at the management server. If DCOM is not enabled, then the software may be unable to discover or monitor Windows servers. Also, install the Integration Service on a virtual machine if your site will monitor a Hyper-V virtual machine. See Considering host names and IP Address Range settings.
• Linux/Solaris servers	IT Operations Analyzer uses SSH to discover Linux and Solaris servers. It also uses password authentication (not certificate authentication), to monitor them. Verify that: • SSH service is installed and running. • SSH2 connection is enabled. • Password authentication is permitted.
• VMware ESX Servers	IT Operations Analyzer cannot correctly monitor Windows or Linux servers on virtual machines unless VMware tools are installed. Verify the supported version: • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4 • VMware ESX 4i • VMware ESX 4.1 • VMware ESX 4.1i • VMware ESX 5 • VMware ESX 5i • VMware ESX 5.1 • VMware ESX 5.1i Also, install VMware Tools on virtual machines.
• Hitachi Modular and Unified Storage	If account authentication or password protection is enabled, then IT Operations Analyzer needs the User ID and Password. Check whether account authentication or password protection is enabled.

Table 2-1: Environment Preparations

Recommended Tasks	
Task	**Details**
• Dell™ servers	By using the built-in Dell Chassis plug-in, Dell server-specific information can be acquired. “Dell Chassis (Windows)” is installed as a plug-in for Windows and “Dell Chassis (Linux)” is installed as plug-in for Linux. Following are the system requirements for Dell servers that are monitored by Analyzer: • Dell OpenManage Server Administrator(OMSA) Versions 6.1.0 or 6.2.0 must be running on the monitored Dell server(s). • SNMP agent is installed and running on the monitored Dell server(s). • “Dell Chassis (Windows)” requires that the DSM SA Data Manager service is running on Microsoft Windows Server. • “Dell Chassis (Linux)” requires that the dsm_sa_datamgrd or dsm_sa_datamgr32d process is running on the Red Hat Enterprise Linux Server.
Optional Tasks	
Task	**Details**
Check monitoring targets:	
• Windows servers	IT Operations Analyzer uses WMI to monitor Windows servers. Windows 2003 must have FCInfo installed to provide FC HBA data through WMI. If your Windows servers use an FC HBA, then install FCInfo.
• IP Switches	Enable sending of SNMP traps. IT Operations Analyzer can receive SNMP traps from IP switches. This task is optional because IT Operations Analyzer can monitor IP switches without traps, by using polling.
• Hitachi Modular and Unified Storage	Enable the Performance feature. By default, the performance feature is disabled. IT Operations Analyzer can discover and monitor the storage, but not performance.

Obtaining environment information

When you use IT Operations Analyzer to discover your servers, storage, and switches, you will be asked to provide certain information. It is easier to complete the discovery process when you have collected this information, beforehand.

Gathering Mail Server access information

Toward the end of the discovery process, you will be given a choice to indicate a recipient for the discovery notification. The discovery notification is an e-mail status that is sent when the discovery process has ended, and the results of the discovered nodes are available.

If you plan to use this feature, then the following information is required:

- **SMTP Server** Note the settings that are associated with the mail server, such as the SMTP server name and port.
- **Secure Connection** To connect to the SMTP server using a secure connection, decide which security protocol that you want to use. The connection type will depend on the current SMTP server configuration. If you use authentication, authentication information such as the name of the administrator and the password are required.

Gathering information about administrator users

Based on the IT administrator support at your site, make a list of the following:

- The names of the administrators who will use IT Operations Analyzer.
- The access privileges that will be granted to each administrator, based on their job function (how the person will be working with the software). For example, administrators who will only be able to view information, and administrators who will be able to configure and modify information.

NOTE: For information about administrator permission levels within IT Operations Analyzer, see Table 4-3.

- The contact information for each administrator (e-mail address).

Planning for the communication speed

During the software installation, you can specify the communication speed between your monitoring targets and the management server. By default, the setting is 100 megabytes per second (100 Mbps) or less, but you can choose 1 gigabytes per second (1 Gbps) or more.

Following are some considerations for keeping the default setting or changing it:

100 Mbps or less When this setting is applied, IT Operations Analyzer controls the flow of data for the discovery processing of monitored devices and the information acquisition processing from monitored devices. With this option, when there are many monitored nodes, the processing performance may be less, compared with the 1 Gbps or more option, even though the management server is connected to a Wide LAN.

1 Gbps or more When this setting is applied, IT Operations Analyzer does not control the flow of data, and the processing performance is improved.

However, if the management server is connected to a LAN that has a limited communication bandwidth, such as 100 Mbps, and the monitored nodes are connected to a LAN with a greater communication bandwidth, such as 1 Gbps, then the acquired volume of information from the monitored nodes might exceed the bandwidth, especially when there is a large volume of monitored nodes. The consequence is that not all information may be received on the management server.

In this case, the recommended setting is 100 Mbps or less.

Planning for the required disk space

During the installation, you will be asked to specify the scale of your database (DB scale). The scale is determined by the number of nodes you plan to monitor, then the following:

Installation Disk Space + Database Disk Space + Trace Log Disk Space = Total Disk Space

So, if your site plans to monitor 250 nodes, a minimum of 20 GB of disk space is required. Note, however, that this total value may be higher, as described in the section after the table.

The following table outlines the disk space requirements that correspond to the number of monitored nodes. The values in the Monitored Nodes column are approximate.

Table 2-2: Disk Space Requirements Based on Monitored Nodes

Monitored Nodes	Disk Space (Install-ation)	Minimum Disk Space (Database)	Maximum Disk Space (Database)	Disk Space (Trace Log)	CPU	Memory (32-bit version)	Memory (64-bit version)
25	1 GB	7 GB	11 GB	2 GB	2 GHz	1 GB	• 12 GB (recommended) • 6 GB (required)
50		8 GB	13 GB	3 GB	2.4 GHz		
125		10 GB	24 GB	6 GB	2.8 GHz	2 GB	
250		13 GB	42 GB	8 GB	3.2 GHz		
500		23 GB	79 GB	17 GB	2 GHz (Quad)	3 GB	
750		33 GB	117 GB	17 GB		4 GB	• 16 GB (recommended) • 8 GB (required)
		43 GB	155 GB	74 GB			
Over 750							• 24 GB (recommended) • 12 GB (required)

NOTE: When planning for the scale of your database (DB scale), if you conclude that you'll want to monitor a larger amount of nodes, you may want consider using IT Operations Repository in addition to IT Operations Analyzer (this can help maintain performance with a very large database). For more information about IT Operations Repository, see the *Hitachi IT Operations Repository Getting Started Guide* or visit the IT Operations Software Portal: http://www.itoperations.com

Important planning notes

- Based on your current device configuration, your actual disk space requirements may be different. For example, if you plan to monitor a large volume of storage nodes, then the value in the Maximum Disk Space (Database) column may be insufficient, and may need to be increased.

- In the **Settings** module of IT Operations Analyzer, you can specify the time frame (start time and frequency) when IT Operations Analyzer should automatically acquire configuration, status, and/or performance information from the monitored nodes. This is called the **Monitoring Interval**. If, after the installation, you decrease this interval, the database storage capacity increases, even if the number of monitored nodes remains the same.
  If you plan on using the Monitoring Interval setting, then account for the required database disk space, as outlined in the Maximum Disk Space (Database) column.

NOTE: At some point after installing and working with the software, your site may need to increase the current number of monitored nodes (and upgrade the software license). In that case, you need to adjust the scale of the database, and the database storage destination, accordingly. You can use the database expansion command, expanddb.exe, to change that database information. The command usage and details are described in the online Help book, *Managing the IT Operations Analyzer Database*.

Considering host names and IP Address Range settings

The virtual IP address of a cluster cannot be used as a monitoring IP address for IT Operations Analyzer. When you monitor a cluster node, please use a physical IP address. Only with the Microsoft Cluster Service (MSCS) does IT Operations Analyzer exclude virtual IP addresses from the discovery. The discovery is completed for other cluster systems. When a virtual IP address is discovered, remove it from the discovered IP address range.

The identity of Microsoft Windows, Microsoft Hyper-V,Linux, and Solaris nodes is determined by the host name. As a result, IT Operations Analyzer cannot simultaneously monitor multiple servers that have the same host name. If your site has several servers that have the same host name, then during the discovery process, only specify the server you intend to monitor within the **Discovery Wizard's Specify IP Address Ranges**.

Permitting communications through a firewall

If a network firewall separates the management server from the mail server or from the nodes you intend to monitor, then it must be configured to allow communication at designated ports. This is particularly the case if the firewall was disabled before installing the software, then set to 'Enabled', afterward.

The following table lists the ports that are used by the management server, by default. (The exception is 20510/TCP for the Web browser and 162/UDP for the IP switch, which are configured during the installation of the software.)

Your site may use a combination of default and ephemeral ports. In order for monitoring information to be collected, the port that is used must permit communication through all paths between the management server, and the monitored nodes.

Table 2-3: Port Numbers for Use With a Firewall

Default Port	Communication From:	Communication To:
161/UDP	Management server	IP switch
162/UDP	IP switch	Management server
22/TCP	Management server	Linux/Solaris server
25/TCP	Management server	Mail server
135/TCP	Management server	Windows server
2000/TCP	Management server	Hitachi storage
5988/TCP	Management server	SMI-S server
5989/TCP	Management server	
80/TCP	Management server	VMware ESX Server
443/TCP	Management server	
20510/TCP	Web browser	Management server
20513/TCP	ODBC, JDBC client machine	IT Operations Analyzer management server
20515/TCP	ODBC, JDBC client machine	IT Operations Analyzer management server
ephemeral port range of JDBC, ODBC client machine	IT Operations Analyzer management server	ODBC, JDBC client machine **NOTE:** Specified in PDCLTRCVPORT within the RepositoryDB.ini file (for JDBC) or RepositorySystemDB.ini file (for ODBC). For the client machine, this is: (0 | n | n1-n2). n, n1, n2 is the value of 5001 to 65535.

NOTE: If needed, you can verify the port numbers that are currently in use, and you can change them. For information, refer to the online Help book, *Modifying Connection Settings*.

IT Operations Analyzer can detect the existence of devices using Ping (ICMP Echo) during the discovery process. To detect the existence of devices using Ping, configure the firewall to allow the ICMP Echo request.

Starting with Windows Server 2008, the Windows Firewall is configured to deny the ICMP Echo request, by default. Following is the procedure to configure the Windows Firewall to allow the ICMP Echo request.

NOTE: For the following instructions, on Windows Server 2012, navigation to the **Start** and **Run** options are different.

To configure the Windows Firewall to allow the ICMP Echo request:

1. After logging on to the Windows server, click **Start**, then **Run**.

2. At the prompt, type **cmd**, then click **OK**.
3. At the command prompt, type the following, then press **Enter**:

   netsh firewall set icmpsetting 8 enable

If you do not want to allow the ICMP Echo request, then configure the **Specify IP Address Ranges** panel of the IT Operations Analyzer's **Discovery Wizard** to disable pinging. In this case, the discovery will take longer to complete.

Installing the software

On the management server, ensure that you are logged on as a user with Administrator permissions. You will run the setup executable (setup.exe) on this machine, which will launch the IT Operations Analyzer InstallShield Wizard. The InstallShield Wizard collects information about your installation preferences, management server configuration, and database scale.

NOTE:

- When you initially install IT Operations Analyzer, a temporary file is created within the TEMP or TMP folder, as specified in the Environment Variable. However, if either 'TEMP' or 'TMP' is not set in the Environment Variable, then the installation will fail.
- IT Operations Analyzer cannot be installed on the same server on which:
  - IT Operations Repository is installed.
  - IT Operations Integrator is installed.

To install IT Operations Analyzer:

1. Run **setup.exe** from the installation media.

   The InstallShield Wizard launches and displays the **Welcome** panel.

2. To continue, click **Next**.

   The **License Agreement** panel displays, and contains information about the software license terms. If it is easier for you to read the terms on paper, click **Print**.

3. To agree to the usage terms, click **I agree to the terms of this license**. Then, click **Next**.

4. Complete the information contained in each of the remaining panels. Note the following:

   - The DCOM setting is displayed if it is disabled. If your site will monitor Windows servers, then enable DCOM as described in the InstallShield Wizard. After the installation, you must restart the management server.
   - If requested, specify the scale of your database, based on the number of nodes you plan to monitor. If you need to change this information later on, you can do so using the database expand command. Refer to the online Help book, *Managing the IT Operations Analyzer Database*.
   - If requested, specify an IP address. If needed, you can change the specified IP address after the installation.

