



User Guide for Cisco TelePresence Readiness Assessment Manager

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for Cisco TelePresence Readiness Assessment Manager
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface	v
Audience	v
Conventions	v
Product Documentation	vi

CHAPTER 1

Introduction	1
What Is Cisco TelePresence Readiness Assessment Manager?	1
Is TelePresence Readiness Assessment Manager Ready to Use?	2
What Is the Dashboard?	3
Getting Started with TelePresence Readiness Assessment Manager	4
Starting TelePresence Readiness Assessment Manager	4
Working with TelePresence Readiness Assessment Manager Windows	4
Using Help	5
Understanding the Displayed Dates and Times	5
Using Displays and Reports	5

CHAPTER 2

Device Management	1
Getting Started with Device Management	1
Understanding the DCR	2
Using TelePresence Readiness Assessment Manager to Add Devices	2
Running TelePresence Readiness Assessment Manager Physical Discovery	2
Filtering Devices for Autodiscovery	3
Editing Device Credentials	5
Modifying Traceroute Paths	6
Viewing Device Discovery Status	6
Selecting Devices for Assessment	7

CHAPTER 3

Inventory Collection and Device Classification	1
Starting Inventory Collection	1
Viewing Inventory Collection Status	2
Modifying Device Classification	2

CHAPTER 4

Compliance, Performance, and TelePresence Traffic Assessment 1

- Running Compliance Analysis 1
- Running Performance Analysis (Creating a Performance Study) 2
 - Viewing Performance Study Details 3
 - Changing Device Poll Settings 3
- Running Telepresence Traffic Analysis 3
 - Installing the Media Traffic Analysis Agent on a System 4
 - Managing Agents 4
 - Managing Simulated TelePresence Traffic Tests 6
 - Viewing Raw Data from Agents 8

CHAPTER 5

Reports 1

- Completing the Questionnaire 1
- Generating the Report 1
- Viewing Reports 2
 - Executive Report 2
 - Performance Utilization Report 2
 - Utilization Calculation Example 1 3
 - Utilization Calculation Example 2 5
 - Compliance Analysis Report 7
 - Traffic Simulation Report 7

CHAPTER 6

Administration 1

- Setting Up Notifications 1
- Configuring Logging Levels 1

APPENDIX A

Appendix A: Open Source License Notices 1

- Notices 1
 - OpenSSL/Open SSL Project 1
 - License Issues 1

INDEX



Preface

This manual describes Cisco TelePresence Readiness Assessment Manager and provides instructions for using and administering it.

Audience

The audience for this document are administrators who want to assess their network's readiness for IP communications deployment.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	<code>screen</code> font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option>Network Preferences
Selecting a menu item in tables	Option>Network Preferences



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation


Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Release Notes for Cisco TelePresence Readiness Assessment Manager 1.0</i>	<ul style="list-style-type: none"> In PDF on the product CD-ROM On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps8542/prod_release_notes_list.html
<i>Quick Start Guide for Cisco TelePresence Readiness Assessment Manager 1.0</i>	<ul style="list-style-type: none"> In PDF on the product CD-ROM On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps8542/prod_installation_guides_list.html
<i>User Guide for Cisco TelePresence Readiness Assessment Manager 1.0</i>	<ul style="list-style-type: none"> In PDF on the product CD-ROM On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps8542/products_user_guide_list.html
<i>Deployment Guide for Cisco TelePresence Readiness Assessment Manager 1.0</i>	On Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps8542/products_installation_and_configuration_guides_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Introduction

These topics provide an overview of Cisco TelePresence Readiness Assessment Manager :

- [What Is Cisco TelePresence Readiness Assessment Manager?](#)
- [Is TelePresence Readiness Assessment Manager Ready to Use?](#)
- [What Is the Dashboard?](#)
- [Getting Started with TelePresence Readiness Assessment Manager](#)

What Is Cisco TelePresence Readiness Assessment Manager?

Cisco TelePresence Readiness Assessment Manager (TelePresence Readiness Assessment Manager) evaluates your network and reports its readiness to deploy the Cisco TelePresence solution in your network. TelePresence Readiness Assessment Manager analyzes your network infrastructure to detect recommended best-practice noncompliances, determine the resource utilization, and assess your network's capability to carry telepresence media traffic. It uses open interfaces, such as Simple Network Management Protocol (SNMP) and Telnet/SSH, to remotely poll read-only data from different devices in deploying a Cisco TelePresence solution.

TelePresence Readiness Assessment Manager has the following key features:

- Automates assessment and increases productivity for network managers.
- Ensures that the network can carry telepresence traffic through a detailed analysis of the current network device configuration and setup.
- Provides telepresence traffic simulation to predict the number of telepresence calls that the network can accommodate and an insight to any voice and video impairment factors.
- Provides customized reports that can provide results and suggestions from recorded analyses and traffic simulation.

Three main tools assess your network:

- [Compliance Analysis](#)
- [Performance Analysis](#)
- [Traffic Analysis](#)

After running these tools, you can view three types of [reports](#) that provide you with analysis information and recommendations for your network.

Is TelePresence Readiness Assessment Manager Ready to Use?

The instructions for installing and configuring TelePresence Readiness Assessment Manager are included in the *Quickstart Guide for Cisco TelePresence Readiness Assessment Manager*.

To use TelePresence Readiness Assessment Manager, you must import devices into the TelePresence Readiness Assessment Manager inventory. See [“Using TelePresence Readiness Assessment Manager to Add Devices” on page 2](#) for more information. TelePresence Readiness Assessment Manager obtains devices to poll from the Common Services Device and Credentials Repository (DCR).

Before TelePresence Readiness Assessment Manager can analyze your network:

- You must discover and select devices in your network.
- TelePresence Readiness Assessment Manager must complete inventory collection.

[Table 1-1](#) lists the steps you must take before using TelePresence Readiness Assessment Manager.

Table 1-1 Adding and Classifying Devices

	Description	References/Notes
Step 1	Add and discover devices. <ul style="list-style-type: none"> • Use TelePresence Readiness Assessment Manager to add devices by using auto discovery. • Add devices manually. • Use a seed file to import devices into the DCR. 	See Chapter 2, “Device Management.” We recommend that you use traceroute auto discovery. This enables TelePresence Readiness Assessment Manager to discover and add all devices in a path (using pathname and source/destination devices) into DCR. More importantly, generated reports provide assessment based on these traceroute paths.
Step 2	Select devices for assessment.	This step is optional. By default, all devices are automatically included in all assessment operations. See “Selecting Devices for Assessment” section on page 2-7.
Step 3	Start inventory collection on selected devices.	See Chapter 3, “Inventory Collection and Device Classification.”
Step 4	Configure device classification.	This step is optional. By default, devices are automatically classified by TelePresence Readiness Assessment Manager. See Chapter 3, “Modifying Device Classification.”

After you import devices, TelePresence Readiness Assessment Manager is ready to analyze your network. [Table 1-2](#) lists tasks that you can attend to after initially configuring devices.

What Is the Dashboard?

The dashboard is the first window that opens when you start TelePresence Readiness Assessment Manager. The dashboard displays a typical user workflow. The icons also provide quick shortcuts to the tasks you want to do. The dashboard also contains a time stamp of all completed or running processes.

Getting Started with TelePresence Readiness Assessment Manager

These topics help you to work with and understand the TelePresence Readiness Assessment Manager user interface:

- [Starting TelePresence Readiness Assessment Manager, page 1-4](#)
- [Working with TelePresence Readiness Assessment Manager Windows, page 1-4](#)

Starting TelePresence Readiness Assessment Manager

To start TelePresence Readiness Assessment Manager from the Windows desktop, select **Start > Programs > Cisco TelePresence Readiness Assessment Manager 1.0**.

To start TelePresence Readiness Assessment Manager, from a browser, enter `http://<machine name>:1741`.

**Note**

If Enhanced Security is enabled on the Windows 2003 system, you must add the TelePresence Readiness Assessment Manager home page to the Internet Explorer Trusted Sites Zone. Otherwise, you will not be able to access it until it is added to the trusted sites. (See [Working with TelePresence Readiness Assessment Manager Windows, page 1-4](#).)

