User Guide for Cisco Hosted Collaboration Mediation

Release 1.2

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

Text Part Number: OL-25072-01

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.

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 Hosted Collaboration Mediation 1.2

CONTENTS

Preface

This section explains the objectives and intended audience of this publication and describes the conventions that convey instructions and other information.

Objectives

This guide explains how to use Cisco Hosted Collaboration Mediation (HCM) Release 1.2. This manual describes and provides instructions for using and administering HCM.

Audience

The primary audience for this guide includes network operations personnel and system administrators. This guide assumes that you are familiar with the following products and topics:

- Basic internetworking terminology and concepts
- Red Hat Enterprise Linux
- Cisco Unified Operations Manager
- Cisco Unified Computing System Manager (UCSM)
- VMware vCenter

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Displayed session and system information	`screen` font
Information that the user must enter	**`boldface screen`** font
Variables that the user must supply	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item	**Option > Network Preferences**

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

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tip Means *the following information will help you solve a problem*.

Product Documentation

Table 1 lists the HCM documentation set.

We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates. You must access the links in Table 1 for the most current HCM 1.2 documentation.

Table 1 Product Documentation

Document Title	Available Formats
User Guide for Cisco Hosted Collaboration Mediation 1.2 (this document)	On Cisco.com: http://www.cisco.com/en/US/products/ps11243/products_user_guide_list.html
Installation Guide for Cisco Hosted Collaboration Mediation 1.2	On Cisco.com: http://www.cisco.com/en/US/products/ps11243/prod_installation_guides_list.html
Release Notes for Cisco Hosted Collaboration Mediation 1.2	On Cisco.com: http://www.cisco.com/en/US/products/ps11243/prod_release_notes_list.html
Programmer's Guide for Cisco Hosted Collaboration Mediation Interface 1.2	On Cisco.com: http://www.cisco.com/en/US/products/ps11243/prod_technical_reference_list.html
Open Source Used In Cisco Hosted Collaboration Mediation 1.2	On Cisco.com: http://www.cisco.com/en/US/products/ps11243/products_licensing_information_listing.html

Related Documentation

Table 2 lists a set of related documentation available on Cisco.com.

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

Table 2 Related Documentation

Cisco Product	Location on Cisco.com
Cisco Unified Operations Manager	http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html
Cisco Unified Computing System Manager (UCSM)	http://www.cisco.com/en/US/products/ps10281/tsd_products_support_series_home.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 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

This chapter describes the Hosted Collaboration Mediation (HCM) software. It includes:

Overview of HCM

HCM is intended for use in a Managed Service Provider (MSP) Network Operations Center (NOC). The main component in HCM is called Service Assurance. For more information, see HCM Service Assurance, page 1-2.

HCM Service Assurance

HCM Service Assurance provides a single pane view of assurance data in the hosted environment and provides various summaries and reports. This component was earlier known as Dashboard Layer. HCM Service Assurance acts as a bridge among customer-specific implementations of the following domain managers, in a virtualized environment:

- Cisco Unified Operations Manager (CUOM)
- VMware vCenter
- Cisco Unified Computing System Manager (UCSM)
- Data Center Network Manager (DCNM) - SAN
- Data Center Network Manager (DCNM) - LAN

HCM Service Assurance aggregates data from multiple instances of these domain managers, so that a user logging into HCM Service Assurance can view aggregated customer data in a single window. HCM Service Assurance comprises a set of Administration and Dashboard portlets and a Diagnostics portlet.

The Service Assurance portlets enable you to aggregate data from each virtualized instance of CUOM, vCenter, UCSM, DCNM-SAN, and DCNM-LAN.

The Administration portlets enable you to cross-launch to the web pages of the individual instances of CUOM, vCenter, UCSM, and DCNM-SAN for customer-centric views.

The portlets leverage the existing APIs and allow API calls to retrieve information from domain managers. HCM Service Assurance supports a VMWare-based deployment and can be installed and operated along with other portal servers or applications.