NOTE: The IP address listed in the hosts file takes precedence. If the host name of the management server is listed in the hosts file, please make sure that the IP address is correct. If the management server has multiple IP addresses, please either add all the IP addresses in the hosts file or delete them all.

- Table 2-4 describes the default ports. Use these unless you identify any port number conflicts. After the installation, you can modify the management server port numbers, if needed. For information, refer to the online Help book, *Modifying Connection Settings*.

Table 2-4: Port Numbers Used by IT Operations Analyzer

Default Port	Usage
20510/TCP	Access to the management server, using the Web browser.
20511/TCP	Communications within the management server.
20512/TCP	
20514/TCP	
20513/TCP	Communications within the management server and access to the database.
20515/TCP	Access to the database, using reporting software.
162/UDP	Receive SNMP traps from monitored nodes.

5. The **Setup Complete** window will appear after installing necessary software and ask you if you want to restart your computer. Choose “No, I will restart my computer later.” and click **Finish** to continue.
6. When the IT Operations Analyzer installation is complete, the **InstallShield Wizard** window will appear and ask you if you want to restart your computer. Choose “Yes, I want to restart my computer now.” and click **Finish**.

   If you chose to launch IT Operations Analyzer after completing the installation, then the login prompt displays. However, you cannot use the software until you have activated your license. See Chapter 3, Activating your license.

Migrating from an IT Operations Analyzer 32-bit version to a 64-bit version

The basic tasks to migrate the database to a 64-bit version of IT Operations Analyzer are as follows:

- Export the existing database from the management server
- Import/migrate the database to a different or the same management server
- Uninstall the 32-bit version of IT Operations Analyzer
- Install the 64-bit version of IT Operations Analyzer

NOTE: The order of these tasks will differ, depending on the migration method that you use.

Before you begin the migrating procedures from the 32-bit IT Operations Analyzer server to the 64-bit IT Operations Analyzer server, be sure to review the following topics:

- Precautions (below)
- “Migrating the Database” in the Help

Precautions

Observe the following guidelines:

- Your server must be running IT Operations Analyzer v3.0 or higher. If you have an older version, you must upgrade IT Operations Analyzer software to be able to migrate the database.
- You cannot migrate from a 64-bit version of IT Operations Analyzer to a 32-bit version.
- You cannot migrate from a server running a newer version of IT Operations Analyzer to a server running an older version of the software. If the migration destination machine is running an older version of IT Operations Analyzer than the previous server, migration will fail. Before migration, verify that the migration destination machine is running a newer version of IT Operations Analyzer than the previous (export) management server.
- You must delete the trace log file before installing the IT Operations Analyzer 64-bit version. See Migrating procedures for additional information.
- After uninstalling the 32-bit version, a trace log file will remain. You must delete this file before migrating the database and installing the 64-bit version of IT Operations Analyzer. If you do not delete the existing file, this may prevent IT Operations Analyzer from generating a new log output file. The following sections describes the deletion method. Please perform these tasks, carefully.

Migrating procedures

There are two types of migrating methods:

- Migrating to a different server
- Migrating to the same server

Select the method that best suits your site requirements.

Migrating to a different server

Follow these instructions to migrate the existing IT Operations Analyzer database to a different server.

1. Run the **export** command, for example:

   export.exe -f "C:\temp"

2. Run the **getlogs** command to obtain potential “obstacle” data to help investigate possible migration problems, for example:

   getlogs.exe -f "C:\temp"

NOTE: It is recommended that you save information from the **getlogs** command for approximately one month.

3. If the 32-bit version Analyzer is installed in the migration destination machine, perform the following tasks:
   a. Copy and save the Argus.properties file from the \conf directory under the 32-bit version IT Operations Analyzer installation directory. You will use the file contents in step 7, as needed.
   b. From the **Start** menu, run the **Analyzer Command** to confirm the operational pass to the bin directory. The path of the installation directory of IT Operations Analyzer is a path that has deleted the “bin” for \Program Files\HITACHI\IT Operations\Analyzer\bin.

NOTE: In Windows Server 2012, navigation to the **Start** menu is different.

4. Perform the following tasks, if the 32-bit version Analyzer is installed in the migration destination machine.
   a. Uninstall the 32-bit version of IT Operations Analyzer from the previous server.
   b. Delete the 32-bit version IT Operations Analyzer installation directory from the previous server.

5. Perform the following tasks in the migration destination machine prior to installing the 64-bit version IT Operations Analyzer:
   a. Delete any files or contents in the intended 64-bit IT Operations Analyzer installation directory.

NOTE: If you do not delete the existing trace log file, this may prevent IT Operations Analyzer from generating a newer log output file.
If the directories and file are not present, no action is required.

The installation directory set up by the default is:
"C:\Program Files\HITACHI\IT Operations\Analyzer"

   b. Install the 64bit versions Analyzer.
   c. Specify an empty directory, when the dialog prompts to change the trace log storage directory that is displayed.
6. Run the **import** command to import the database that you exported in step 1, for example:

   import.exe -f "C:\temp"

   As of IT Operations Analyzer V3.3.0, the **import** command does not overwrite the contents of the Argus.properties file of the migration destination machine. IT Operations Analyzer saves it as the following alias file:

   Argus.properties.export
7. Check the contents of the Argus.properties file under a \conf directory against the information the Argus.properties.export file. Replace it with the contents of the Argus.properties file that you copied and saved in step 3, as needed.
8. Reboot services.
9. Uninstall the 32-bit version of IT Operation Analyzer from the previous management server, after a successful migration.

Migrating to the same server

Follow these instructions to migrate the existing IT Operations Analyzer database to the same server.

1. Backup the database by using a commercial-release tool (only), prior to uninstalling the original 32- bit version of IT Operations Analyzer.

NOTE: If data migration fails, you can use the backup data to recover the environment. If this happens, run the migration procedure again, once the environment is recovered from the backup data. Prior to recovery, use the **getlogs** command to help determine the cause of the migration failure (see step 3).

2. Run the **export** command, for example:

   export.exe -f "C:\temp"

3. Run the **getlogs** command to obtain potential “obstacle” data for possible investigating, for example:

   getlogs.exe -f "C:\temp"

NOTE: It is recommended that you save information from the **getlogs** command for approximately one month.

4. Perform the following tasks:
   a. From the **Start** menu, run the **Analyzer Command** to confirm the operational pass to the bin directory. The path of the installation directory of IT Operations Analyzer is a path that has deleted the “bin” for \Program Files\HITACHI\IT Operations\Analyzer\bin.

NOTE: In Windows Server 2012, navigation to the **Start** menu is different.

   b. Uninstall the 32-bit version of IT Operations Analyzer from the previous server.
   c. Delete the 32-bit version IT Operations Analyzer installation directory from the previous server.
5. Perform the following tasks in the migration destination machine prior to installing the 64-bit version IT Operations Analyzer:
   a. Delete any files or contents in the intended 64-bit IT Operations Analyzer installation directory. Make sure this directory is empty.

NOTE: If you do not delete the existing trace log file, this may prevent IT Operations Analyzer from generating a newer log output file.
If the directories and file are not present, no action is required.

The installation directory set up by the default is:
"C:\Program Files\HITACHI\IT Operations\Analyzer"

   b. Install the 64bit versions Analyzer.
   c. Specify an empty directory, when the dialog prompts to change the trace log storage directory that IT Operations Analyzer displays.
6. Run the **import** command to import the database that you exported in step 2, for example:

   import.exe -f "C:\temp"

   As of IT Operations Analyzer V3.3.0, the **import** command does not overwrite the contents of the Argus.properties file of the migration destination machine. IT Operations Analyzer saves it as the following alias file:

   Argus.properties.export
7. Check the contents of the Argus.properties file under a \conf directory against the information the Argus.properties.export file.
8. Reboot IT Operations Analyzer services.

3

Activating your license

This chapter describes the license activation options and the associated activation process. After the license activation is completed, you can review license information.

Overview

Before you can log in and start any monitoring activities, a valid license is required: The license contains information about the maximum number of nodes that you can monitor, and other data. The monitoring capacity and time frame that you have while working with IT Operations Analyzer are based on the type of license.

NOTE: If your site has more than one management server, a separate license is required for each machine.

In addition, Adobe® Flash® Player is required to launch IT Operations Analyzer. Be sure to install and enable this software prior to operation.

License activation

The activation process is customized depending on whether this is the first time you are installing the trial or purchased software, or whether you are upgrading your existing software version:

- After installing the software for the first time, at the IT Operations Analyzer log in prompt, click:
  - **Free Trial** for the trial software.
  - **Activate License** for the purchased software.
- After upgrading the software, at the IT Operations Analyzer log in prompt, click the **License** button to open the **License Information** panel. Within this panel, click the **Activate License** button to launch the License Activation Wizard and start the activation process.

Depending on your Internet access options, you can either complete the license activation online, or offline using the Web or e-mail:

- **Activate the license online** if your client machine has an Internet connection and can access the management server using a browser. This is the most common approach, since most client machines can access the Internet through a proxy server. The Online License Activation option can also be used if the management server has Internet access, and you want to complete the license activation directly from the management server.
- **Activate the license offline** if your client machine does not have an Internet connection, and cannot access the management server, using a browser. This method also applies when the management server does not have Internet access. This option is called 'offline' because although you can perform a portion of the license activation on the client machine, you need to use a computer that does have an Internet connection to send license-related files using the Web or e-mail.

Resuming the license activation process

Because it takes a few minutes to download and register files for the offline method, you may choose to exit the License Activation wizard while you wait to receive the LicenseKey.xml file, and resume the license activation process later.

In the following example, two options are selected:

- **I do not have internet access**
- **I have a license key file**

These selections let you continue with the license activation, offline. This example is associated with the license activation of the purchased software.

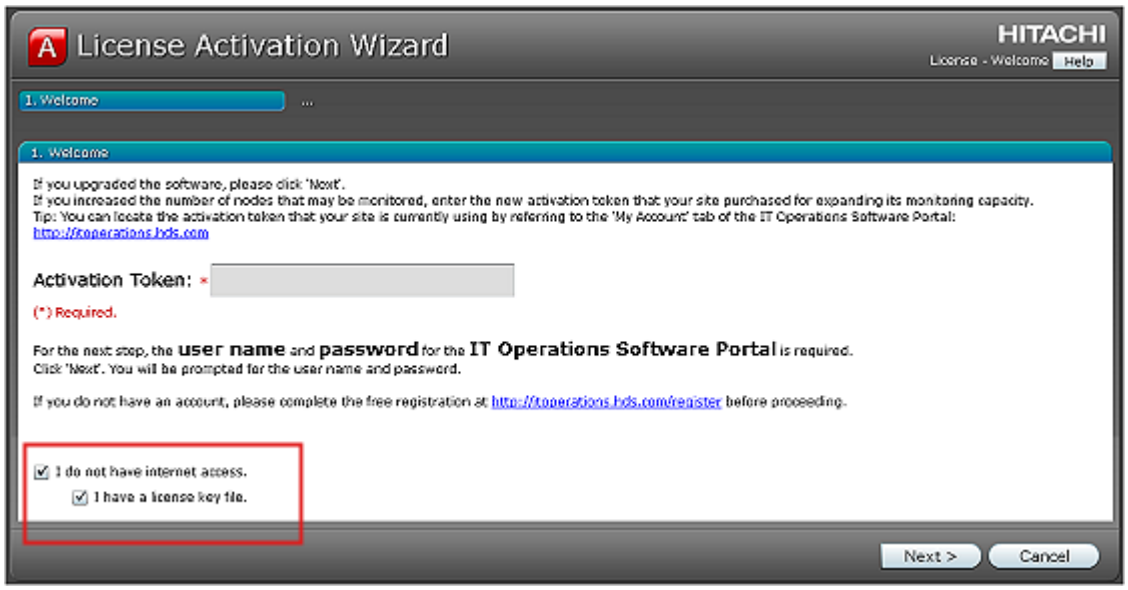

Figure 3-1: Resuming the License Activation

Before you begin

Verify that you have registered on the IT Operations Software Portal:

http://www.itoperations.com

The registration is free, and it will provide you with a user name (an e-mail address that you specify) and a password. These items are required for the license activation process.