Working with TelePresence Readiness Assessment Manager Windows

This topic focuses on questions you might have when you first start to work with the TelePresence Readiness Assessment Manager user interface:

- [Why are multiple windows open?, page 1-4](#)
- [When I press the Enter key, why doesn't TelePresence Readiness Assessment Manager complete the current task?, page 1-4](#)
- [Where is the Help button?, page 1-5](#)

Why are multiple windows open?

For ease of use, TelePresence Readiness Assessment Manager opens separate browser windows for many displays. Having multiple windows open enables you to:

- Refer to information from one window to complete a task in another window.
- Rapidly compare information on different window.

When TelePresence Readiness Assessment Manager opens a new browser window, it does not close previously opened windows. You can close browser windows manually when you are done with them.

When I press the Enter key, why doesn't TelePresence Readiness Assessment Manager complete the current task?

TelePresence Readiness Assessment Manager does not accept pressing the Enter key as a substitute for clicking buttons, such as **OK**, **Finish**, or **Next**, on the application page.

Where is the Help button?

The Help button is located in the top right corner of the window.

Using Help

To start help, click the **Help** button in the top right corner. If a display is open, click the question mark icon.



Note If you selected an option in the navigation tree, the context-sensitive help for that option is displayed.

Help is displayed in a separate browser window that remains open until you close it. Online help includes an index and search capability.

Understanding the Displayed Dates and Times

Dates and times displayed by TelePresence Readiness Assessment Manager reflect the date, time, and time zone set on the server of which TelePresence Readiness Assessment Manager is installed. If the client system you use to run TelePresence Readiness Assessment Manager is located in a time zone other than the time zone set on the server, you will notice the difference; for example:

- Status “as of” the current date and time will not display your local time and time zone and might not match your local date.
- Dates and times shown for previous events are recorded (and displayed) with the server time stamp, which is offset from your local time.

Using Displays and Reports

TelePresence Readiness Assessment Manager presents information in displays, and you can also generate reports. The displays and reports usually use table formats. Tables ease the task of handling information by providing the following features:

- **Sorting**—You can sort a display in the order you prefer by clicking a column heading.
- **Direct page access (only in reports)**—You can browse a report screen by screen or jump to any screen number in the range by entering a screen number.



Note A report can show up to 2,000 records. If more than 2,000 records exist and you need to access additional records, you can use the data export icon to export all records.

- **Data export**—You can export data from a display to a comma-separated values (CSV) file, PDF file, or both, depending upon the display that you are using.
- **Print-friendly format**—You can format the display for a printer and print the result from the browser. Like the display, the print-friendly browser display includes a maximum of 2,000 records.
- **Paging and Sorting Displays and Reports**—The sort order for any display or report is indicated by a triangle in the column heading you will see the triangle. After you click a column heading. A triangle pointing down indicates descending order, which is the default, while a triangle pointing up indicates ascending order.

Step 1 To sort a display, click any blue column-heading label.

The first time you click a column heading on a previously unsorted column, data in that column is sorted in descending order. If you click the column heading again, the records will be sorted in the reverse order.



Note When you sort a display or report, if more than 2,000 records are available, only the first 2,000 records are displayed after sorting.



CHAPTER 2

Device Management

These topics explain how to use Cisco TelePresence Readiness Assessment Manager (TelePresence Readiness Assessment Manager) device management:

- [Getting Started with Device Management, page 2-1](#)
- [Using TelePresence Readiness Assessment Manager to Add Devices, page 2-2](#)
- [Viewing Device Discovery Status, page 2-6](#)
- [Selecting Devices for Assessment, page 2-7](#)

Getting Started with Device Management

Before you can use TelePresence Readiness Assessment Manager to assess your network, you must add devices to the CiscoWorks Common Services Device and Credentials Repository (DCR). Use the DCR to do the following:

- Adding devices (adding a device manually)
- Importing devices (using a seed file)
- Exporting devices
- Changing device credentials

TelePresence Readiness Assessment Manager is the front end for performing the following operations on devices in the TelePresence Readiness Assessment Manager inventory:

- Adding devices using discovery
- Viewing device details
- Performing inventory collection on selected devices



Note

- Configuration changes on a device are discovered by TelePresence Readiness Assessment Manager only during inventory collection. Therefore any changes to a device's configuration will not be shown by TelePresence Readiness Assessment Manager until the next inventory collection after the configuration change.
- If Telnet credentials are wrong or not provided, the devices will be discovered but will be marked as failed during inventory collection.

Understanding the DCR

The DCR is a centralized device repository. Changes to the DCR are propagated to TelePresence Readiness Assessment Manager. To access DCR, click **CiscoWorks** in the top right corner of the window and select **Device and Credentials** to open the Device Management window to add, delete, or view devices. For details on how you can add devices to the DCR, see the Common Services online help.

TelePresence Readiness Assessment Manager inventory is separate from the DCR inventory. After a device is added to the DCR, the DCR assigns a DCR ID to every managed component. The DCR maps components to devices using either the device name or IP address. After the DCR device is added to TelePresence Readiness Assessment Manager, TelePresence Readiness Assessment Manager maps the DCR ID to the name of a device during inventory collection.



Note

Do not confuse the TelePresence Readiness Assessment Manager physical discovery (which adds devices to the DCR) or the TelePresence Readiness Assessment Manager inventory collection process (which probes devices and updates components in TelePresence Readiness Assessment Manager inventory) with DCR synchronization. TelePresence Readiness Assessment Manager inventory collection is a process that affects only the TelePresence Readiness Assessment Manager inventory.

Using TelePresence Readiness Assessment Manager to Add Devices

TelePresence Readiness Assessment Manager adds devices to the DCR through physical discovery.



Note

To add devices manually or by using bulk import (importing from an NMS or from a file), you must go through DCR. For more information, see the instructions in the Common Services online help.

From **Devices > Discover > Discovery Configuration**, you can select any of the following radio buttons:

- **Discovery**—Enable device discovery on this page by choosing one or more of the following discovery methods: CDP, Ping Sweep, and Traceroute. For more information, see the [“Running TelePresence Readiness Assessment Manager Physical Discovery”](#) section on page 2-2.
- **Credentials**—Discovery requires SNMP or SNMPv3 or both, SSH and Telnet credentials. If the credentials are not configured, enter device credentials on this page. For more information, see the [“Editing Device Credentials”](#) section on page 2-5.
- **Filters**—Set up any filters on this page during device discovery. You can set up filters based on IP address, DNS domain, or sysLocation. For more information, see the [“Filtering Devices for Autodiscovery”](#) section on page 2-3.

Running TelePresence Readiness Assessment Manager Physical Discovery



Note

- Discovery requires SNMP or SNMPv3 credentials or both. If credentials are not configured, the Credentials page appears. For more information, see the [“Editing Device Credentials”](#) section on page 2-5.

- If Telnet enable credentials are not entered, some device compliance rules will not get applied to the device. For more information on device compliance, see the [“Running Compliance Analysis” section on page 4-1](#).

Step 1 To enable device discovery, select **Devices > Discover > Discovery Configuration**. The Discovery Configuration page appears.

Step 2 Check the **Discovery** radio button and enter data, as described in the following table.

Field	Action/Description
Use Cisco Discovery Protocol (CDP)	Enter a seed device IP address or a comma-separated list of IP addresses. You can also select the Use devices currently in the system check box to include all devices in DCR. Select the number of hops using the hops list to provide a boundary condition for discovery.
Use ping sweep	The CDP, ping sweep, and traceroute options can be used in an either/or mode. Specify a comma-separated list of IP address ranges using the <i>/netmask</i> specification. For example, use 172.20.57.1/24 to specify a ping sweep range starting from 172.20.57.1 and ending at 172.20.57.255.
Use traceroute (recommended method)	The CDP, ping sweep, and traceroute options can be used in an either/or mode. To find devices using traceroute, enter a pathname for a given set of source and destination devices. Select a source and a destination to discover the path. For information on modifying a path, see “Modifying Traceroute Paths” section on page 2-6 . Traceroute is the preferred method for device discovery. Generated reports provide assessment based on the traceroute path. Note Telnet credentials are required for traceroute.
Run	Select a radio button and enter the schedule: <ul style="list-style-type: none"> • Now—Select to run immediately. • Schedule—Enter time and day on which to run.