Terminology Used In HCM

The following list explains the terminology used in HCM:

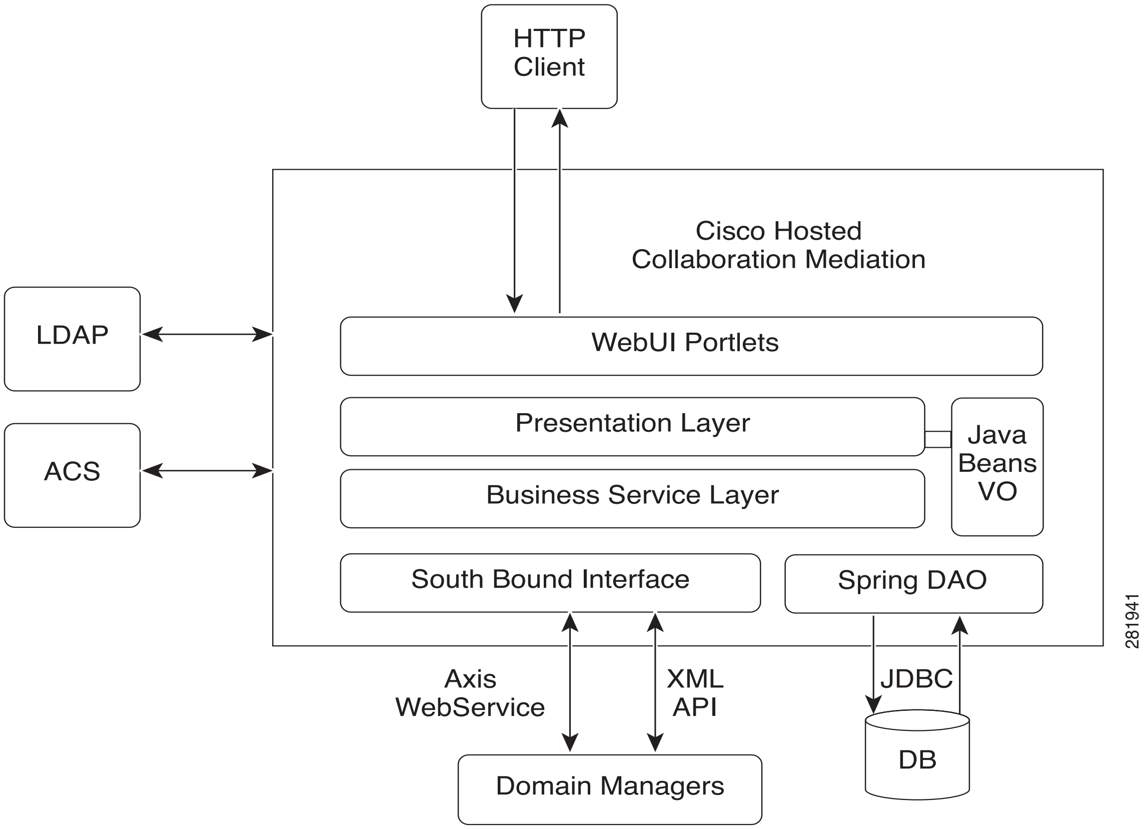
- ACS—Cisco Secure Access Control Server. An access policy control platform that is used for authentication and access control.
- LDAP—Lightweight Directory Access Protocol. A protocol that is used for authentication and access control.
- CUOM—Cisco Unified Operations Manager. A product from the Cisco Unified Communications Management Suite. It provides a comprehensive and efficient solution for network management and monitoring of Cisco Unified Communications deployments.
- VMware vCenter—VMware vCenter provides centralized control and visibility at every level of virtual infrastructure and unlocks the power of vSphere through proactive management.
- UCSM—Cisco Unified Computing System Manager. UCSM provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System, across multiple chassis and thousands of virtual machines.
- JBOSS_HOME—The path in which JBoss is installed. The JBOSS_HOME is *HCM_Dashboard_Install_Directory*/thirdparty/jboss.
- DCNM—Data Center Network Manager (DCNM) is a management solution that increases overall data center infrastructure uptime and reliability, hence improving business continuity. Cisco DCNM:
  - Automates the provisioning process

- Proactively monitors the SAN and LAN by detecting performance degradation
- Secures the network
- Streamlines the diagnosis of dysfunctional network elements.