Launching the login panel

The license activation wizard is accessed directly from the IT Operations Analyzer login panel, shown below.

Figure 3-2: Login Panel

Use the host name and port data that you entered during the installation, to specify the IT Operations Analyzer URL.

To log in:

1. Launch the Web browser.
2. In the address bar, specify the URL of the management server, using the following format:

   http://*hostname*:*portnumber*/Analyzer/Analyzer.jsp

   For example, if the host name is Analyzer and the port number is 20510, then type: http://Analyzer:20510/Analyzer/Analyzer.jsp

   The IT Operations Analyzer login panel displays.

Online activation

You can complete the license activation online when the client machine is connected to the Internet and it has network access to the management server, using a browser.

To activate your license online:

1. Open the login panel for IT Operations Analyzer.
2. Click the appropriate button:
   - Click **Activate License** (purchased software)
   - Click **Free Trial** (trial software).

NOTE: If you have completed an upgrade installation, then click the **License** button to open the **License Information** panel. Within this panel, click the **Activate License** button.

   The **License Activation Wizard** displays.

   If you have completed an upgrade installation, or if you have purchased a license, then the end user license agreement displays. To agree to the usage terms, click **I agree to the terms of this license**. Then, click **Next**.

3. The **Welcome** panel is for specifying the Activation Token:
   - If you are registering the free trial version of the software, it is not necessary to specify the Activation Token. You can continue to step 4.
   - If you are completing an upgrade installation, and your Software Maintenance contract is active, then your existing Activation Token is entered for you.
   - If you are registering a new purchased license, then enter the new Activation Token.
4. Click **Next**.
5. Enter the **User name** (e-mail address) and **Password** that were provided when you (or a contact for your site) registered on the IT Operations Software Portal.

   The activation process may take a few minutes. If your license is activated, then the last panel indicates that you have successfully completed the wizard.
6. Click **Close** to exit the wizard.

Offline activation

You can complete the license activation offline, when the client machine does not have an Internet connection and cannot access the management server using a browser. In this case, you can use your client machine to complete a portion of the license activation process, but you will need a computer that does have Internet access, to send and receive license-related files.

When completing the portion of tasks that require using a computer that has Internet access, you can use the IT Operations Software Portal or you can use e-mail.

To activate your license offline:

1. Open the login panel for IT Operations Analyzer.
2. Click the appropriate button:
   - Click **Activate License** (purchased software)
   - Click **Free Trial** (trial software).

NOTE: If you have completed an upgrade installation, then click the **License** button to open the **License Information** panel. Within this panel, click the **Activate License** button.

   The **License Activation Wizard** displays.

   If you have completed an upgrade installation, or if you have purchased a license, then the end user license agreement displays. To agree to the usage terms, click **I agree to the terms of this license**. Then, click **Next**.

3. The **Welcome** panel is for specifying the Activation Token:
   - If you are registering the free trial version of the software, it is not necessary to specify the Activation Token. You can continue to step 4.
   - If you are completing an upgrade installation, and your Software Maintenance contract is active, then your existing Activation Token is entered for you.
   - If you are registering a new purchased license, then enter the new Activation Token.
4. Check the box next to **I do not have Internet access**, then click **Next**.

   The creation of an activation file begins.
5. Click **Download the Activation File.**

   The name of the downloaded file is **Activation.xml**.

NOTE: In the License Activation wizard, the **Next** button will become active only after the **Activation.xml** file has finished downloading.

6. Click **Next**.

   The **Receive License Key File** panel displays.

NOTE: Because the client machine is not connected to the Internet, you will complete a portion of the following steps on a computer that does have an Internet connection, and can access the IT Operations Software Portal. You can either exit the License Activation wizard now, or leave it open.

7. After the **Activation.xml** file has been downloaded, take it to a computer that has Internet access. (For example, copy the file to a memory stick, and paste it onto the Desktop of a computer that has an Internet connection.) You can complete the next steps using either the Web or e-mail.

To register the Activation File using the Web:

a. Use the following link to access the **IT Operations Software Portal**: http://itoperations.hds.com/activation

b. Enter the **User name** (e-mail address) and **Password** that were provided when you (or a contact for your site) registered on the IT Operations Software Portal.

c. After your information is confirmed, upload the **Activation.xml** file, as requested.

d. After the Activation.xml file has been received and processed, a **LicenseKey.xml** file is provided for download. Download this file to the computer. If you used a memory stick at step 7, then copy the file onto the memory stick, and return to your client machine.

e. If you:

   Exited the **License Activation** wizard (after step 6), then refer to the section, Resuming the license activation process.

   Left the **License Activation** wizard open (after step 6), then within the wizard, click **Next**. Go to step 8.

To register the activation file using E-mail:

a. Open your electronic mail application.

b. In the **From**: portion of the e-mail, specify the valid e-mail address that was used for the **IT Operations Software Portal** registration.

c. Copy the following address and paste it in the **To**: portion of the e-mail: **ItOperationsActivate@hds.com**

d. Send, as an attachment, the **Activation.xml** file to the e-mail address.

e. After the Activation.xml file has been received and processed, a **LicenseKey.xml** file is sent to your e-mail. Download this file to your computer. If you used a memory stick at step 7, then copy the file onto the memory stick, and return to your client machine.

f. If you:

Exited the **License Activation** wizard (after step 6), then refer to the section, Resuming the license activation process.

Left the **License Activation** wizard open (after step 6), then within the wizard, click **Next**. Go to step 8.

8. Click **Browse** to navigate to the location of the **LicenseKey.xml** file (for, example, specify the memory stick location). Once the file path is displayed in the field, click **Next**.

The activation process may take a couple of minutes.

- If your license is activated, then the last panel indicates that you have successfully completed the wizard. Click **Close** to exit the wizard.
- If there was a problem with the license activation, then the **License activation results** panel indicates the failure. You have two options:

  You can try the activation process again, using the same method as before. In this case, click the **Try Offline Again** button or **Try Online Again** button, as appropriate.

  You can try the activation process again, using a different method. In this case, click the **Try Offline** button or **Try Online** button, as appropriate.

Resuming the license activation process

Refer to the following steps if you have completed a portion of the license activation process, you have the LicenseKey.xml file, and you want to finish the license activation.

To resume the license activation process:

1. Open the login panel for IT Operations Analyzer.
2. Click the appropriate button:
   - Click **Activate License** (purchased software)
   - Click **Free Trial** (trial software).

NOTE: If you have completed an upgrade installation, then click the **License** button to open the **License Information** panel. Within this panel, click the **Activate License** button.

The **License Activation Wizard** displays.

If you have completed an upgrade installation, or if you have purchased a license, then the end user license agreement displays. To agree to the usage terms, click **I agree to the terms of this license**. Then, click **Next**.

3. In the **Welcome** panel, ensure that both check boxes are selected. Then, click **Next**:
   - **I do not have Internet access**
   - **I have a license key file**
4. Click **Browse** to navigate to the location of the **LicenseKey.xml** file. Once the file path is displayed in the field, click **Next**.

   The activation process may take a few minutes. If your license is activated, then the last panel indicates that you have successfully completed the wizard.
5. Click **Close** to exit the wizard.

   The activation process may take a couple of minutes.
   - If your license is activated, then the last panel indicates that you have successfully completed the wizard. Click **Close** to exit the wizard.
   - If there was a problem with the license activation, then the **License activation results** panel indicates the failure. You have two options:

     You can try the activation process again, using the same method as before. In this case, click the **Try Offline Again** button or **Try Online Again** button, as appropriate.

     You can try the activation process again, using a different method. In this case, click the **Try Offline** button or **Try Online** button, as appropriate.

Accessing license information after the activation

To review the current monitoring capacity and check other license related details, refer to the **License Information** panel.

You can access this panel from the following areas:

- **Login** panel

  The **License** button is always active. Click it to launch the **License Information** panel.

- **Settings** module

  After logging in, click the **Settings** tab. From the **License** area, select **License Information**.

- **Help** menu

  Clicking **About** from the **Help** menu displays the **License Information** panel.

Data in the **License Information** panel is updated after you increase or decrease the number of monitored nodes:

- Whenever you add discovered nodes to your monitoring routine.
- Whenever you expand the monitoring capacity, then specify the nodes to be monitored.
- Whenever you remove nodes.

Figure 3-3 is an example of the panel when it is accessed from the Login panel or Help menu.

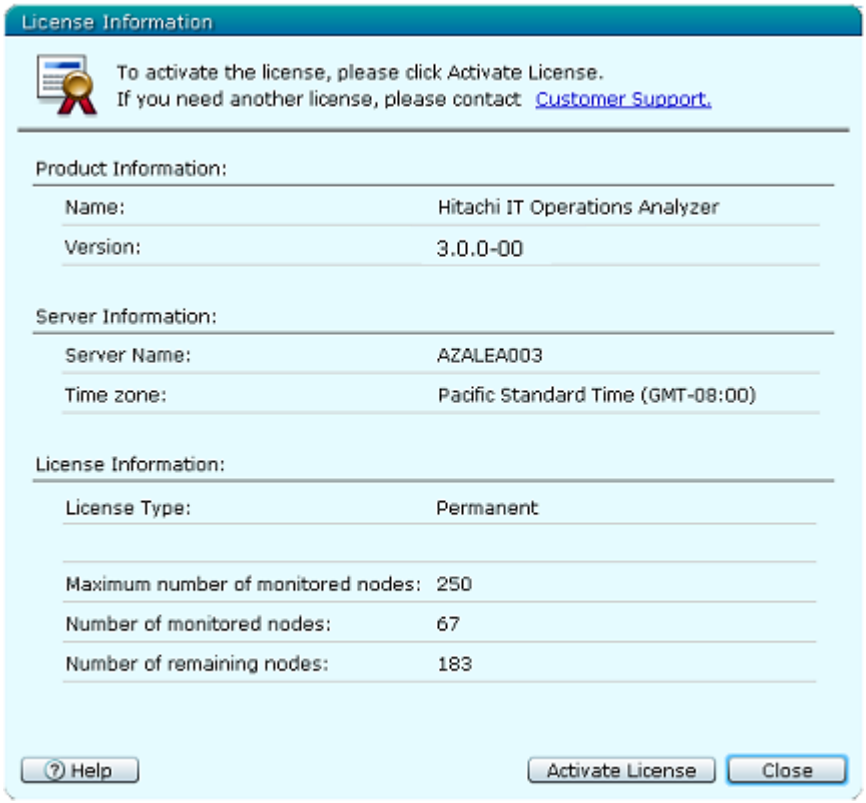

Figure 3-3: Example License Information Panel

4

Logging in and completing initial setup tasks

This chapter describes how to launch the login panel and enter the requested information, and it introduces the modules with which you will be working. It also describes how to change the default administrator password, so you can protect the security of your information. Afterward, to prepare for the initial system discovery, you will add other administrator users.

Overview

Now that you have activated your license, you are ready to log in and work with IT Operations Analyzer. After reviewing an introduction to the software layout, you will complete the following configuration tasks:

- **Changing the password of the built-in administrator account**.

  To prevent unauthorized users from logging in, change the password information for the built-in (default) administrator account.

- **Adding administrator accounts**.

  If your site has multiple IT administrators for different functions, you can create accounts for those users. Later on, these accounts will be necessary when you start the discovery process, and need to identify recipients of certain e-mail notifications.

Logging in

Use the host name and port data that you entered during the installation, to specify the IT Operations Analyzer URL. A user identifier (ID) and password is built into the application, so you will use this information to log in.

To log in:

1. Launch the Web browser.
2. In the address bar, specify the URL of the management server, using the following format: http://hostname:portnumber/Analyzer/Analyzer.jsp

   For example, if the host name is MonitoringMachine and the port number is 20510, then type: http://MonitoringMachine:20510/Analyzer/Analyzer.jsp

   The IT Operations Analyzer login panel displays.
3. Enter the built-in user information. Note that the **Password** is case-sensitive:
   - **User ID**: system
   - **Password**: manager
4. Click **Log in**.

   The **Home** module displays.

NOTE: If you specify the wrong password three consecutive times, the account is temporarily locked. Only a user with Admin privileges can remove the lock. For information about removing the lock, please refer to the Online Help.