Step 3 Click **OK**. Discovery starts to run and might take some time depending on the number of devices being discovered. (Check the status of discovery from **Devices > Discovery > Discover Status**.)

Filtering Devices for Autodiscovery

You can exclude or include specific devices you want discovered by specifying IP addresses, DNS Domains, or sysLocation OIDs.



Note

- Discovery requires SNMP or SNMPv3 credentials or both. If credentials are not configured, the Credentials page appears. For more information, see the [“Editing Device Credentials” section on page 2-5](#).

- If Telnet enable credentials are not entered, some device compliance rules will not get applied to the device. For more information on device compliance, see the [“Running Compliance Analysis” section on page 4-1](#).

Step 1 To set up any filters during device discovery, select **Devices > Discovery > Discovery Configuration**. The Discovery Configuration page appears.

Step 2 Check the **Filters** radio button and enter data described in the following table.

Field	Action/Description
IP Address	<p>(Optional) Enter comma-separated IP addresses or IP address ranges for devices:</p> <ul style="list-style-type: none"> • Include—In the autodiscovery process. • Exclude—From the autodiscovery process. <p>You can use wildcards when specifying the IP address range.</p> <p>An asterisk (*) denotes the octet range of 1-255. You can use the [xxx-yyy] notation to constrain the octet range.</p> <p>For example:</p> <ul style="list-style-type: none"> • To include all devices in the 172.20.57/24 subnet in autodiscovery, enter an include filter of 172.20.57.*. • To exclude devices in the IP address range of 172.20.57.224 - 172.20.57.255 from autodiscovery, enter an exclude filter of 172.20.57.[224-255]. <p>Both types of wildcards can be used in the same range specification; for example, 172.20.[55-57].*. If you specify both include and exclude filters, the exclude filter is applied first before the include filter. After you apply a filter, a discovered device, no other filter criterion can be applied to the device. If a device has multiple IP addresses, the device will be processed for autodiscovery provided that it has one IP address that satisfies the include filter.</p>

Field	Action/Description
DNS Domain	<p>(Optional) Enter comma-separated DNS domain names for devices to:</p> <ul style="list-style-type: none"> • Include—In autodiscovery processing. • Exclude—From autodiscovery processing. <p>The DNS names can be specified using wildcards. An asterisk (*) matches any combination of mixed uppercase and lowercase alphanumeric characters, along with the hyphen (-) and underscore (_) characters, of an arbitrary length. A question mark (?) matches a single uppercase or lowercase alphanumeric character or a hyphen or an underscore character. For example:</p> <ul style="list-style-type: none"> • *.cisco.com matches any DNS name ending with .cisco.com. • *.?abc.com matches any DNS name ending with .abc.com, or .abc.com, etc.
SysLocation	<p>(Optional) Enter comma-separated strings that will match the string value stored in the sysLocationOID in MIB-II, for devices to:</p> <ul style="list-style-type: none"> • Include—In autodiscovery processing. • Exclude—From autodiscovery processing. <p>The location strings can be specified using wildcards. An asterisk (*) matches, up to an arbitrary length, any combination of mixed uppercase and lowercase alphanumeric characters, hyphen (-), underscore (_), and, white space (spaces and tabs). A question mark (?) wildcard matches a single occurrence of any of the above characters. For example, a sysLocation filter of San * will match all sysLocation strings starting with San Francisco, San Jose, etc.</p>

Editing Device Credentials

The Default Credentials page enables you to specify credentials that automatic discovery uses in order to physically discover the devices in the network. As soon as autodiscovery determines the correct credentials for a device, it enters those credentials in the DCR for that device. The credentials specified on the Default Credentials page are not used for any other purpose.



Note

If a device has both SNMP V2 and SNMP V3 configured on it, and if you enter both credentials in the Default Credentials page, automatic discovery tries all SNMP V3 credentials before trying SNMP V2 credentials.

Step 1 To add or modify default discovery configuration parameters select **Devices > Discovery > Discovery Configuration**.

Step 2 Select the **Credentials** option and do one of the following:

- Click **Add** to enter credentials for a given target. Enter appropriate credentials.
- Click **Edit** to modify credentials for a given target. Enter appropriate credentials
- Click **Delete** to remove default credentials for a given target.

**Note**

- Discovery requires SNMP or SNMPv3 credentials or both. If credentials are not configured, the Credentials page appears. For more information, see the [“Editing Device Credentials” section on page 2-5](#).
- If Telnet enable credentials are not entered, some device compliance rules will not get applied to the device. For more information on device compliance, see the [“Running Compliance Analysis” section on page 4-1](#).

Step 3 Click **OK**.

Modifying Traceroute Paths

To add or delete a device from a path:

Step 1 Select **Devices > Discovery > Traceroute Path Management**.

Step 2 Select a path to modify.

Step 3 Click **Modify Path**.

Step 4 Do one of the following:

- Click **Add a new device to this path**.
- Click **Remove a device from this path**.

Step 5 Select the appropriate path, and click **Next**.

Step 6 Select the device and its interfaces.

Step 7 Click **Next**.

Step 8 Enter port information, and click **Done**.

**Note**

Path information will be updated after the next inventory collection.

Viewing Device Discovery Status

Select **Devices > Discovery > Discovery Status** to view device discovery status or a list of discovered devices. This page appears after TelePresence Readiness Assessment Manager finishes discovery. You can click the Refresh button to see the most current device discovery status. You can also click Reconfigure if you want to go back to the Discovery configuration page.

The Discovery Status page displays the following information:

- Start Time—Time device discovery started or time it is scheduled to start.
- End Time—Time device discovery was complete. This field is blank if discovery is running, scheduled, or has failed.

- Status:
 - In progress—Device discovery is running.
 - Completed—Device discovery is finished.
 - Failed—Seed devices are not accessible.

The link that appears at the bottom of the page takes you to a report that lists all discovered devices.

Selecting Devices for Assessment

All devices discovered by TelePresence Readiness Assessment Manager are included in assessment operations by default.

Excluding Devices from Assessment

- Step 1** To exclude discovered devices from inventory collection, compliance analysis, and performance data collection, select **Devices > Discovery > Device Selection**. This page displays a list of all discovered devices. To see only a particular set of devices, see [Filtering the Device List, page 2-7](#).
 - Step 2** Select the devices to exclude.
 - Step 3** Click **Exclude Devices**. A dialog box appears asking if you are sure you want to exclude the devices you selected.
 - Step 4** Click **Yes**.
-

Including Devices from Assessment

If you exclude devices, you can include the devices again.

- Step 1** Click **Include Devices**. A window appears with a list of devices that have been excluded.
 - Step 2** Select devices to include.
 - Step 3** Click **Submit**.
-

Filtering the Device List

If you have a very long device list, you might want to view only a specific set of devices. You can choose to filter (by IP address, DNS name, device classification (role), status, and traceroute pathname) which devices to view by selecting an item from the available lists located at the top of the page. For example, if you want to view all devices with IP addresses that begin with 172.20.12.*, do the following:

- Step 1** From the first list, select **IP Address**.
- Step 2** From the second list, select **starts with**.
- Step 3** Enter **172.20.12** in the text field.
- Step 4** Click **Filter**. A window appears with a filtered device list.

Step 5 Select devices to exclude.

Step 6 Click **Submit**. The window closes, and now the devices you previously selected are also checked in the Device Selection Page.



CHAPTER 3

Inventory Collection and Device Classification

From the inventory tab, you can start inventory collection, view collection progress, and modify device classifications.

These topics describe how to perform inventory collection and device classification:

- [Starting Inventory Collection, page 3-1](#)
- [Viewing Inventory Collection Status, page 3-2](#)
- [Modifying Device Classification, page 3-2](#)

Starting Inventory Collection

The main inventory collection page displays details of all discovered devices TelePresence Readiness Assessment Manager recognizes.