HCM Service Assurance Architecture

Figure 1-1 shows the HCM Service Assurance architecture.

Figure 1-1 HCM Service Assurance Architecture



In Figure 1-1, the portal client logs into HCM Service Assurance with the provided username and password. The username and password details are stored in Cisco Secure ACS or LDAP. Cisco Secure ACS or LDAP is used to authenticate a user. After the user is authenticated, the client can log into HCM Service Assurance.

HCM interfaces with either Cisco Secure ACS 5.1 or Lightweight Directory Access Protocol (LDAP) server for client authentication. During the process of installation, you are prompted to choose an authentication server between ACS 5.1 and LDAP. This functionality is also available for users who upgrade from HCM 1.1 to HCM 1.2.

In Cisco Secure ACS 5.1, the default authorization policy for device administration is set to Deny. You must edit the authorization policy for device administration and set it to permitAccess for the HCM server.

For detailed information, see the *ACS 5.x Policy Model* Chapter in *User Guide for the Cisco Secure Access Control System 5.1*.

HCM uses HTTP or HTTPS protocols for communication and supports a VMware-based deployment and JBoss Clustering. VMware-JBoss Clustering is used so that the server is always available to the client.

The Scheduler periodically collects data from multiple CUOM, vCenter, and UCSM instances, deployed in a virtualized environment. It does this using Web Services API and XML-based API.

The collected data is then updated in the HCM database.

Pluggable user interface (UI) components called portlets, act as an individual application that retrieves data from various domain managers and displays information.

When you cross-launch the domain managers, CUOM, UCSM, DCNM-SAN, HCM Service Assurance uses single sign-on to cross launch these applications, using the HTTPS connection. HCM Service Assurance does not support single sign-on for vCenter. When you cross-launch the vCenter web page, you must sign in by entering the vCenter username and password.

HCM Service Assurance cross-launches the domain managers that support web-based UI. For domain managers without web-based UI, the alarm or event is retrieved using API calls and it is displayed in a separate window. HCM Service Assurance communicates with the domain managers using Web Services APIs and XML-based APIs.

What's New in HCM 1.2

The following table describes the new features added in HCM release 1.2.

Table 1-1 What's New in HCM 1.2

Summary	Description	Reference
Service Assurance		
Support to monitor additional domain managers—DCNM-SAN and DCNM-LAN.	You can monitor the alarms generated by the two domain managers DCNM-SAN and DCNM-LAN, using a newly-added portlet called the Aggregated Data Center. You can also cross-launch to the domain manager DCNM-SAN. You can add, view, edit, and delete the domain managers DCNM-LAN and DCNM-SAN using Customer Administration Portlet.	Terminology Used In HCM, page 1-2 Understanding HCM Service Assurance User Interface, page 1-10 Aggregated Data Center Portlet, page 2-26 Configuring DCNM-LAN, page 2-13 Configuring DCNM-SAN, page 2-13 DCNM-LAN, DCNM-SAN and HCM Service Assurance Alarm Mapping, page 2-32

Table 1-1 What's New in HCM 1.2 (continued)