Introducing the IT Operations Analyzer desktop and Help

After you log in, you will see the desktop of IT Operations Analyzer. The **Home** module is always displayed, and provides an at-a-glance view of the status of your monitored environment.

Because you have not yet completed the **Discovery Wizard** (which finds your system components and reports the results), no data is displayed.

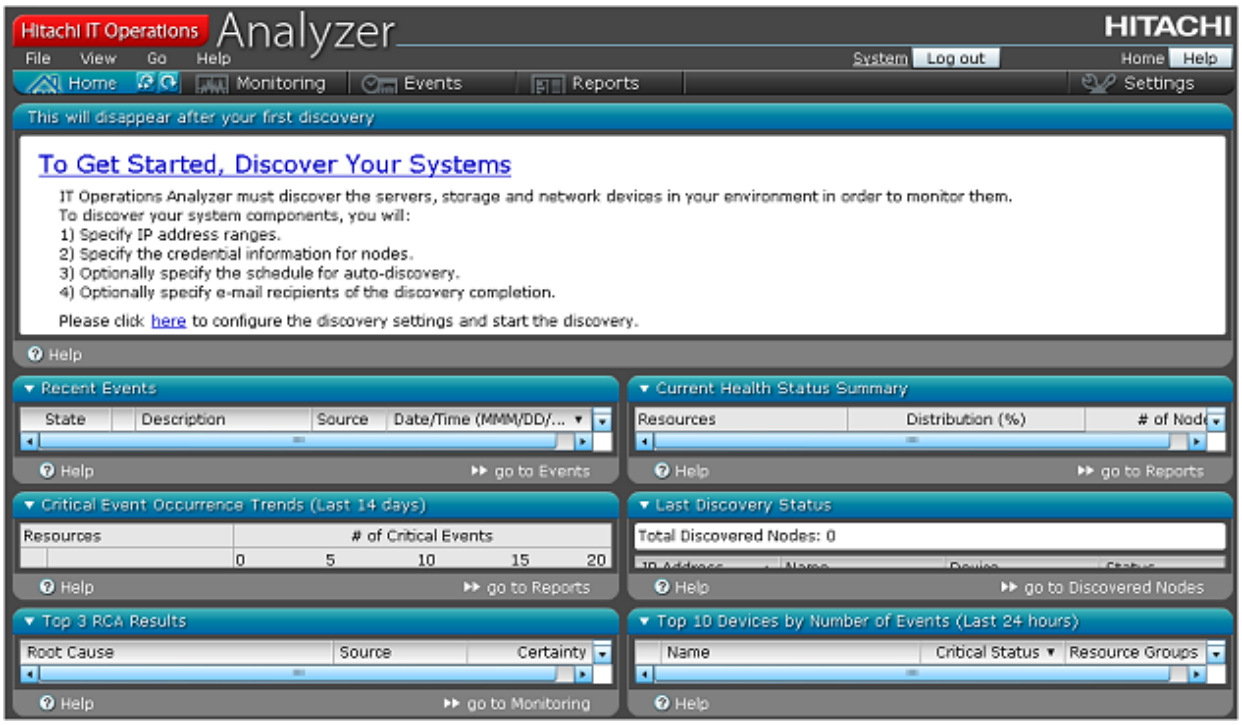

Figure 4-1: Initial Desktop View

In this example, the top group box labeled **This will disappear after your first discovery** is where you will start the discovery process. This reminder disappears after you complete the wizard. However, if the number of monitored nodes should ever decrease to '0', then the reminder will redisplay.

About the desktop components

In the documentation, portions of the IT Operations Analyzer desktop are referred to specifically; for example, module, pane, and so on. Those areas are numbered, and are described in Table 4-1.

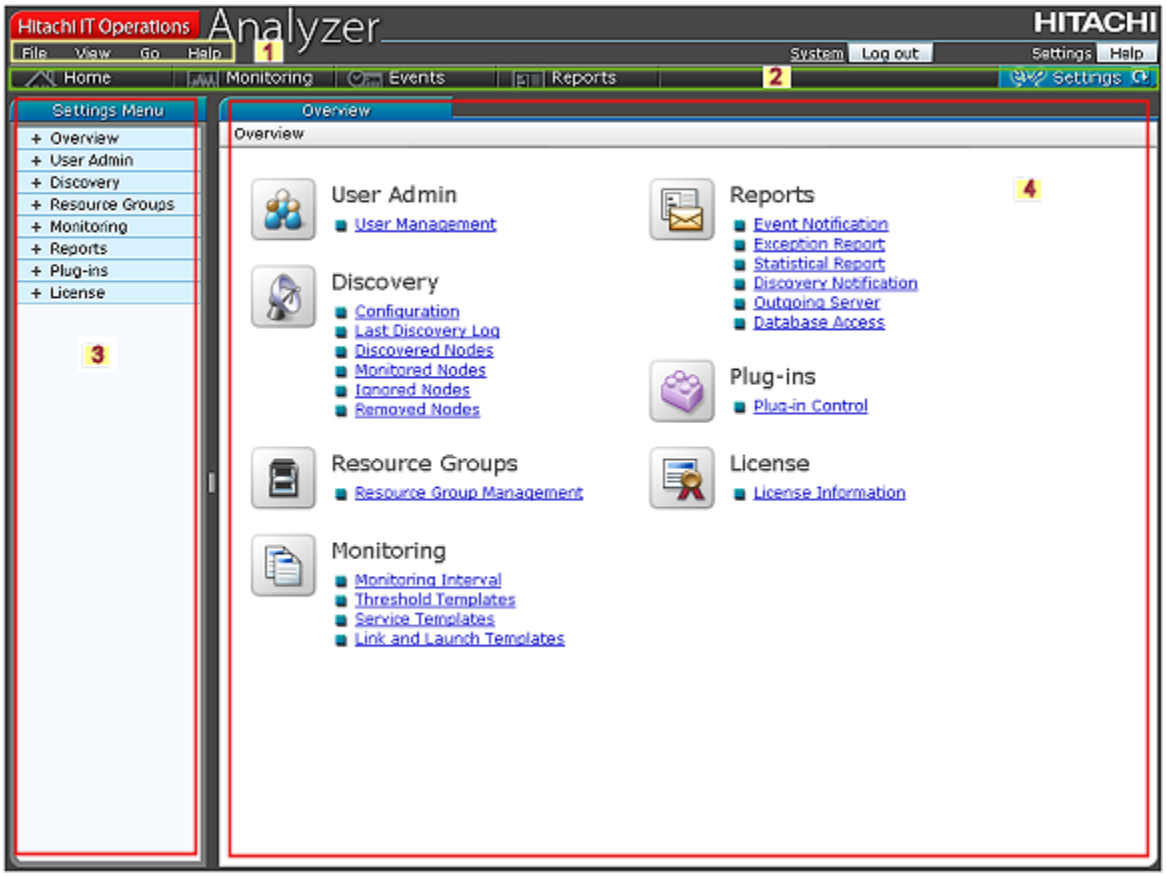

Figure 4-2: Desktop Components

Table 4-1: Desktop Components

Area		Details
1	Menu	**File** This menu lists the **Log out** option, which ends your software session and displays the Login prompt. **View** This menu lists the **Restore Default Screen Layout** option. Clicking it reverts any display changes (such as moved panels in the Home module) to their default settings. **Go** This menu lists the following options: **Analyzing RCA Availability Snapshots** and **Analyzing RCA Performance Snapshots**, which launch the **Monitoring** module; **Start Discovery Wizard**, which launches the wizard for capturing information about your environment; and **Change Profile**, which launches the **Edit User** dialog, where the logged in administrator can change personal account settings. **Help** This menu lists two options: **Online Help**, which launches the Help system for IT Operations Analyzer, and **About**, which displays license information. The right side menu area shows the logged-in administrator's ID. In Figure 4-2, **System** is indicated. Clicking the ID displays the **Edit User** dialog.
2	Module	**Home** This module provides an overview of your system's status. Each pane gives a summary of the monitored environment, from different perspectives. **Monitoring** This module provides information about event statuses and troubleshooting resources, such as root cause analysis. **Events** This module categorizes all detected events. **Reports** This module provides a daily, weekly, or monthly reporting schedule of performance statistics and other data. **Settings** This module provides system-wide configuration, such as discovery schedule settings, user account administration, and threshold settings.
3	Module menu	This area shows the key resources that are associated with the selected module. When you make a selection from the menu, details about it are displayed in the information area.
4	Information	This area changes depending on the selected module and your selection from the module menu. Depending on your permissions and the options that are available based on the selected menu item, you may also be able to add, edit, or delete data.

Referring to the Online Help

Product usage information is available from the **Help** menu: Click **Help**.

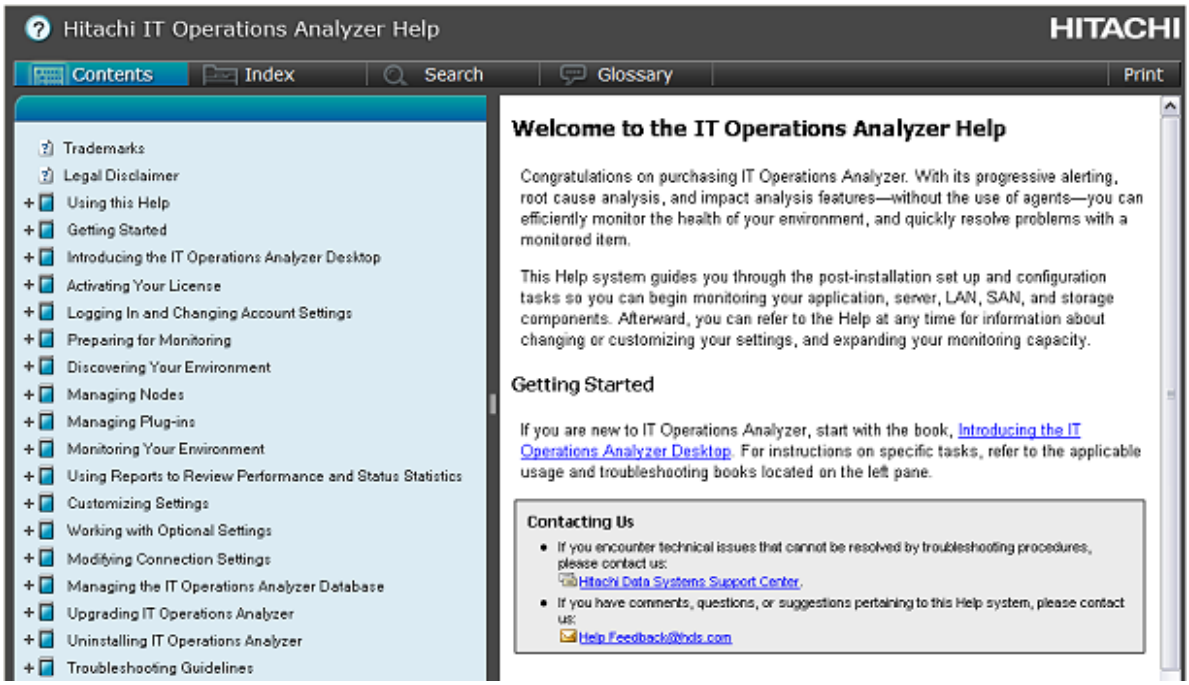

Figure 4-3: Initial View of the Online Help

Referring to the in-context Help

Clicking **Help** when working in the following areas will provide you with task-specific information:

- Any module
- Wizards, dialogs, and pop-ups.

Specifying browser language settings

If needed, you can work with IT Operations Analyzer in German, Simplified Chinese, and Spanish, by specifying your language preferences within the browser. The following language options are supported:

Table 4-2: Supported Language Options

Language	Options
English	[en], [en-gb], [en-us], [en-ie], [en-au], [en-ca], [en-jm], [en-zw], [en-tt], [en-nz], [en-ph], [en-bz], [en-za]
German	[de], [de-at], [de-ch], [de-li], [de-lu]
Simplified Chinese	[zh-cn], [zh-sg], [zh-hans-cn], [zh-hans-sg]
Spanish	[es], [es-ES]

To set language preferences:

1. Open the Web browser.
2. Depending on your browser, selection, complete the following steps.

   For Microsoft Internet Explorer:

   a. From the **Tools** menu, select **Internet Options**.