Note

TelePresence Readiness Assessment Manager discovers device configuration changes only during inventory collection. It does not show configuration changes until the next inventory collection after the configuration change is made.

Inventory collection occurs only for included devices. For more information on included and excluded devices, see [“Selecting Devices for Assessment” section on page 2-7](#) or [“Running TelePresence Readiness Assessment Manager Physical Discovery” section on page 2-2](#).

Step 1 Select **Inventory > Inventory Collection**.

Step 2 Click **Start Inventory Collection**. The Inventory Collection Status page appears.

Step 3 Do the following:

- Click **Refresh** to view inventory collection progress.
- Click **Rerun for Failed Devices** to run inventory collection again for failed devices.



Note

-
- The number of failed devices is a link to an inventory report that lists all devices that failed and reason as to why they failed.
 - If Telnet credentials are wrong or not provided, the devices are discovered but are marked as failed during inventory collection.
-

Viewing Inventory Collection Status

The Inventory Collection Status page appears after inventory collection starts. The page summarizes the status of all the devices with respect to the current inventory collection. If you want to see the status without running inventory collection again, do the following:

-
- Step 1** Select **Inventory > Inventory Collection**.
- Step 2** Click **Status Report**. The Status Report page appears.



The number of successful, failed, and pending devices are links to the appropriate inventory report. The report displays a list of devices, along with IP address, the time that inventory collection for device was complete, and, if applicable, the reason why inventory collection failed for that device.

Modifying Device Classification

By default, TelePresence Readiness Assessment Manager assigns a default role to each device. You can change the default device classification.

You can also choose to export or import device classifications. This enables you to work on device classification at a later time and import the list back into TelePresence Readiness Assessment Manager.

To modify device classification:

-
- Step 1** Select **Inventory > Device Classification**.
- Step 2** Select devices to modify, and do one of the following:
- To export device classifications to a .csv file, click .
 - Enter a filename or click **Browse** to navigate to an existing file that you want to overwrite.
 - Click **Export**. You can now work with this file and change device classification as needed.
 - To import device classifications from a .csv file, click .
 - Enter a filename or click **Browse** to navigate to the file that contains the device classification information.
 - Click **Import**.
 - To change device classification, select **Change Role**. A popup window appears.
 - Select the appropriate device classifications: Access Switch, Aggregation Router, Branch Router, Core Switch, or Distribution Switch.
 - Click **Apply**.
 - To reset a device so that it has no role, select **Reset Role**.
-



CHAPTER 4

Compliance, Performance, and TelePresence Traffic Assessment

During assessment, devices are evaluated to determine whether the network is ready for the deployment of a Cisco TelePresence solution. Assessment consists of three operations:

- [Running Compliance Analysis, page 4-1](#)
- [Running Performance Analysis \(Creating a Performance Study\), page 4-2](#)
- [Running Telepresence Traffic Analysis, page 4-3](#)

Running Compliance Analysis

Compliance analysis checks your devices against best practice rules for device software and hardware in the telepresence industry. You can view information about the best practice rules from the appendix of the [Compliance Analysis Report](#). To check if the devices in your network comply with Cisco TelePresence deployments, do the following:

-
- Step 1** Select **Assessment > Compliance**.
- Step 2** Click **Start Compliance**. A confirmation window appears.
- Step 3** Click **OK** to start the compliance analysis. Progress is shown in the status field:
- In Progress—Compliance analysis is in progress.
 - Completed—Compliance analysis has completed successfully.
 - Failed—Compliance analysis failed.

You can also click Refresh to check the status periodically.

Running Performance Analysis (Creating a Performance Study)

Performance analysis collects performance data for the devices in your network. The first time you run performance analysis, you select a subset of devices and set a schedule. Polling various devices in the network and gathering performance-related information over a period of time is called a *study*. Only one study can be processed at a time. After initial setup, the Status window always appears.

-
- Step 1** Select **Assessment > Performance > Performance Study**. A list of devices that are in the TelePresence Readiness Assessment Manager inventory are displayed. If the list is long and you want to view only a subset of those devices, see [Filtering the Device List, page 4-2](#).
- Step 2** Select devices to include in the study.
- Step 3** Click **Next**.
- Step 4** Do one of the following:
- Select the **One Time** radio button to perform one study that will run continuously for a period of time.

In the From: field:

 - Enter or select from the calendar icon the date you want the study to begin.
 - From the lists, select the time you want the study to begin.

In the To: field:

 - Enter or select from the calendar icon the date you want the study to end.
 - From the lists, select the time you want the study to end.
 - Select the **Recurring** radio button to perform a study that will run within a specified time for a number of days.
 - In the From: field, enter or select from the calendar icon the date you want the study to begin.
 - In the To: field, enter or select from the calendar icon the date you want the study to end.
 - From the lists, select the times you want the study to begin and end.
- Step 5** Click **Finish**. The Performance Data Collection Status page displays the details of the study that you just created. For more information, see [Viewing Performance Study Details, page 4-3](#).
-

Filtering the Device List

If you have a very long device list, you might want to view only a specific set of devices. You can choose to filter (by IP address, DNS name, device classification (role) and polling interval) which devices to view by selecting an item from the available lists located at the top of the page. For example, to view all devices with IP addresses that begin with 172.20.12.*, do the following:

-
- Step 1** From the first list, select **IP Address**.
- Step 2** From the second list, select **starts with**.
- Step 3** Enter **172.20.12** in the text field.
- Step 4** Click **Filter**. A window appears with a filtered device list.

- Step 5** Select devices to include in the study.
- Step 6** Click **Submit**. The window closes, and the devices you previously selected are also selected in the Study Device Details Page.

Viewing Performance Study Details

If a performance study was set up, this is the first page you will see after selecting **Assessment > Performance > Performance Study**. If you did not set up a performance study, see [Running Performance Analysis \(Creating a Performance Study\)](#), page 4-2.

This page displays details of the study that was created. The following table lists available status and the function that can be performed.

Status	Description	Available Task
Scheduled	A study set up for the future.	You can modify or delete this study.
Running	A study is running.	You can modify, delete, or stop this study.
Completed	The study is finished.	You can delete this study.
Stopped	The study has been stopped.	You can modify or restart this study.

The link in the Device Details field takes you to the Device Poll Settings page. For more information, see [Changing Device Poll Settings](#), page 4-3.

Changing Device Poll Settings

Device poll settings can be changed according to their device categories (roles). Any changes to the poll settings are applied to all devices that belong to a particular device category. You can access this page from **Assessment > Performance > Device Details**.

- Step 1** From each category, use the n list to select the new number of minutes for poll settings.
- Step 2** Click **OK**.

Running Telepresence Traffic Analysis

TelePresence Readiness Assessment Manager enables you to simulate high-load telepresence traffic to run at different time intervals. It simulates telepresence traffic to predict the number of calls that the network can accommodate and gives insight to any voice and video impairment factors. It also provides audio and video QoS data that enables you to analyze network performance.

You can do a number of different scenarios, for example:

- Run a series of tests for an extended period of time to determine the stability of a network's performance. For example, you can run nightly tests for 15 days and vary certain parameters (video profile, video resolution, TOS settings, etc).

- Determine maximum bandwidth of a system by testing multiple systems simultaneously across a single network.
- Run multiple systems at different locations and simulat traffic at all possible point-to-point combinations.

To start simulating telepresence traffic in your network, you must have the Media TelePresence Analysis Agent installed on at least two systems in the network.

**Note**

Before simulating traffic tests, close all open applications on the system. TelePresence Readiness Assessment Manager requires a dedicated system to accurately simulate telepresence traffic.

See the following topics:

- [Installing the Media Traffic Analysis Agent on a System, page 4-4](#)
- [Managing Agents, page 4-4](#)
- [Managing Simulated TelePresence Traffic Tests, page 4-6](#)

Installing the Media Traffic Analysis Agent on a System

Download the agent from the TelePresence Readiness Assessment Manager server to your system.