Summary	Description	Reference
Indication to denote a change in the number of alarms since the last poll.	A new icon in the alarm summary table alerts you on the changed alarm count since the last poll. This functionality applies to the following portlets: • Aggregated Alarm Summary • Alarm Summary • Phone Summary.	Understanding Domain Manager Specific Alarms, page 2-30
Option to choose between LDAP and ACS 5.1 for authentication.	When you install or upgrade to HCM 1.2, you can select either ACS 5.1 or LDAP as your authentication server.	*Installation Guide for Cisco Hosted Collaboration Mediation, 1.2*
Ability to monitor alarms generated by UCSM Chassis.	You can monitor the alarms generated by UCSM Chassis besides the UCSM Blade. The alarms generated on the chassis are reported by the newly-added portlet, Aggregated Data Center.	Terminology Used In HCM, page 1-2 Understanding HCM Service Assurance User Interface, page 1-10 Aggregated Data Center Portlet, page 2-26
Ability to import customer and inventory data in bulk using a customized spreadsheet in limited number of steps.	Using a customized spreadsheet that contains customer and inventory information, you can easily add data to HCM and the underlying domain managers.	Adding Customer Data in Bulk, page 2-6 Troubleshooting Customer Onboarding Error Messages, page A-4
Availability of a new CUOM API that can invoked to update the NOC operator data.	You can share user credentials between HCM and CUOM by invoking an API in CUOM. The new CUOM API enables you to share operator data after entering the information only once.	Configuring CUOM, page 2-10
Multi-customer support for domain manager CUOM.	You can view customer-wise data for all alarms generated on CUOM.	Cross-Launching CUOM, page 2-17
Ability to upgrade to HCM 1.2 from HCM 1.1 without loss of data.	You can seamlessly migrate from HCM 1.1 to HCM 1.2 without loss of data.	*Installation Guide for Cisco Hosted Collaboration Mediation, 1.2*

Getting Started with HCM 1.2

You can install or upgrade to HCM 1.2 using either ACS or LDAP for authentication.

Using ACS

Step 1 Log in as **portaladmin.**

Step 2 Create a customer. For details, see Adding a Customer, page 2-6

Step 3 Create user. For details, see Adding a User, page 2-24

Step 4 Log out and log in with the user credentials you created.

Using LDAP

Step 1 Log in as **portaladmin.**

Step 2 Configure LDAP in Enterprise Admin portlet. For information, see *Installation Guide for Hosted Collaboration Mediation, 1.2*.

Step 3 Create a customer. For details, see Adding a Customer, page 2-6

Step 4 Create user. For details, see Adding a User, page 2-24

Step 5 Log out and log in with the user credentials you created.

The following are the other tasks that you need to perform:

- Add domain managers—See Configuring Domain Managers, page 2-10
- Add portlets—See Administration Portlets, page 2-4, Service Assurance Portlets, page 2-26
- Adding devices—See Adding Devices to a Customer, page 2-15,

As a pre-requisite to view alarms in aggregated data center, make sure you add DCNM-LAN, DCNM-SAN, and UCSM.

Starting HCM Service Assurance

You can launch HCM Service Assurance from your web browser.

To launch HCM Service Assurance:

Step 1 In your web browser, enter `http`://*Portal_Server*:*Port_Number*

Portal_Server is the IP address or the machine name of the server on which HCM Service Assurance is installed and *Port_Number* is the port number used.

The HCM Service Assurance login page appears.

Step 2 Enter your login credentials in the username and password fields.

Step 3 Click **Sign In** to log into HCM Service Assurance.

The HCM Service Assurance page appears.

An error message is displayed if the login credentials are wrong. To clear the wrong username and password, click **Clear**.

HCM Service Assurance users are subject to user privileges. Depending on your user profile, you might not see certain portlets or have access to certain functions. For more information about user privileges, see Understanding HCM Service Assurance Roles, page 1-16.

Configuring Session Timeout Value

The default session timeout value is 60 minutes. After 55 minutes, a message alerts you, and you will be prompted to extend the session; click **Extend** to extend the session. The session expires if you do not click the Extend option.

You can configure the session timeout value in the web.xml file.

To configure the session timeout value:

Step 1 Go to the *HCM_Root_Directory*\thirdparty\jboss\server\default\deploy\ROOT.war\WEB-INF directory.