      The **Internet Options** dialog opens.

   b. From the **General** tab, click **Languages...**

      The **Language Preference** dialog displays.

   c. If it is not already specified in the **Language:** box, click **Add** to specify one or more of the supported languages.

   d. Go to step 3.

   For Mozilla Firefox:

   a. From the **Tools** menu, select **Options**.

      The **Options** dialog opens.

   b. From the **Content** option, click **Choose** for the **Languages**.

      The **Languages** dialog displays.

   c. If it is not already specified in the **Languages in order of preference:** box, click the **Select a language to add** list, to specify a supported language, then click **Add**.

   d. Go to step 3
3. Promote the language that you want to see, by default, by selecting the language, then clicking **Move Up** until it is the first language in the list
4. Click **OK** to save your changes.

Changing the password of the built-in administrator account

A built-in administrator account is enabled in IT Operations Analyzer, so you can log in and begin completing some of the initial set up and system discovery tasks.

For security, we recommend that you change the password that is associated with the account, and customize the other account settings as necessary. Changing the default information prevents unauthorized access to the software, and to your monitored environment.

You can add, modify, and delete user accounts within the **Settings** module (in **User Management** of the **User Admin** section).

NOTE: You cannot delete the built-in account, even after creating other records. Also, the **ID** and permissions are fixed, and cannot be changed.

To change the password of the built-in user account:

1. Log in.
2. Click the **Settings** module.
3. From the **Settings** menu, navigate to the **User Admin** section, and select **User Management**.

   The **User Management** panel opens, and lists the built-in user account.
4. Click **edit**.

   The **Edit User** dialog displays.
5. Change the password:
   a. Select **Check this box to change the password**.
   b. Type the password in the **New Password** field.
   c. Type the password again, in the **Retype the password** field.
6. Optionally change the other account settings:
   a. **Name** Enter the administrator's name.
   b. **E-mail** Specify the e-mail address, for example: sam@Hitachi.com

NOTE: You can specify up to 255 ASCII-type characters. Use the at sign, @, once. Characters must exist before and after the @. Do not include a period at the beginning or end of the address. Also, do not use any of the following symbols: ( ) < > [ ] : ; \,

   The e-mail address that you specify will be displayed in the 'From' portion of the e-mail notification. **Note**: If an e-mail is not specified for the built-in user account, then the 'From' portion will be blank.

   c. **Description** Enter a short description of the type of user account that you are creating. It is helpful to use a description of the type of functions that the administrator will be performing. You can type up to 80 characters.
7. Click **OK** to save your changes and close the dialog.

Adding administrator accounts

Depending on the size of your site's IT infrastructure, there may be multiple administrators for different functions. In this case, you can create accounts for those administrators and assign appropriate permissions within the **Settings** module. After logging in using the built-in account, you can set up the permissions for each user account, as described in the following table.

Table 4-3: Administrator Permission Levels

Permissions	Referenced in this Guide and the Help
View information, only	View permissions
View, add, edit, and delete information, except for the user accounts and user account settings of other administrators	Operator permissions
View, add, edit, and delete information, including the user accounts and user account settings of other administrators	Admin permissions

Later on, you can use these accounts when you start the discovery process, and need to identify recipients of certain e-mail notifications.

To add an administrator account:

1. Log in.
2. Click the **Settings** module.
3. From the **Settings Menu**, navigate to the **User Admin** section, and select **User Management**.

   The **User Management** panel opens, and lists the built-in user account.
4. Click **Add User**.

   The **Add New User** dialog displays.
5. Enter a unique identifier for the user in the **ID** field. Note that when you save this record, the ID will be fixed (you cannot change it).
6. Specify a unique password in the **New Password** field. Then, type the password again, in the **Retype the password** field.
7. Specify the other account settings:
   a. **Name** Optionally enter the administrator's name.
   b. **E-mail** Optionally specify the administrator's e-mail address.
   c. **Description** Optionally enter a short description of the type of user account that you are creating. You can type up to 80 characters.
   d. **Permission** At least one permission selection is required:

      Admin: View, add, edit, and delete information, including user accounts.

      Operator: View, add, edit, and delete information, except for user accounts.

      View: View information, only.
8. Click **OK** to save your entry and close the dialog.
9. To add other user accounts, repeat steps 4-8.

5

Discovering your environment

This chapter describes how IT Operations Analyzer locates your servers, storage, and switches using the information that you will enter in the Interactive Discovery Wizard.

Overview

The **Discovery Wizard** is the first step toward monitoring your system. It lets you specify information about your environment, such as the IP addresses in your network, and associated credentials.

The information you supply is based on the work that you completed in Chapter 2, Setup and installation. IT Operations Analyzer uses the data to locate the nodes in your environment, then it sends an e-mail notification when the process is finished.

In the future, IT Operations Analyzer completes the discovery process based on a default schedule, or the schedule that you set within the **Discovery Wizard**.

About the Discovery Wizard options

After you launch the **Discovery Wizard**, the following panel displays. Notice the area that has been highlighted by the red box:

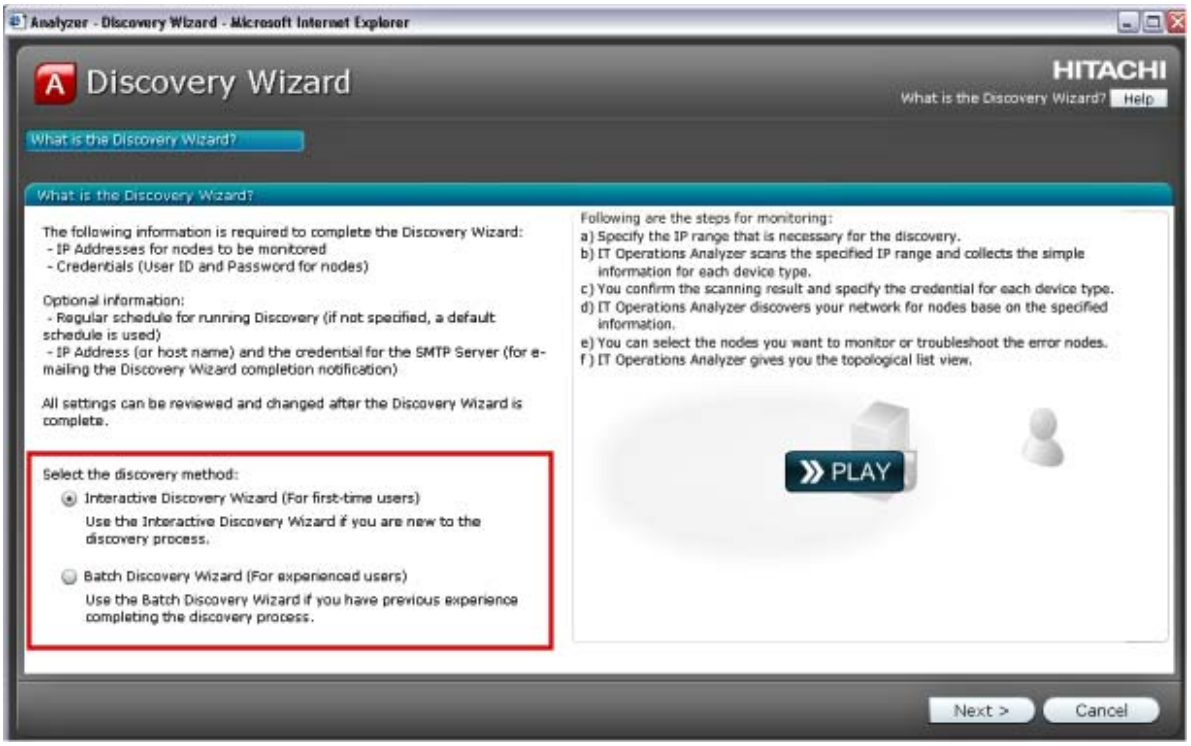

Figure 5-1: Discovery Wizard Options

Here, you are presented with two usage options:

- **Interactive Discovery Wizard** Select this option if this is the first time that your site is completing the discovery process.
- **Batch Discovery Wizard** Select this option if your site has already completed the discovery process and is familiar with the procedure.

In this document, the discovery process using the **Interactive Discovery Wizard** is described. For information about using the **Batch Discovery Wizard** for future discoveries, please refer to the Help.

Using the Interactive Discovery Wizard

To start the discovery of your environment:

NOTE:

- Admin or Operator privileges are required.
- Details about each panel of the **Discovery Wizard** are available by clicking **Help**. Also, use the **Help** button that is located within add and edit dialogs, as needed.

1. Log in.

   The **Home** module displays. The top panel shows the prompt to start the **Discovery Wizard**, and is labeled **This will disappear after your first discovery**.

2. To launch the wizard, click either of the following links:

   To Get Started, Discover Your Systems

   Please click **here** to configure the discovery settings and start the discovery.

3. The **Discovery Wizard** launches and displays the overview panel of the discovery process, **What is the Discovery Wizard?** Select **Interactive Discovery Wizard**.

4. After making your selection, optionally click **PLAY** to watch an overview of the discovery process. Otherwise, to start with your selection, click **Next**.

   The **Specify IP Address Range** panel displays.

Specifying an IP Address Range

The **Specify IP Address Ranges** panel lets you indicate where IT Operations Analyzer should locate the servers, storage, and switches in your environment.

Because the software will check all addresses in the range that you specify, we suggest that you use smaller ranges of two IP addresses per range. The discovery process will complete faster, and it prevents problems from occurring when only one IP address exists, with one type of credential. If you have a larger configuration, you should consider increasing the Discovery Timeout Value.

1. Click **Add IP Address Range**.
2. Enter the following information in the **Add IP Address Range** dialog:
   - **Name** Enter the name for the server range to be scanned for the discovery. Use a unique name (do not enter an existing name).

- **From**, **To** Enter the range of IP addresses to be scanned for the discovery. If this is the first time that your site is completing the discovery process (when no registered IP addresses exist), then by default, the IP address of the server on which IT Operations Analyzer is installed is entered in the **From** field.

NOTE: The identity of Microsoft Windows, Microsoft Hyper-V, and Linux, and Solaris nodes is determined by the host name. As a result, IT Operations Analyzer cannot simultaneously monitor multiple servers that have the same host name. If your site has several servers that have the same host name, then only specify the server you intend to monitor.

For Microsoft Windows and Microsoft Hyper-V, IT Operations Analyzer uses the NetBIOS name as the host name. As a result, for those Operating Systems, IT Operations Analyzer recognizes the first 15 characters as the host name.

- **Ping enabled** By default, the setting is **Enabled**. **Enabled** means that the target server will be pinged before the scan. If the device does not respond to the ping at this point, it will not be discovered. If you have not allowed the ICMP Echo request, as described in the Chapter 2 section, Permitting communications through a firewall, then choose **Disabled** (before the scan). If the setting is **Disabled** before discovery, the device will still be discovered by using the registered credential information, regardless of the ping response.

3. Click **OK**.

NOTE: If you have already entered one search range, and if you used an IP address that exists in another IP Address Range, you will be prompted to correct the overlap. Within the **Modify Existing IP Address Range** dialog, you can compare your entry against the suggested range. To accept the change, click **OK**.

4. Repeat steps 1 - 3 to add more search ranges.

   When you have multiple ranges, they are listed in ascending order, based on the IP address in the **Name** column. If needed, click **edit** to make changes to your entries, or click **remove** to delete an entry from the list.

5. By default, Analyzer will check the provided IP addresses and categorize the devices that are found on your network by type. We recommend that you keep this default selection. However, if you do not want the software to perform this check, select **I do not want to scan these IP Addresses**.

6. Click **Next** to proceed to the **Specify Credentials** panel.

   If you kept the default setting so that scans against the provided IP addresses are performed, then a **Confirmation** dialog displays. If there are any IP addresses that you do not want to scan, then clear the selection for the particular range. To start the scan, click **Start scan**.

   The progress of the scan is displayed within the next panel of the **Discovery Wizard**, **Specify Credentials**.

Specifying Credentials

The information that is displayed in the **Specify Credentials** panel depends on your selection in the **Specify IP Address Range** panel:

- If you kept the default setting so that scans against the provided IP addresses are performed, then an **Overview** area is displayed. This area indicates the progress and status of the scan, and whether there are any detected IP addresses, or if no responses were detected.