**Note**

To simulate traffic, the Media TelePresence Analysis Agent must be installed on at least two systems (typically connected to the same switch that the proposed Cisco TelePresence Site (CTS) will be connected to).

-
- Step 1** From your web browser, log in to TelePresence Readiness Assessment Manager server (see [Starting TelePresence Readiness Assessment Manager, page 1-4](#)).
- Step 2** Select **Assessment > Traffic Analysis > Download Agent**.
- Step 3** Click **Save** to copy the mtaaSetup.exe file to your system.
- Step 4** Follow the installation wizard prompts. For more information, see *Quick Start Guide for Cisco TelePresence Readiness Assessment Manager*.
-

Managing Agents

From the Agent Management page, you can add, modify, delete, and view information for Media Traffic Analysis Agents.

To add agents:

-
- Step 1** Select **Assessment > Traffic Analysis > Agent Management**
- Step 2** Click **Add**.

Step 3 Enter all appropriate data for the system on which the agent is installed:

- **Agent Name**—Enter a name for this agent. TelePresence Readiness Assessment Manager uses the agent name as a unique identifier, and it cannot be modified unless you delete and re-create the agent.
- **IP Address/DNS Name**—Enter IP address or DNS name.
- **Description**—Enter an appropriate description for this agent, for example, a location, a site name, etc.
- **SOAP Port**—The default Simple Object Access Protocol (SOAP) port appears. If you made any changes, enter the SOAP port assigned to the system.
- **HTTP Port**—Default port appears. If you made any changes, enter the HTTP port assigned to the system.
- **Username**—Enter the username you entered when you installed the agent.
- **Password**—Enter the password you provided at the time of agent installation.

Step 4 Click **Submit**.



Note

- Adding the agent this way does not install it on the system. To start simulating telepresence traffic in your network, the Media TelePresence Analysis Agent must be installed on at least two systems (typically connected to the same switch that the proposed Cisco TelePresence Site (CTS) will be connected to). For more information, see [“Installing the Media Traffic Analysis Agent on a System.”](#)
- If authentication fails, try adding the agent by entering the correct username and password.

To modify agent configuration:

Step 1 Select **Assessment > Traffic Analysis > Agent Management**.

Step 2 Select an agent from the TelePresence Traffic Analysis Agents list.

Step 3 Click **Modify**.

Step 4 Modify all appropriate fields.

Step 5 Click **Submit**.

To delete an agent from TelePresence Readiness Assessment Manager:

Step 1 Delete all tests associated with the agent:

- a. Select **Assessment > Traffic Analysis > Traffic Analysis Tests**.
- b. Select the test associated with the agent that you want to delete.
- c. Click **Delete**.
- d. Repeat steps until all tests associated with the agent are deleted.

Step 2 Select **Assessment > Traffic Analysis > Agent Management**.

Step 3 Select an agent from the TelePresence Traffic Analysis Agents list.

Step 4 Click **Delete**.

**Note**

Deleting an agent from TelePresence Readiness Assessment Manager does not automatically uninstall the agent from the system. For more information on deleting an agent, see the *Quick Start Guide for Cisco TelePresence Readiness Assessment Manager*.

To view information about an agent:

Step 1 Select **Assessment > Traffic Analysis > Agent Management**.

Step 2 Click an agent name. A window appears, displaying the following information:

- Agent Software Version
- System Uptime
- IP Address
- MAC Address
- NTP Server Host
- NTP Synchronization Status
- Process Status
- SOAP Server Port
- HTTP Server Port
- SIP Server Port
- Media Stream Ports
- Voice VLAN
- Time of Last Error / Last Error Description
- Last Result Query Time
- Ctrl Server / TestID / Other Party / VLAN

Managing Simulated TelePresence Traffic Tests

From the Traffic Analysis Tests page, you can add, stop, resume, or delete a test.

**Note**

Before simulating traffic tests, close all open applications on the system. TelePresence Readiness Assessment Manager requires a dedicated system to accurately simulate telepresence traffic.

To add a test:

-
- Step 1** Select **Assessment > Traffic Analysis > Traffic Analysis Tests**.
- Step 2** Click **Add**.
- Step 3** Enter appropriate parameters:
- Network Path—Enter network pathname or select one from the list.
 - Test Name—Enter a name for this simulation.
 - Agent 1 and Agent 2—Select the pair of agents from the drop-down lists.
 - CTS Options—Select or check the appropriate options.
 - Call Options—Enter the appropriate values.
 - Select Frequency: **One Time**— Select this radio button to run simulation continuously for the length of time.
 - In the From: field:
 - Enter or select from the calendar icon the date for simulation to begin.
 - From the lists, select the time for simulation to begin.
 - In the To: field:
 - Enter or select from the calendar icon the date for simulation to end.
 - From the lists, select the time for simulation to end.
 - Select Frequency: **Recurring**—Select this radio button to run simulation within a specified time for a number of days.
 - In the From: field, enter or select from the calendar icon the date for simulation to begin.
 - In the To: field, enter or select from the calendar icon the date for simulation to end.
 - In the lists, select the times for simulation to begin and end during the day.
- Step 4** Click **Add**.
-

To view, stop, or resume a test:

-
- Step 1** Select **Assessment > Traffic Analysis > Traffic Analysis Tests**.
- Step 2** Select the appropriate test.
- Step 3** Click **Manage**.
- Step 4** Do one of the following:
- Click **Resume** to resume the test.
 - Click **Stop** to stop the test.
 - Close the window if you do not want to perform any actions.
-

To delete a test:

-
- Step 1** Select **Assessment > Traffic Analysis > Traffic Analysis Tests**.
 - Step 2** Select the appropriate test.
 - Step 3** Click **Delete**.
-

Viewing Raw Data from Agents

You can view data captured by each agent. The data files are located in `$NMSROOT/data/traffic` and are named `<Agent name>-mmddYYY-hour.csv`. The files are maintained for 15 days and are captured every hour if test data is available. The csv file format is

TestID, StreamType, SrcHost, CallID, Codec, StartTime, EndTime, RecordTime, TOS, Jitter, Latency, NetworkPacketLoss, MOS.



CHAPTER 5

Reports

After you complete your assessments, you can generate four [reports](#) that show your network's readiness for deploying a Cisco TelePresence solution. You should complete the [questionnaire](#) before generating the report.

Completing the Questionnaire

The questionnaire extracts information about your network that cannot be determined through inventory collection or compliance analysis. Although this step is optional, we recommend it for a more thorough and accurate assessment of your network. It contains questions about the following:

- IP addressing
- WAN design
- QoS and CAC
- Microsoft Exchange design
- Telephony infrastructure
- IP security
- Bandwidth percentage
- Type of information to display—By default, only values that violate acceptable thresholds are displayed.

Generating the Report

Step 1 Select **Reports > Reports**.

Step 2 Do one of the following:

- Click **Start**, if this is the first time you are generating a report.
- Click **Regenerate Report**, if you have generated a report in the past.

Step 3 On the Generate Report page, enter the appropriate values to customize the report.



Note You must enter text in the first three fields: name of company receiving the assessment, name of company performing the assessment, and name of engineer performing the assessment.

Step 4 Click **Finish**.

Viewing Reports

After you complete the steps to [generate](#) the report, the Report Generation Status page appears. Three buttons are available on this page:

- Refresh—Updates status of report generation. Click this button to see updated progress.
- Regenerate Report—Generates the report again. You should regenerate the report if the report fails to generate correctly.
- View Reports—After you click this button, a list displays:
 - Executive Report—Summary of device compliance, Cisco TelePresence recommendations, and utilization statistics based on network paths.
 - Performance Utilization Report—Detailed utilization statistics for the devices selected for the performance study.
 - Compliance Analysis Report—Analysis of device compliance (according to device network best practices), recommendations on Cisco TelePresence systems, and recommendations based on the answers you entered in the [questionnaire](#).
 - Traffic Simulation Report—Cisco TelePresence traffic analysis of your existing network. The video and audio traffic analysis is based on reports provided by the traffic analysis agents deployed at strategic locations for each network path in your network.