Step 2 Open the web.xml file.

Step 3 Edit the value within the `<session-timeout>` and `</session-timeout>` tags.

For example, after changing the user timeout value to 60 minutes, the `<session-config>` element in the web.xml file should look like:

```
<session-config>
            <session-timeout>60</session-timeout>
</session-config>
```

Step 4 Restart the HCM Service Assurance server:

a. Go to the *HCM_Root_Directory*/bin directory.

b. Run **`./stop-hcm.sh`**.

c. Run **`./start-hcm.sh`**.

Modifying Database User Password in HCM Service Assurance Configuration File

You can modify the database user password by editing the configuration file. To do this:

Step 1 From the JBoss home directory, enter the following command and change the *password* instance with the new password:

```
../jdk/bin/java -cp
lib/jboss-common.jar:lib/jboss-jmx.jar:server/default/lib/jbosssx.jar:server/default/li
b/jboss-jca.jar org.jboss.resource.security.SecureIdentityLoginModule password
```

The encoded password appears.

For example, encoded password—5dfc52b51bd35553df8592078de921bc.

Step 2 Copy the encoded password that is generated.

Step 3 Go to the *HCM_Root _Directory*/thirdparty/jboss/server/default/conf directory.

Step 4 Open the login-config.xml file.

Step 5 Edit the value and paste the encoded password that you copied within the `<module-option name="password">` and `</module-option>` tags.

Note The `<module-option name="password">` and `</module-option>` tags appear twice in the login-config.xml file. You must edit the value at both instances.

The following is a sample of the login-config.xml file after the encoded password is modified. The `<module-option name="password">` and `</module-option>` tags have been highlighted.

```
<!-- Security domains for HCM encrypted database password jca framework -->
             <application-policy name="HCMEncryptDBPassword">
                <authentication>
                        <login-module
code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
                            <module-option name="username">db_username</module-option>
                        <module-option name="password">5dfc52b51bd35553df8592078de921bc
</module-option>
                            <module-option
name="managedConnectionFactoryName">jboss.jca:name=HCM_PORTAL,service=LocalTxCM</module
-option>
                        </login-module>
                </authentication>
            </application-policy>

    <!-- Security domains for HCM encrypted database password jca framework -->
             <application-policy name="HCMEncryptLocalDBPassword">
                <authentication>
                        <login-module
code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
                            <module-option name="username">db_username</module-option>
                        <module-option name="password">5dfc52b51bd35553df8592078de921bc
</module-option>
                            <module-option
name="managedConnectionFactoryName">jboss.jca:name=HCM_LOCAL,service=LocalTxCM</module-
option>
                        </login-module>
                </authentication>
            </application-policy>
```

Modifying ACS Password in HCM Service Assurance Configuration File

You can modify the ACS password by editing the configuration file. To do this:

Step 1 Enter the following command and change the *password* instance with the new password:

```
../jdk/bin/java -cp
server/default/lib/msdtportal.jar:server/default/lib/bcprov-jdk15-142.jar
com.cisco.util.Encryptor password
```

The encoded password appears.

For example, encoded password—47|-112|-52|126|-82|31|-15|46|-40|32|-87|45|72|-65|18|-15.

Step 2 Copy the encoded password that is generated.

Step 3 Go to the *HCM_Root_Directory*//thirdparty/jboss/server/default/deploy/ROOT.war/WEB-INF directory.

Step 4 Open the acs.properties file.

Step 5 Paste the encoded password that you copied in the ACS_SECRETKEY parameter.

The following is a sample of the acs.properties file after the encoded password is modified. The ACS_SECRETKEY parameter has been highlighted.

```
#ip address of the ACS server
ACS_IPADDRESS=172.20.120.145

#port number of the ACS Server
ACS_PORTNUMBER=49

#Secret Key Used for ACS Communication
ACS_SECRETKEY=47|-112|-52|126|-82|31|-15|46|-40|32|-87|45|72|-65|18|-15
```

Performing a Manual Backup and Restore

This section explains the procedure to manually backup and restore HCM 1.2 database and configuration files. Cisco recommends that you use a third party package or a VMware backup/restore tool for the procedure.