  When the **Status** of the scan is **Completed**, the results are listed in the **Device Type Summary** area. Each grouped result (for example, Server, FC Switch, Storage, etc.) is a button. The following information is provided:

  - The number of credentials that are associated with the device. (For the initial discovery, all values are 0.)
  - The number of **Detected new** IP addresses that were identified for the device.
- If you chose not to perform the scan, then there is no **Overview** area, and the **Device Type Summary** area indicates '-' in place of a value, for the **Detected new** devices.

To specify server access protocols and user authentication information:

1. From the **Device Type Summary** area, click a device type button; for example, **FC Switches** or **Storage**.

   The **Credential List** dialog displays. It provides information about the credentials that are associated with the device and the scanned IP addresses:

   - If you select **Automatically discover FC switches and storage that have associated credentials**, then the credentials that are used for other devices will be used to discover FC switches and storage.
   - The **Used Credentials** area lists the following details for each credential:

     Name The name of the credential.

     Protocol The server access protocol that is used for the device.

     ID The administrator identifier that is associated with the login for the server.

     #of Used Nodes The number of nodes that use the credential.
2. Manage the credential information as follows:

   - To delete a credential from the **Used Credentials** list, click **remove**.
   - To change information for a credential, click **edit**.

3. To add additional credentials, click **Add Credential**.

NOTE: Depending on the security measures that exist for the devices you want to discover, a device may reject a login if there have been a series of unsuccessful login attempts by a particular credentialed user. This can result in a locked account. Account locking can also occur when you have associated credentials that specify the same protocol and user ID of an existing IP address range.

The **Associate Credentials** dialog identifies those problems and lets you specify different credentials to use for the IP address range. Credentials that may have an account locking problem are identified by an icon:

Click **Associate Credentials**, then choose the **Select** option and check the box next to the credentials that may be causing the account locking issue, for the specified IP address range.To apply your changes and start the discovery process, click **OK**.

If the IP Address Range is wide, this operation may not be able to solve the problem; in this case, you can narrow the IP Address Range. To do so, click on the **go to Specify IP Address Range** link. This will return you to the **Specify IP Address Ranges** panel of the **Discovery Wizard**, where you can make changes to the IP Address Range.

4. Click **Next** to continue to the next panel of the **Discovery Wizard**.

Discover and Monitor Devices

The **Discover and Monitor Devices** panel lets you view the discovery progress, and when the discovery has finished, you can review a summary of the devices that were successfully discovered, those that have errors, and those that are monitored. Below each device category, the total number of associated credentials are displayed.

The **Overview** provides the following buttons and information:

- **Rediscover Troubleshot Nodes** Click this button to rediscover devices that, in a previous discovery, had errors and for which troubleshooting updates have since been applied. Based on the troubleshooting fixes applied by administrators at your site, this rediscovery should successfully identify the nodes. This button is active when no discovery process is currently running.
- **Rediscover** and **Cancel Discovery** If no discovery is in progress, then you can click **Rediscover**. If the discovery is currently running, then you can cancel it by clicking **Cancel Discovery**.
- **Status** This indicates the status of the discovery: **Canceled**, **Completed**, **Error**, or **Running**.
- **Elapsed Time** Indicates the duration of the discovery.
- **Progress** Indicates the discovery progress.
- **Detected IP Addresses in Scan** The number of IP addresses that were discovered by the scan. **new** Indicates the number of new IP addresses. If the scanning process is skipped, then **0** is displayed.

- **Discovered Nodes** Indicates the number of nodes that are not are not currently monitored.
- **Error IP Addresses** The number of IP addresses, except those for which there was no response, that could not be identified by the discovery process.
- **Monitored Nodes** The number of monitored nodes that were identified by the discovery.

The **Device Type Summary** provides a group of the identified devices (for example, Server, FC Switch, Storage, etc.). Each device type is a button. The following information is provided:

- The number of discovered nodes.
- The number of IP addresses, except those for which there was no response, that could not be identified by the discovery process.
- The number of monitored nodes.
- The number of credentials that may have been used to discover the device type. Server credentials are composed of WMI, SSH, and VMware credentials. IP Switch credentials are composed of SNMP credentials. FC Switch credentials are composed of SMI-S WBEM credentials. Storage credentials are composed of SMI-S WBEM and Hitachi Storage credentials.

All values that are displayed are not fixed until the **Status** of the discovery is **Completed**. The buttons become active when the discovery has finished.

1. Click a Device Type to review information that is contained in the **Discovery Log**. The **Discovery Log** dialog provides information about the results of the discovery. It also lets you resolve errors. There are three information components:
   - **Summary**

     This area indicates the number of nodes that were discovered, IP addresses which IT Operations Analyzer could not identify, and nodes that are monitored. Click the **Select devices to monitor** button to launch a separate dialog, in which you can indicate the nodes you want to monitor or ignore.
   - **Error list**

     This area lists the devices that have errors, and it provides the following details for each device: The type of device, the protocol that it uses, the error that was identified (such as an authentication error), the number of nodes that are affected by the error, and in the **Action** column, a **Solve** button. Click **Solve** to review the error nodes and start troubleshooting.
   - **Discovered IP list**

     This area indicates whether the discovery of IP addresses was successful. If an IP address requires some troubleshooting, then a link to the troubleshooting dialog is displayed.
2. Click **Next** to continue to the next panel of the **Discovery Wizard**.

Setting Discovery Notifications

Use the **Set Discovery Notifications** panel to indicate the personnel who will receive an e-mail notification when the discovery process is complete. The contacts that you add in this panel will also receive e-mailed reports that IT Operations Analyzer generates when there are events that require action.

- If you completed Chapter 4, Logging in and completing initial setup tasks, then you modified the built-in user account, and you added other administrator users. They are listed in the **Set Discovery Notifications** panel.
- If you did not finish the tasks in Chapter 4, then only the built-in user account is listed.You can enter the e-mail address of an existing IT Operations Analyzer user, which will be associated with this account.

To set discovery notifications:

1. Select **Check this box to set the Discovery Notification** to enable the data entry fields.
2. If administrator users were not previously added, then only the built-in user account is listed. If this account was not modified before you started the **Discovery Wizard**, then specify the recipient of the e-mail notification.
3. Indicate the mail server that will be used to generate the notification:
   - **Discovery Notification Destination** Keep the selections next to the administrators who should receive a notification. Otherwise, clear the appropriate boxes. If administrator users were not previously added, then only the built-in user account is listed. If this account was not modified before you started the **Discovery Wizard**, then enter the e-mail address of the person who will receive the notification; for example, Lin@Hitachi.com. You can enter up to 255 characters, provided that they are not control codes, and the characters must exist before and after the ampersand, @.
   - **Outgoing SMTP Server Setting** Specify the settings that are associated with the mail server, such as the SMTP **Server Name** and **Port** number.
   - **Secure Connection** To connect to the SMTP server using a secure connection, indicate the security protocol that you want to use. Note that a default port is used for the SSL option (465), and for the TLS option (465).

     If authentication is required, check the **Use Authentication** box, and enter the administrator's **User Name**. If you are using authentication, and you want to change the password for the SMTP server, then select **Check this box to change the password**, and enter the password information.

4. To verify that the e-mail addresses specified in the **Discovery Notification Destination** are valid, click **Send Test E-Mail**. Clicking the button launches a confirmation message that indicates that an e-mail with the subject, [TEST], will be sent to the addresses.

NOTE: A test e-mail cannot be sent unless at least one e-mail address has been specified in the **Discovery Notification Destination**. If the e-mail cannot be sent to a particular recipient, then a message stating so displays. Also, An e-mail notification is not sent when rediscovering troubleshot nodes in either the **Discovery Log** or within the **Troubleshooting** dialog of the **Discovery Wizard**.

5. Click **Next** to proceed to the next panel of the **Discovery Wizard**.

Continue or Finish

In the last step of the **Discovery Wizard**, **Continue or Finish**, you have several options. You can:

- **Review a summary of all the nodes that were identified**, and whether they were successfully discovered, are currently monitored, or if there were discovery errors. If you do not have other changes to make, such as adding other credentials or IP address ranges, then exit the **Discovery Wizard** by clicking **Finish**. Afterward, the **Monitoring** module launches and displays the topology of your environment.

  For information about the Topology View, refer to the Help topic, “Reviewing the Topology of the Monitored Environment” contained in the Help book, “Monitoring Your Environment”.

- **Add IP address ranges**. To include additional IP address ranges, click **Add IP Address Range**. You will return to the **Specify IP Address Ranges** panel.
- **Add credentials**. To include additional credentials, click **Add Credentials**. You will return to the **Specify Credentials** panel.
- **Change the default discovery schedule**. Future discoveries are scheduled every week, Sunday at midnight. You can specify a different schedule by clicking **Edit Discovery Schedule**.

Accessing the Discovery Wizard

In the future, if you need to launch the wizard and make changes to the discovery profile, you can do so by selecting **Start Discovery Wizard** from the **Go** menu.

Figure 5-2: Discovery Access from the Go Menu

You can also make discovery configuration changes within the **Configuration** panel of the **Settings** module.

6

Starting to Monitor

After IT Operations Analyzer completes the discovery of your system components, you can select the nodes you want to monitor. This chapter provides information about checking the discovery results and selecting nodes. It includes a roadmap for other tasks that you can complete, such as managing nodes and customizing settings.

- Selecting the Nodes to be Monitored
- Looking Forward: Task Recommendations
- Additional monitoring and connection information

Selecting the Nodes to be Monitored

After the discovery process has completed, the results are reflected in the:

- **Last Discovery Status** panel of the **Home** module
- **Discovered Nodes** panel of the **Settings** module

Figure 6-1 provides an example of the lower portion of the **Discovered Nodes** panel. The **Discovery** column indicates the discovery success or issue that is associated with each node.

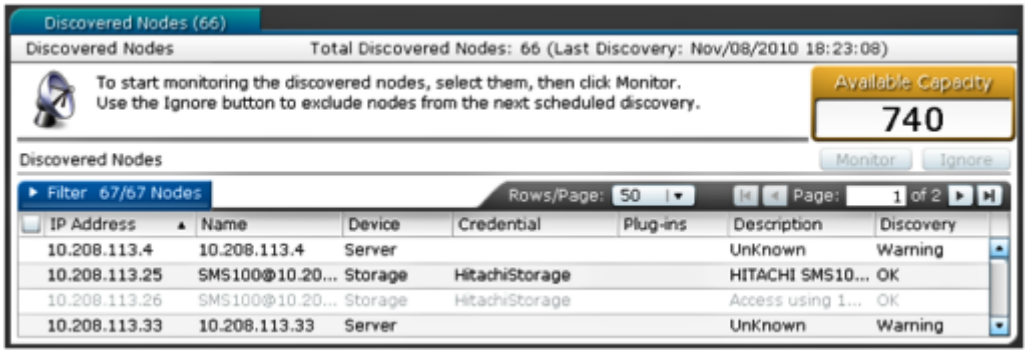

Figure 6-1: Discovered Nodes in the Settings Module

Depending on the discovery results, administrators who have IT Operations Analyzer Admin permissions may have several different node management options. The text in parenthesis indicates the discovery status, which is indicated in the **Discovery** column:

- Nodes with a normal status (**OK**) can be monitored. Monitored nodes are listed in the **Monitored Nodes** panel.
- Nodes with a normal status (**OK**) can be excluded from the monitoring routine, and future discoveries. Excluded nodes are listed in the **Ignored Nodes** panel.
- Nodes that could be reached, but have an issue (**Warning**) can be reviewed.

NOTE: For information about nodes that have any associated errors, please refer to the **Last Discovery Log** panel of the **Settings** module.

In addition to the node's discovery status, the following information is provided:

- **IP Address** This indicates the IP address of the discovered node.
- **Name** This indicates the name of the discovered node.
- **Device** This indicates the device type (Server, Storage, Network Device).
- **Credential** This indicates the server authentication protocol that is currently in use, and that corresponds to the IP Address. Clicking the column heading lets you change the current sort order.
- **Plug-ins** This indicates the plug-in that is used by the node.

- **Description** This is a description of the device. For a Server device, the OS, Vendor, Model, Serial number are displayed. For a Storage or Network Device, the firmware version, Vendor, Model, and Serial number are displayed.