Executive Report

This report gives feedback on your organization's network readiness to deploy a Cisco TelePresence Solution. Recommendations and feedback for planning and designing your network are based on the state of your network and the deployment options you chose at the beginning of the assessment.

This report

- Recommends types of Cisco TelePresence systems
- Analyzes device compliance with best practices
- Analyzes telepresence traffic
- Captures utilization statistics

Performance Utilization Report

This report contains information about how individual devices perform on each network path or in network inventory.

Utilization is calculated by taking the daily or hourly average CPU/memory/bandwidth utilization of each device and separating them into the following threshold categories:

- OK—Average utilization of a router or a switch is less than or equal to 30%.
- Minor—Average utilization of a router or a switch is more than 30% but less than or equal to 50%.

- Major—Average utilization of a router or a switch is more than 50%.

Utilization Calculation Example 1

This example explains how utilization is calculated for one day.

Performance Study Details

- Pathname: ABC-XYZ
- Number of devices: 5
- Length of study: 12 hours for 2 days = 24 hrs = 1440 minutes
- Polling interval: Every 5 minutes



Note The default polling interval is every 3 minutes. To change the polling interval, select **Assessment > Performance > Device Poll Settings**. To simplify explanation, the polling interval for this example is set to 5 minutes.

- Number of samples collected for each device: $1440 / 5$ (length of study/polling interval) = 288 samples.



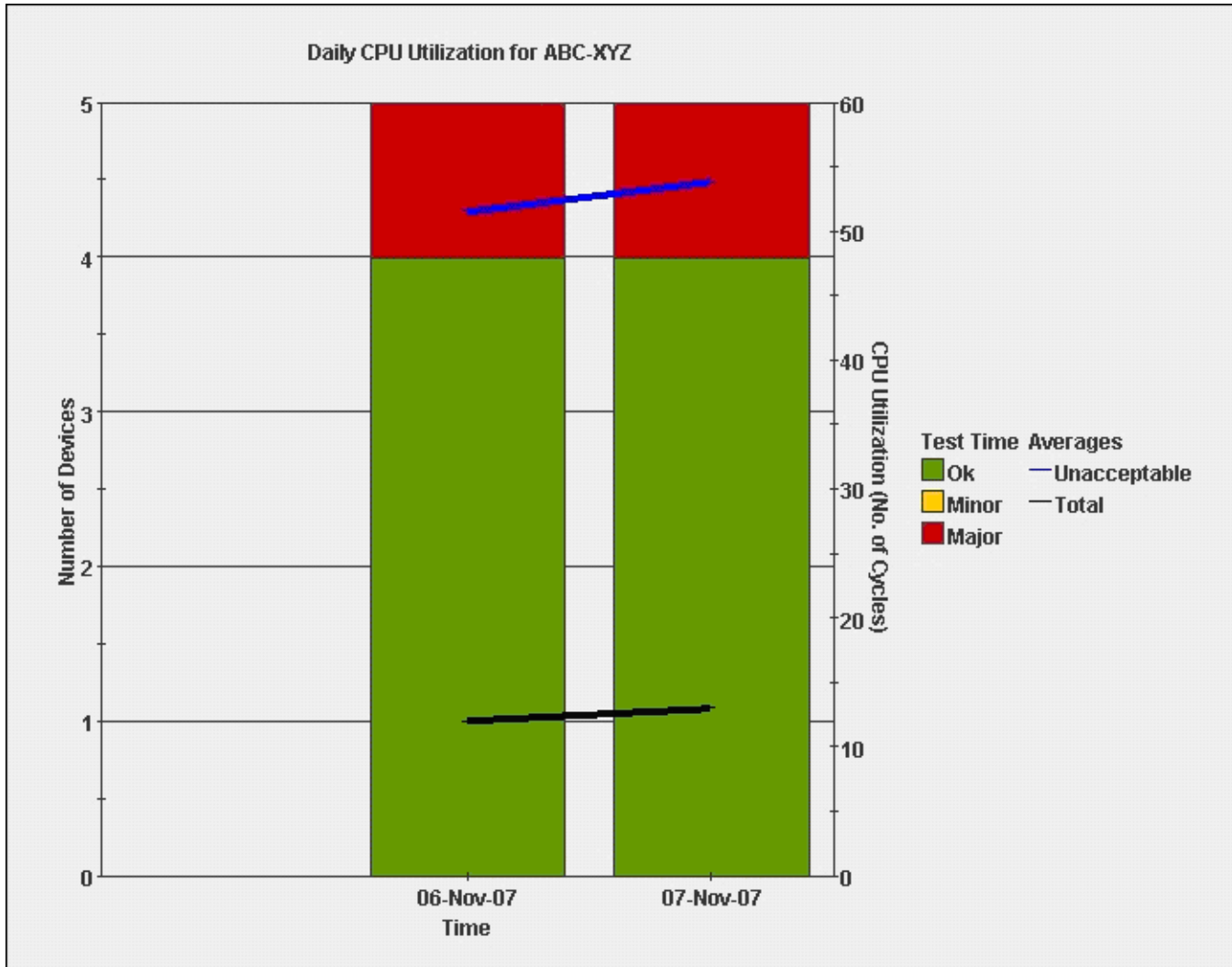
Note The term *sample* represents the utilization data captured at the time TelePresence Readiness Assessment Manager polled the device.

Utilization Severity Levels and Threshold Percentages:

- OK—Average utilization of a router or a switch is less than or equal to 30% (0-30%).
- Minor—Average utilization of a router or a switch is more than 30% but less than or equal to 50% (31-50%).
- Major—Average utilization of a router or a switch is more than 50% (51% or more).

The report displays the graph shown in [Figure 5-1](#):

Figure 5-1 ABC-XYZ Path : Average Device Utilization for Two Days



TelePresence Readiness Assessment Manager checks each sample value against the threshold and marks it as bad or good depending on the threshold violation. The bad sample rate is obtained by dividing the number of bad samples by the total number of samples. If the bad sample percentage is greater than 20% then the device is considered as bad. The category of the severity of the device depends on the average of the bad sample values.

For example, Device 1 had the following utilization values for November 6:

- 188 samples = 4% (OK)
- 40 samples = 20% (OK)
- 60 samples = 52% (Major)

Device 1 average utilization = $((4 \times 188) + (40 \times 20) + (60 \times 52)) / 288 = 16.2\%$

**Note**

Actual thresholds for each sample will vary. Only three threshold values are used in this example to simplify calculation.

Devices are considered bad if 20% or higher of the samples are bad. Bad samples are samples that violate the threshold (51% or higher). In this example, Device 1 is considered bad since 21% (60 samples / 288 samples) of the samples had Major utilization (52%). All other devices recorded on November 6 had the following average utilization:

- Device 2 = 13%
- Device 3 = 17%
- Device 4 = 10%
- Device 5 = 12%

The daily average for all devices on November 6 is $(16.2 + 13 + 17 + 10 + 12) / 5 = 13.64\%$ (as shown in [Figure 5-1](#)). The bad average is 52%.

The following values were taken on November 7:

- Device 1
 - 280 samples = 5% (OK)
 - 8 samples = 40% (Minor)

There are no bad samples. 90% (280 / 288) of samples are categorized with severity level OK.

- Device 2
 - 288 samples = 6% (OK)
- Device 3
 - 208 samples = 10% (OK)
 - 80 samples = 54% (Major)

There is a bad sample average of 28% (80 / 288) with severity level Major. This device is considered bad since the bad sample average is more than 20%.

- Device 4
 - 288 samples = 6% (OK)
- Device 5
 - 288 samples = 8% (OK)

There are no bad samples. Samples are categorized with severity level OK.

[Figure 5-1](#) shows the bar graph with four devices having good utilization with severity level OK (green color). Since Device 3 has a bad sample average of 28%, the November 7 bar graph displays one device having high utilization with severity level Major (red color).

The total and bad sample averages are shown as line graphs. The right y-axis represents utilization. The black line denotes total average of samples. The blue line denotes total average of bad samples.