  If a particular node has multiple IP addresses, then only the primary address is in black text. The remaining addresses are listed in grey text and cannot be updated.

  Nodes for which the software could not determine the device type, such as a server or switch, are indicated by **Unknown**.

NOTE: During discovery processing, IT Operations Analyzer identifies the nodes to be monitored by the node identifier (Node ID). So, even if there are identical IP addresses, nodes are distinguished by the Node ID. In the case where a node does not have credentials defined for it, it will be identified as an **Unknown** node in the discovery results, and IT Operations Analyzer assigns a Node ID. Later on, if your site specifies credentials for that node, and, for example, the protocol is specified as WMI, then in the subsequent discovery processing, your site will see two versions of the node in the discovery results. In this case, the Node ID that IT Operations Analyzer had previously assigned differed from the host name, so it was regarded as a different node.

When selecting the nodes to be monitored, we recommend including both the management server and network devices that connect the management server to the monitored nodes. This improves the accuracy of any future Root Cause Analysis.

Sorting Information

There are two ways to adjust the display of information in the **Discovered Nodes** list. You can:

- Click the arrow in the **Filter** tab to sort information by:
  -All Devices (or, a specific device)
  -All Monitoring Statuses (or, a specific status)
  -All Discovery Statuses (or, a specific status)
- Click column headings, except for the **Plug-ins** column, to change the sort order of information.

To select the nodes to be monitored:

1. Open the **Settings** module.
2. From the **Settings Menu**, go to the **Discovery** section, then click **Discovered Nodes**.
3. Check the box in the **IP Address** column for the nodes with the **OK** status that you want to monitor.
4. Click **Monitor**.

From now on, you can manage monitored nodes in the **Monitored Nodes** panel of the **Settings** module. Note that the available capacity that is associated with your license decreases accordingly.

Looking Forward: Task Recommendations

At this point of the getting started process, you have some task options to consider. Table 6-1 outlines the types of tasks that you will likely complete frequently, occasionally, and as needed, once monitoring has begun. The table is provided as a general guideline for typical task functions, but actual tasks and their frequency depend on your monitored environment.

The column, Online Help Book, indicates where you can locate related topics (overviews and instructions).

Table 6-1: Task Guidelines

Frequent Tasks			
Task	**Details**	**Module**	**Online Help Book**
Check for discovered nodes.	If you set up an e-mail notification when a scheduled discovery is complete, check the results in the Discovered Nodes panel of the Settings module. You can also check the discovery status in the Home module.	• Home • Settings	Discovering Your Environment
Manage discovered nodes.	When nodes are discovered, check their status and determine how you want to handle them: -Ignore the nodes -Monitor the nodes -Modify node settings	Settings	Managing Nodes
Respond to event notifications.	Based on the different types of reports that can be defined in the Settings module, different administrators can review and acknowledge events.	• Monitoring • Events	• Monitoring Your Environment • Evaluating and Addressing Events and Failures
Troubleshoot events.	Use the root cause analysis (RCA) feature to determine the source of the event, its impact on other areas, and troubleshoot it.	• Monitoring • Events	
Check operational status of your monitored environment.	Refer to the Home module for a quick overview of system statuses. Use reports in the Reports module to check operating rates and performance for resource groups, devices, networks, and so on.	• Home • Reports	Monitoring Your Environment
Occasional Tasks			
Task	**Details**	**Module**	**Online Help Book**
Manage IT Operations Analyzer administrator accounts.	• Add user accounts • Change user accounts • Delete user accounts	Settings	Managing Users (within Customizing Settings)
Change reports.	Modify reporting options and e-mail recipients.	Settings	Customizing Settings

Table 6-1: Task Guidelines

As Needed Tasks			
Task	**Details**	**Module**	**Online Help Book**
Change the discovery configuration.	Make changes to the monitoring interval, recipient(s) of the discovery notification, and so on.	Settings	Customizing Settings
Optionally set up Resource Groups.	Resource Groups are groups of related devices. You can group all nodes that support a particular application, such as Oracle, SQL, Microsoft Exchange, or nodes that are used to support a particular business function, such as your finance or human resources departments.	Use either the Settings module or the Monitoring module.	Working with Optional Settings
Optionally establish and manage templates.	Add, edit, and remove templates that can be applied to servers, storage, and switches, for alert thresholds; and to Windows, Linux, and Solaris services, for monitoring purposes.	Settings	
Manage installed plug-ins.	If your site installed plug-ins on the management server, then you can use the Plug-in Control feature to complete tasks such as checking plug-in information and taking plug-ins offline as part of scheduled maintenance activities,	Settings	Managing Plug-ins
Upgrade your license.	When your monitoring capacity is reaching its limit, you can continue to add newly discovered nodes by upgrading your license.	Settings	Working with Licenses (within Activating Your License)
Maintain the IT Operations Analyzer database.	Plan and implement a backup schedule for both the database repository and environmental setting file. Also, if your site plans to upgrade its monitoring capacity, check that there is sufficient disk space, and expand it, if necessary.	(Not Applicable)	Managing the IT Operations Analyzer Database
Correct problems.	Review fixes relating to discovery issues and error messages.	Settings	Troubleshooting Guidelines
Upgrade the software.	In the future, your site may want to upgrade to the next version of the software.	(Not Applicable)	Upgrading IT Operations Analyzer
Uninstall the software.	Normally, this is not required unless warranted by extreme error conditions.	(Not Applicable)	Uninstalling IT Operations Analyzer

Table 6-1: Task Guidelines

As Needed Tasks			
Task	**Details**	**Module**	**Online Help Book**
Check connections to a selected node.	Plan volume backups and migrations by viewing connection and mapping access points to a selected node. Check the status of access points to the node.	Monitoring	Monitoring Your Environment

Additional monitoring and connection information

IT Operations Analyzer Version 3.3.0 and later provide enhanced monitoring of connection information. Following provides additional notes about connection information that affects monitoring of your site.

- The FC networks information of host machines and virtual machines that are connected with virtual switches are not displayed.
- IT Operations Analyzer may monitor ports that have the same MAC address. Consequently, connections of ports that have the same MAC address may not be displayed correctly.
- In the **Connections** tab of the **Monitoring** module, connection information to the IP switch and IP network consists of addresses, based on the ARP table information collected from the IP switch during the configuration acquisition period from ethernet subnets. As a result, connection information might not be acquired from a port, if communication does take place during this acquisition period However, "indirectly" connected addresses may be displayed, even if network cables from the node are not directly connected to the IP switch. This is possible because communication between the node port and IP switch (through a subnet) had occurred during configuration acquisition of the ARP table.

7

Upgrading the software

This chapter describes the preparations your site should make before upgrading to a major software release. A major release is identified by the product version number in our Release Notes: 3.2.1, for example, is a major release but 3.2.1-01 is not.

Overview

If your site is currently working with an installed, purchased version of IT Operations Analyzer, then you can choose to upgrade to the latest software version. Upgrading is recommended in order to take advantage of recent product enhancements and other features.

After a decision is made to upgrade, the next steps you will take depend on the status of your Software Maintenance contract:

- If your site's Software Maintenance is active, then you can install the software upgrade and proceed with the license activation.
- If your site's Software Maintenance has expired, then you need to purchase a new license in order to upgrade.

You have two choices for checking the status of the Software Maintenance: You can either confirm the status:

- within the License Activation wizard, or
- by referring to the IT Operations Software Portal before using the License Activation wizard.

The following section describes how to check the status before using the License Activation wizard.

Preparing for the upgrade

You can determine whether your site's Software Maintenance is active from the IT Operations Software Portal:

1. Launch the IT Operations Software Portal: http://www.itoperations.com
2. From the menu bar, click **Sign In**.
3. Enter the **login ID** and **Password** for your site. Then, click **Sign-in**.

NOTE: This is the ID and Password that were provided when you (or a contact for your site) previously registered on the IT Operations Software Portal.

4. Click the **My Account** tab and review the section, **My Products and Licenses**.
   - If your account has an **Active** status, then you can start upgrading, and activate the license afterward. You do not need to note the **Activation Token**--it will automatically be displayed within the License Activation wizard.
   - If your account is no longer active, then purchase a license. Your purchase will include a new Activation Token.
5. After you have the valid Activation Token, proceed to the next section, Upgrading.

Upgrading

Once you have determined the Software Maintenance status, and have secured the Activation Token, you are ready to upgrade.

Following is an outline of the upgrade procedure and references to the related sections in this manual:

1. **Installing the software**.

   Complete the steps in Chapter 2, Installing the software.

NOTE: If your site encounters a database import error during the upgrade process, then please refer to Chapter 8, Resolving installation issues.

2. **Logging in**.

   Complete the steps in Chapter 3, Launching the login panel.

3. **Activating the license**.

   Complete the instructions based on whether you are currently connected to the Internet. If you are:

   - Online, see Chapter 3, Online activation.
   - Offline, see Chapter 3, Offline activation.

NOTE: After you have completed an upgrade installation, your license may automatically revert to a trial status, with a usage limit of the trial period. After you upgrade, check the status of your license. If the license is a trial one, then complete the license activation process before the trial license expires.

8

Troubleshooting

This chapter addresses any issues that your site might experience with the installation process, and the discovery notification. It also includes guidelines for resolving those issues.

- Resolving installation issues
- Resolving issues with the discovery process: Scan results
- Resolving issues with the discovery notification
- Collecting log data

Resolving installation issues

Based on the information provided in the Installation Wizard, and other factors, such as available disk space, certain alert messages might be presented. Unless the cause of the issue is resolved, the installation cannot proceed.

To help you identify the issue you may have encountered, refer to the following list of issues, then review the Possible Causes and Solution columns for the troubleshooting guidelines.

Table 8-1: Installation Issues and Solutions

Issue	Possible Causes	Solution
I received the following message, and I cannot run the Installation Wizard: **The Microsoft Windows Administrator privilege is required for installation**.	You might not be logged in with the right permissions.	Make sure that you have logged onto the management server with Administrator group privileges. Then, restart setup.exe.
I received the following message during the installation: **There is insufficient disk space in the specified storage location of the database file. Please change the storage location**.	Either the drive that was used as the installation destination, or the specified installation destination does not have enough capacity.	Either create more space or specify a different installation destination. Then, continue with the installation.
I received a **non-usable character** message.	A mistake was made when entering information in the Installation Wizard (for example, a port number has a letter and numbers instead of numbers).	Check the information that was provided and make corrections, as needed.
I received either of the following messages: • IT Operations Analyzer setup failed. A lack of memory occurred when setting up the database. • IT Operations Analyzer setup failed. A lack of memory occurred when creating a database table.	The capacity of the Windows desktop heap is insufficient.	Check the capacity of the Windows desktop heap.

Table 8-1: Installation Issues and Solutions

Issue	Possible Causes	Solution
I received a database import error during the upgrade installation of IT Operations Analyzer.	An unforeseen problem occurred when importing database data, during the software upgrade.	Recover the database data. The following is the database recovery procedure: 1. Back up the export data folder, ITOA_exportdata, to a new, backup directory. 2. Uninstall IT Operations Analyzer. 3. Reinstall the upgrade version of IT Operations Analyzer. 4. Import the data you backed up at step 1, using the import command: import -f <Backup data location>
I received the following message: It is necessary to start the Analyzer service manually. After the installation has completed, run the following command from the IT Operations Analyzer command prompt: “controlservice.exe -a start”	Some (or all) of the IT Operations Analyzer services have not started.	On the management server, start the IT Operations Analyzer service manually: **Note**: On Windows Server 2012, the steps to navigate to the **Analyzer Command** are different. 1. Click **Start** and select **All Programs**. 2. Click **Hitachi IT Operations** and run the **Analyzer Command**. **Note**: 'Hitachi ITOperations' may be named differently, depending on the name that was used for the program folder, during the product installation. 3. Enter the command: controlservice.exe -a start
I received the following message: This file is broken.	The setup.exe file was launched from a folder containing double-byte character codes.	Switch to a folder that does not contain double-byte character codes, then run the setup.exe again.

Resolving issues with the discovery process: Scan results

When working within the Discovery Wizard, after a scan of the IP addresses is completed, and if the host name is not listed within the scan results, then it is possible that IT Operations Analyzer could not complete a reverse lookup of the target host name.

In this case, check the following:

- Confirm whether it is possible to complete a reverse pull of the target host's host name from the server on which IT Operations Analyzer is installed.
- Confirm the root of the server to use for the server name solution (DNS, WINS) and confirm the server on which IT Operations Analyzer is installed.

Resolving issues with the discovery notification

If no discovery notification e-mail was sent after the discovery process completed, then refer to the following troubleshooting guidelines.

Table 8-2: Causes of the Discovery Notification Issue and Solutions

Possible Causes	Solution
The e-mail address might not be configured for the user account, or it might be incorrect.	1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **User Admin** section and click **User Management**. 3. Locate the user account to which you want to send the e-mail notification, then click **edit**. 4. In the e-mail area, enter an appropriate e-mail address, then click **OK**.
The e-mail recipient might not be specified.	There are two settings that might affect event notification: Notification level and filter conditions. Notification level determines what level of severity triggers a notification, and filter conditions determine what device type, event category, or resource group triggers a notification. For more information on filter conditions, see the *Hitachi IT Operations Analyzer Help*. **To verify the notification settings**: 1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **Reports** section and click **Discovery Notification**. 3. Select **Discovery Configuration**. 4. For the **Notification of Discovery Completion**, click **edit**. 5. For the **Discovery Notification Destination**, select the e-mail recipient. 6. Click **OK**.
The server name or port for the outgoing server might be incorrect.	1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **Reports** section and click **Outgoing Server**. 3. Verify the **Server Name** and **Port** settings and make changes, as needed. 4. Click **Save**.
The Use Authentication option of the Outgoing Server is enabled for SMTP Authentication; however, the User Name or Password might be incorrect.	1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **Reports** section and click **Outgoing Server**. 3. For the **Use Authentication** setting, verify the **User Name** and **Password**. Make changes, as needed. 4. Click **Save**.
The Use Authentication option of the Outgoing Server might be disabled for SMTP Authentication.	1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **Reports** section and click **Outgoing Server**. 3. Verify that the **Use Authentication** setting is selected. 4. Specify the **User Name** and **Password**. 5. Click **Save**.

Table 8-2: Causes of the Discovery Notification Issue and Solutions

Possible Causes	Solution
The Secure Connection setting for the Outgoing Server is enabled for the SSL/TLS capable server. However, the port number might be invalid.	1. Within IT Operations Analyzer, open the **Settings** module. 2. From the **Settings Menu**, locate the **Reports** section and click **Outgoing Server**. 3. Verify whether the **Secure Connection** setting is used. 4. Confirm that the **Port** value is correct, then click **Save**.
The mail server might not have been started.	Confirm the server's status.

Collecting log data

In the event that a failure occurs with IT Operations Analyzer which requires you to contact Hitachi Data Systems Support, you may be asked to provide information from log files. Information may be required from the following sources to help resolve the failure:

- Any messages that were displayed in the software
- IT Operations Analyzer message log files
- Windows event logs

If these sources do not provide sufficient information, you may be asked to use the Reliability, Availability, and Serviceability (RAS) collection command to collect information from IT Operations Analyzer. The RAS collection command allows you to access information such as:

- Operating system environmental information
- System or application event logs, and general trace logs
- IT Operations Analyzer data

NOTE: The following instructions require the use of commands. Only ASCII characters can be used when specifying the name of a directory or file. If the name of the directory or file contains any single-byte spaces, then the name must be enclosed by quotation marks: “”

Understanding the Command Format and Arguments for the RAS Collection Command

When needed, you will run the RAS collection command (getlogs.exe) to collect the failure data. The **getlogs.exe** command is located in the following directory: <*IT Operations Analyzer installation directory*>\bin

Following is the example command format (the underscores ‘_’ represent a single byte space):

getlogs.exe_{-f_<*output directory name*>[_-s][_-n][_-w_<*temporary working directory name*>]|-h}

Following are the details of each command option:

- -f: Indicates the name of the directory in which to output the collected information. Specify a full or relative path.
- -s: When the ITOARasInfo directory located below the specified directory already exists, specify this argument when you are not asked if it is permissible to remove the directory.
- -n: Indicates that the data file that is exported to the database is not collected.
- -w: This is the temporary working directory, which is specified by a full or relative path. The temporary working directory is a maximum of 54 strings with a path changed to a full path. When the temporary working directory is not specified, a directory that is set to an environment variable becomes the current working directory.
- -h: Outputs the Help for the getlogs.exe command.

For more information about the command options, refer to the *Hitachi IT Operations Analyzer Help*.

To use the RAS collection command for IT Operations Analyzer:

CAUTION! Use this command only within the context of troubleshooting a failure situation, and with the specific data collection instruction / guidance provided by the Hitachi Data Systems Support contact. It is important to contact support as soon as possible, because after a certain period of time, the log records containing information about the problem might be lost.

1. On the Management server, open the **Windows Start** menu.
2. Click **All Programs**, [Hitachi IT Operations], then **Analyzer Command**.

NOTE: *Hitachi IT Operations* may be named differently, based on the name that was used for the program folder, during the product installation.

On Windows Server 2012, the steps to navigate to the **Windows Start** menu and **Analyzer Command** are different.

3. Type the following command (for example purposes, the underscores '_' represent a single byte space):

   getlogs.exe_{-f_<*output directory name*>[_-s][_-n][_-w_<*temporary working directory name*>]|_-h}
4. Provide the data that is requested by the Hitachi Data Systems Support contact.

Understanding the Command Format and Arguments for the RAS Collection Command on the ODBC or JDBC client system

When needed, you will run the RAS collection command (getlogs4client.exe) to collect failure data on the ODBC or JDBC client system. The getlogs4client.exe command is located in the following directory: <IT Operations Analyzer ODBC/ JDBC installation directory>\bin

Following is the example command format (the underscores '_' represent a single byte space):

getlogs4client.exe_{-f_<*output directory name*>[_-s][_-c]|-h}

Following are the details of each command option:

- -f: Indicates the name of the directory in which to output the collected information. Specify a full or relative path.
- -s: When the ITOA_CRasInfo directory located below the specified directory already exists, specify this argument when you are not asked if it is permissible to remove the directory.
- -c: Prevents collecting the RAS information that the getlogs.exe command normally collects.
- -h: Output the help for the getlogs.exe command.

To use the RAS collection command on the ODBC or JDBC client system:

NOTE: On Windows Server 2012, the steps to navigate to the **Windows Start** menu and Command Prompt are different.

1. On the client system, open the **Windows Start** menu.
2. Launch the Command Prompt.
3. Go to the <ODBC/JDBC *installation directory*>/bin and type the following command (for example purposes, the underscores '_' represent a single byte space):

   getlogs4client.exe_{-f_<*output directory name*>[_-s][_-c]|_-h}
4. Provide the data that is requested by the Hitachi Data Systems Support contact.

For more information, refer to the *Hitachi IT Operations Analyzer Help*.

Glossary

This glossary provides definitions of general storage networking terms as well as specific terms related to the technology that supports IT Operations Analyzer. Click the letter of the glossary section to display that page.

A

Activation Token

This is an alphanumeric code that identifies the license and the number of supported nodes.

Admin

This is an administrator account where the permissions have been set to allow viewing, adding, editing, and deleting information, including account information pertaining to other administrators.

API

An Application Programming Interface is a set of functions, procedures, methods, classes or protocols that an operating system, library, or service provides to support requests made by computer programs.

C

Capacity

The amount of information (usually expressed in megabytes) that can be stored on a disk drive. It is the measure of the potential contents of a device; the volume it can contain or hold.

CIM

The Common Information Model is a standard that is defined by the Distributed Management Task Force (DMTF). It defines how elements that are managed within an IT infrastructure are handled as a common set of objects. As a result, these elements can be managed consistently, and without any dependencies on the vendor or the manufacturer.

Client Machine

This is a computer that is used to access the management server.

D

DCOM

The Distributed Component Object Model is Microsoft's technology for software components that are distributed across several networked computers. This is so that the components can communicate with each other.

DMTF

The Distributed Management Task Force is an organization that develops and maintains standards for systems management of IT environments in enterprises and the Internet.

F

Fabric

The hardware that connects workstations and servers to storage devices in a SAN. The SAN fabric enables any-server-to-any-storage device connectivity through the use of Fibre Channel switching technology.

FC

A Fibre Channel is a serial computer bus intended for connecting high-speed storage devices to computers.

fcinfo

The Fibre Channel Information tool is a Microsoft product that runs on certain Microsoft Windows Server systems. It discovers the SAN resources and configuration information on your Fibre Channel SAN.

Firmware

Software embedded into a storage device. It may also be referred to as Microcode.

H

HBA

Host bus adapter, a circuit board and/or integrated circuit adapter installed in a workstation or server that provides input/output processing and physical connectivity between a server and a storage device. An iSCSI HBA implements the iSCSI and TCP/IP protocols in a combination of a software storage driver and hardware.

HTTP

HyperText Transfer Protocol is a request and response standard between a client (the user) and a server (the Web site). Any resources to be accessed by HTTP are identified using Uniform Resource Locators (URLs) using http or https.

I

I/O

Input/output refers to the communication signals that are sent (input) by a person (or computer) to an information processing system, and the data that is returned (output) by that system.

IP

Internet Protocol, specifies the format of packets and addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255 (for example, 192.168.0.200).

K

Kernel

Connects the application software to the computer's hardware.

L

LAN

Local Area Network, a computer network that spans a relatively small area, such as a single building or group of buildings.

M

Management Server

This is the server on which IT Operations Analyzer has been installed.

MIB

A Management Information Base is used for device management in a communications network. This type of database is made up of a collection of objects in a virtual database for managing components in a network.

Monitoring Targets

Refers to the nodes (computers, storage, switches) that you intend to monitor.

MSCS

Refers to the Microsoft Cluster Service.

N

Namespace

Refers to conceptual space that groups classes, identifiers, and so on to prevent problems with items that have the same names, and that are used in other code.

NAS

Network Attached Storage. A computer that is connected to a network, and provides storage services to other clients and devices on the network.

Node

Refers to the targets of IT Operations Analyzer monitoring: computers, switches, storage, and so on.

O

Operator

This is an administrator account where the permissions have been set to allow viewing, adding, editing, and deleting information, except account information pertaining to other administrators.

R

RAS

Reliability, Availability, and Serviceability (RAS) collection command. This command is used to collect data from IT Operations Analyzer, such as operating system environmental information, system or application event logs, and general trace logs.

RCA

A Hitachi proprietary feature of IT Operations Analyzer, Root Cause Analysis provides the top root causes for a critical event. This important feature helps administrators accurately pinpoint the source of the problem, for troubleshooting purposes.

S

SAN

Storage Area Network, a network of shared storage devices that contain disks for storing data.

SMI-S

The Storage Management Initiative Specification defines DMTF management profiles for storage systems.

SMTP

The Simple Mail Transfer Protocol is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SNMP

The Simple Network Management Protocol monitors network-attached devices for any alerting conditions.

SSH

Secure Shell is a network protocol that is mostly used on Linux and Unix® based systems. It allows data to be exchanged using a secure channel between two networked devices.

SSL

Secure Socket Layers are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet.

Switch

A network infrastructure component to which multiple nodes attach. Switches have internal bandwidth that is a multiple of link bandwidth, and they can rapidly switch node connections from one to another. Usually, switches can accommodate multiple, simultaneous full link bandwidth transmissions between different pairs of nodes.

T

TCP

Transmission Control Protocol provides reliable, ordered delivery of a stream of bytes from one program on one computer to another program on another computer.

TCP/IP

Transmission Control Protocol/Internet Protocol is the set of communications protocols used for the Internet and other similar networks.

U

UDP

With the User Datagram Protocol, programs on networked computers can send short messages to one another, using Datagram Sockets.

V

View

This is an administrator account where the permissions have been set to allow viewing information, only.

W

WBEM

Web-Based Enterprise Management is a set of systems management technologies developed to unify the management of distributed computing environments. It is based on Internet standards and Distributed Management Task Force (DMTF) open standards.

Web Browser

A software application, such as Internet Explorer, Safari, Firefox, and Google Chrome, that allows users to access the World Wide Web, and obtain information from a Web page at a Web site, or from a local area network (LAN).

WMI

Windows Management Instrumentation is Microsoft's implementation of the WBEM and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF).

Index

M

N

O

P

R

S

T

U

V

W

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2629
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-98IOS001-15