Utilization Calculation Example 2

This example shows how utilization is calculated each hour. Calculation is based on the average samples collected each hour.

Performance Study Setup

- Pathname: ABC-XYZ

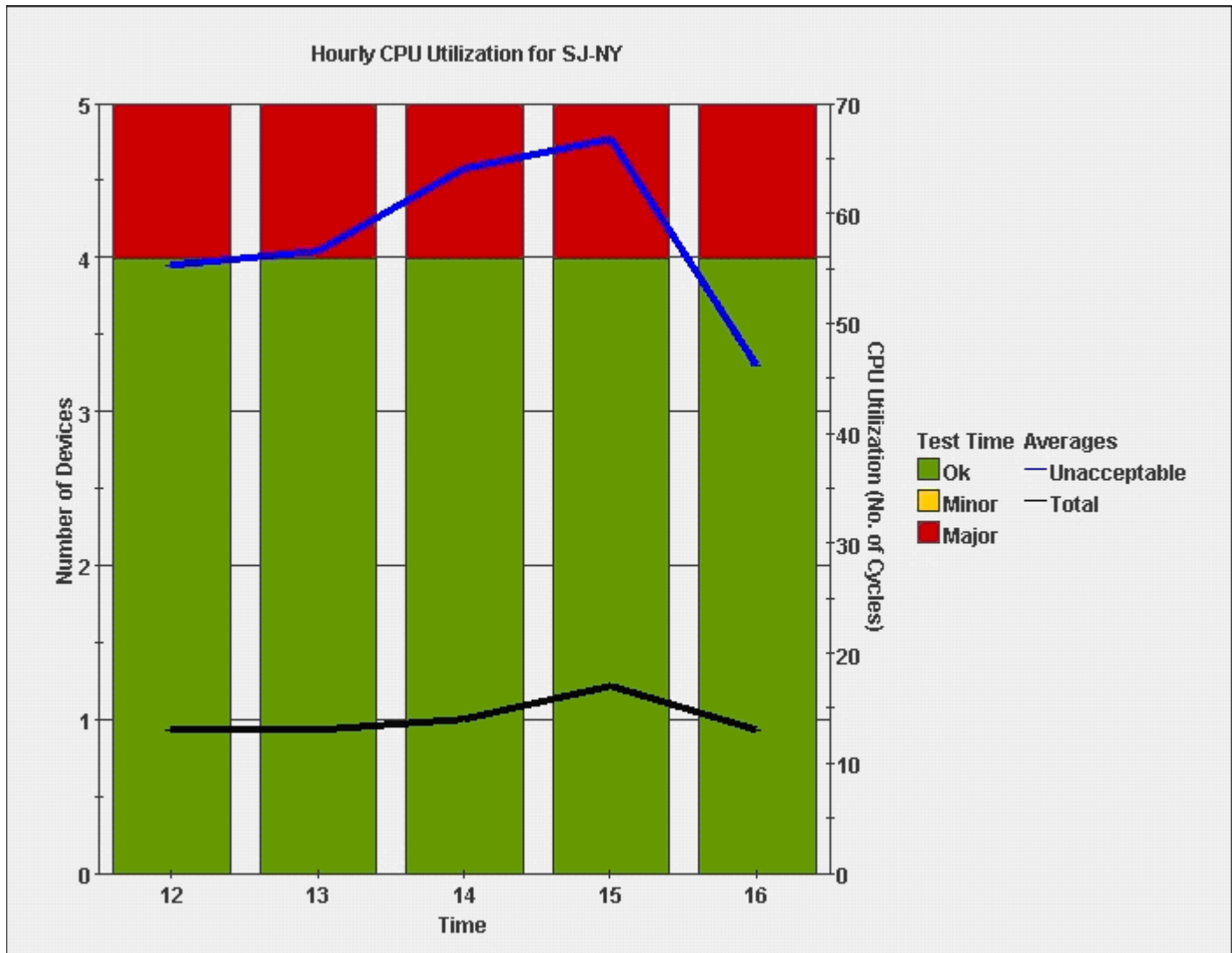
- Number of devices: 5
- Length of study: 2 days from 12 pm – 5 pm
- Polling interval: 5 minutes
- Daily number of samples collected for each device each hour: $60/5$ (hour/polling interval) = 12 samples
- Total number (two days) of samples collected each hour = 24 samples

Threshold Percentages:

- OK—Average utilization of a router or a switch is less than or equal to 30% (0-30%).
- Minor—Average utilization of a router or a switch is more than 30% but less than or equal to 50% (31-50%).
- Major—Average utilization of a router or a switch is more than 50% (51% or more).

The report displays the graph shown in [Figure 5-2](#)

Figure 5-2 ABC-XYZ Hourly CPU Utilization



On November 6, Device 1 had a bad sample average value of 55% for hours 12 and 13. All other devices for hours 12 and 13 had good samples. On the graph, the red color for hours 12 and 13 represent Major utilization for Device 1. The blue line represents the bad sample average (55%).

Device 2 had good samples on November 6, but had bad samples on November 7 for hours 14, 15, and 16. Since at least one device (Device 1 or Device 2) had bad samples across all hours, the graph shows one device in red with major utilization.

The table following the graph displays the devices that experienced major utilization per hour information including violated thresholds, maximum values, and corresponding timestamps.

Compliance Analysis Report

This report analyzes device compliance (according to device network best practices), recommends types of Cisco TelePresence devices, and displays recommendations based on the answers you gave in the [questionnaire](#).

Device compliance is calculated using the highest severity of a rule that the device does not comply with.





Note

The Best Practice Analysis rules and their associated severity levels (Informational, Warning, and Critical) are listed at the end of the Compliance Analysis Report.

For example, if Device 1 does not comply with Rule 1: STP Convergence (Informational) and Rule 8: Check QOS (Critical), the device is shown as noncompliant and assigned a severity level of Critical (bar will be red). See the following example ([Figure 5-3](#)):

Figure 5-3 Device Compliance Summary Example

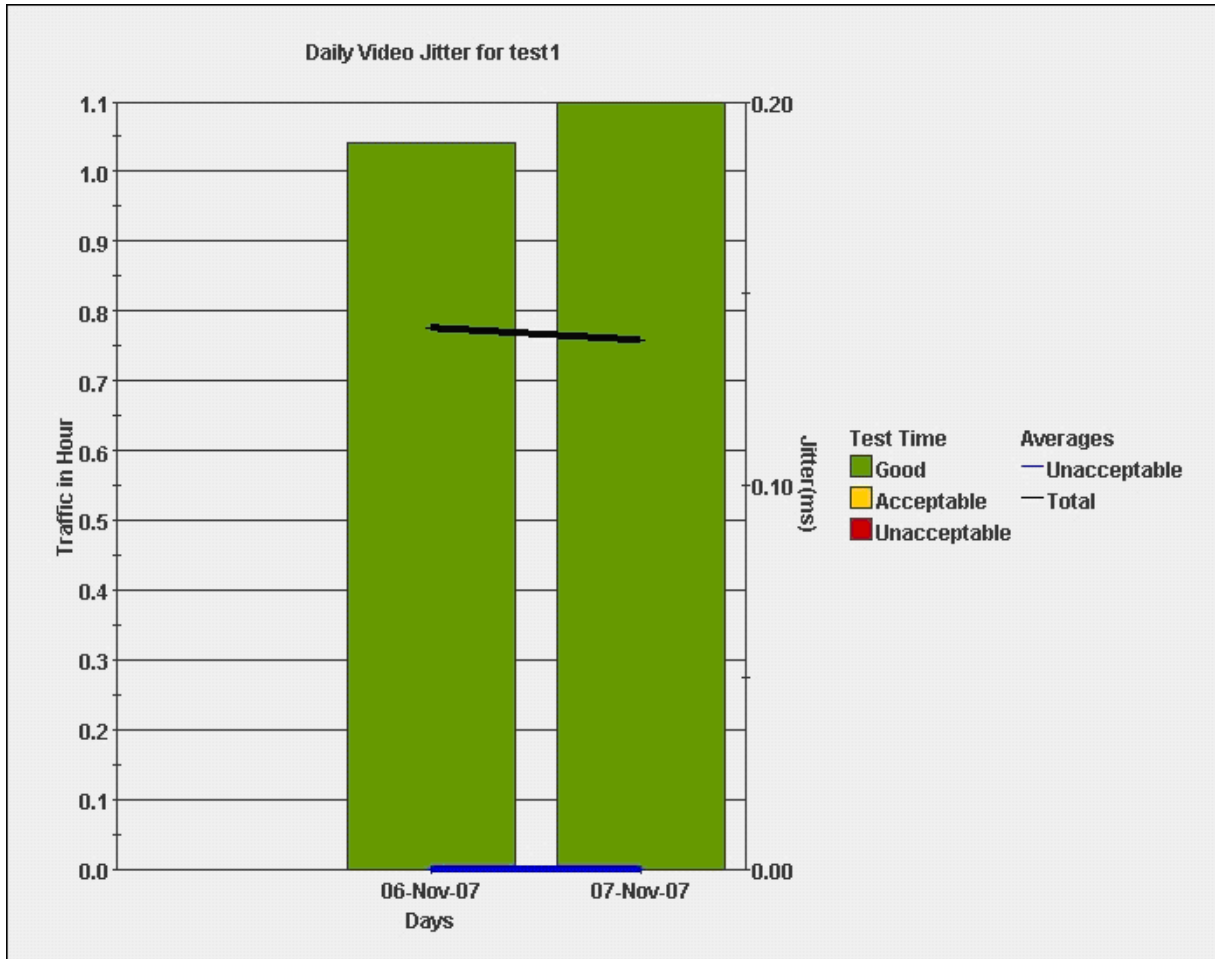
Path Name	Number of Devices	Device Compliance Summary	Severity of Noncompliance
New York	2	0 - Compliant 2 - Noncompliant 0 - NotApplied	
San Jose	3	0 - Compliant 1 - Noncompliant 0 - NotApplied	

Traffic Simulation Report

This report analyzes Cisco TelePresence traffic in your existing network. Video and audio traffic analysis is based on reports for each network path from traffic analysis agents deployed at strategic locations in your network .

[Figure 5-4](#) is an example of a traffic simulation graph displaying daily video jitter results.

Figure 5-4 Traffic Simulation Graph for Daily Video Jitter



Performance Study Setup

Test name: test 1

Length of study: 2 days

Calculations are similar to those described in the [Performance Utilization Report](#). The bar represents the traffic time. If the sample violates the threshold, the 30 second traffic time is marked as bad and the severity is dependant on the average violated sample value. The line graphs represent the total average and bad average value.



Note

Sampling rate is 30 seconds.

In this example, jitter has the following time thresholds:

- Good—Average value of jitter less than or equal to 20 ms.
- Acceptable—Average value greater than 20 ms but less than or equal to 40 ms.
- Unacceptable—Average value higher than 40 ms.

**Note**

Latency and packet loss have different thresholds which are listed in the report.



CHAPTER 6

Administration

You can send event notifications and configure module logging levels using the tools available in the Administration pages. The following topics are available in this section:

- [Setting Up Notifications, page 6-1](#)
- [Configuring Logging Levels, page 6-1](#)

Setting Up Notifications

- Step 1** Select **Admin > Notification**.
 - Step 2** Enter the SMTP Server. This is the name of the mail server, for example, mailman.cisco.com.
 - Step 3** Enter email addresses or pager numbers or both to which notifications are to be sent.
-

Configuring Logging Levels

- Step 1** Select **Admin > Logging**.
 - Step 2** From the list, select the appropriate logging levels for each module.
 - Step 3** Do one of the following:
 - Click **Apply** to apply changes.
 - Click **Default** to restore default logging levels for each module.
-



APPENDIX **A**

Appendix A: Open Source License Notices

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.
 The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



INDEX

A

about

- dashboard [3](#)
- devices, adding and classifying [2](#)
- TelePresence Readiness Assessment Manager [1](#)

adding

- agent [4](#)
- credentials [5](#)
- traffic analysis test [6](#)

administrative tasks [1](#)

agent

- adding [4](#)
- deleting [4](#)
- downloading [4](#)
- installing [4](#)
- modifying [4](#)
- uninstalling [6](#)
- viewing [6](#)

analysis

- compliance, running [1](#)
- performance, running [2](#)
- traffic [3](#)

assessment

- devices, excluding [7](#)
- devices, including [7](#)

audience for this document [v](#)

C

cautions

- significance of [v](#)

CDP, using for discovery [2](#)

classification, device [2](#)

- exporting [2](#)
- importing [2](#)

Compliance Analysis Report, description [2](#)

configuration changes, device [1](#)

conventions in this document, typographical [v](#)

credentials, device

- default, purpose of [5](#)
- editing [5](#)

D

dashboard, about [3](#)

DCR

- accessing [2](#)
- inventory, compared with [2](#)
- physical discovery, compared with [2](#)

debugging, configuring [1](#)

deleting

- agent [4](#)
- credentials [5](#)

Device and Credentials Repository. *See* DCR

devices

- adding, process for [2](#)
- classifying [2](#)
- configuration changes, when discovered [1](#)
- discovered, report [6](#)
- excluding from
 - assessment [7](#)
 - discovery [3](#)
- including in
 - assessment [7](#)
 - discovery [3](#)

discovery

- CDP 2
- excluding devices from 3
- including devices 3
- physical, running 2
- preferred method for 2
- status, viewing 6
- traceroute 2

DNS domain, including in discovery 3

documentation vi

- audience for this v
- obtaining vi
- typographical conventions in v

downloading agent 4

E

editing

- agent configuration 4
- device credentials 5

e-mail notification, configuring 1

enable password 5

Enter key 4

excluding devices from

- assessment 7
- discovery 3

Executive Report

- viewing 2

exporting device classification 2

G

getting started

- analysis, performing 3
- devices, adding 2
- questionnaire, answering 3
- traffic simulation, performing 3

H

help

- button 4
- using 5

I

importing device classification 2

including devices in

- assessment 7
- discovery 3

inventory

- classification 2
- collection
 - running 1
 - status report 2

L

logging, configuring 1

M

Media TelePresence Analysis Agent. *See* agent

Microsoft Word 1

modifying agent configuration 4

N

notifications, configuring 1

O

obtaining documentation vi

P

- pager notification, configuring [1](#)
- paths
 - traceroute, modifying [6](#)
- performance study
 - creating [2](#)
- Performance Utilization Report, description [2](#)
- ping sweep, using for discovery [2](#)

Q

- questionnaire, about [1](#)

R

- reports
 - about [1](#)
 - examples [1](#)
 - generating [1](#)
- resuming traffic analysis test [6](#)
- role, device. *See* classification

S

- security [4](#)
- significance of cautions [v](#)
- simulation
 - scheduling [6](#)
 - TelePresence traffic, running [3](#)
- SMTP server, configuring [1](#)
- SNMP V2 credentials [5](#)
- SNMP V3 credentials [5](#)
- SOAP port, used by agent [4](#)
- SSH credentials [5](#)
- starting
 - help [5](#)
 - TelePresence Readiness Assessment Manager [4](#)

- study, performance, creating [2](#)
- subnets
 - excluding from discovery [3](#)
 - including in discovery [3](#)
- SysLocation, discovery by [3](#)

T

- Telnet credentials [5](#)
- traceroute [2](#)
 - paths
 - modifying [6](#)
 - when updated [6](#)
 - using for discovery [2](#)
- traffic analysis
 - running [3](#)
 - test
 - adding [6](#)
 - resuming [6](#)
- traffic simulation [3](#)
- Traffic Simulation Report, description [2](#)
- Trusted Sites Zone, Internet Explorer [4](#)
- typographical conventions in this document [v](#)

U

- understanding
 - DCR [2](#)
 - discovery status [6](#)
- uninstalling agent [6](#)
- user interface, understanding [4](#)

V

- viewing
 - agent [6](#)
 - discovery status [6](#)
 - reports [2](#)

W

Windows 2003 Enhanced Security [4](#)