To automatically execute nightly backup, you can schedule cron jobs that call the assurancedb-backup.sh and hcm-assurance-backup.sh scripts.

The following steps explain the procedure to backup and restore database and configuration files.

Database

- Backup

```
cd <HCM_ROOT>/bin
./assurancedb-backup.sh user password host port BACKUP_DIRECTORY
```

- Restore

```
mysql -u root -p  <  <BACKUP_DIRECTORY>/assurance-db-backup.sql
```

Configuration Files

- Backup

```
cd <HCM_ROOT>/bin
./hcm-assurance-backup.sh install_root backup_dir
```

Note You can ignore the error message “File Not Found” that may appear. This message appears for missing optional files.

- Restore

```
cd <HCM_ROOT>
./bin/hcm-assurance-restore.sh backup_configuration_file
```

Understanding HCM Service Assurance User Interface

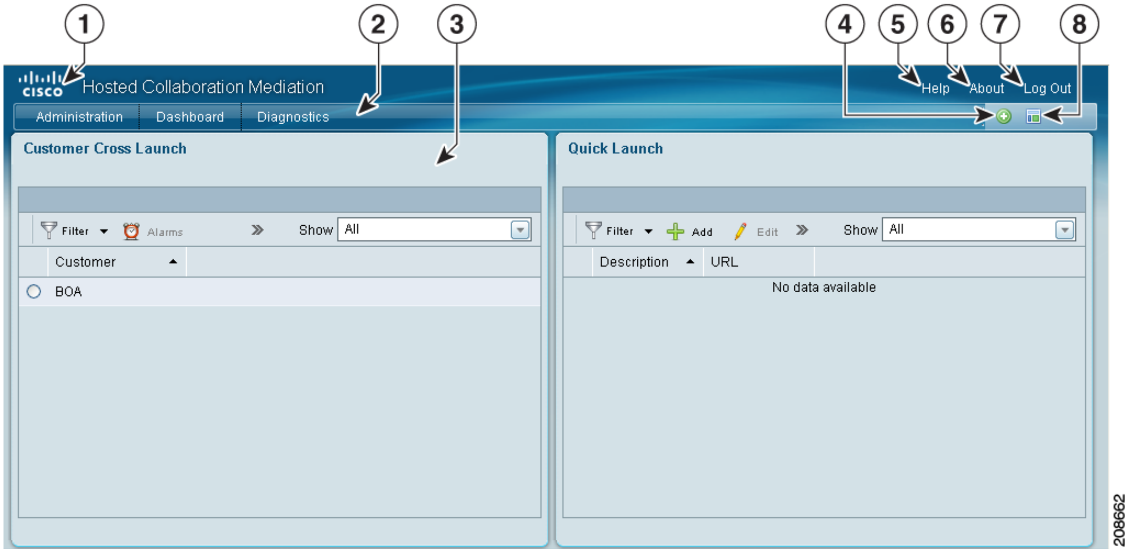
HCM Service Assurance offers an intuitive UI. This section describes the key components of the HCM Service Assurance UI:

- Common UI Elements and Options, page 1-11
- Adding Portlets, page 1-12
- Managing Screen Layout, page 1-13
- Understanding Portlets, page 1-14
- Changing the Look and Feel of the Portlet, page 1-15

Common UI Elements and Options

Figure 1-2 shows the common elements and options in the HCM Service Assurance UI.

Figure 1-2 HCM Service Assurance User Interface



Show All

Show All

No data available

Table 1-2 describes the common elements and options in the HCM Service Assurance UI.

Table 1-2 Common HCM Service Assurance UI Elements or Options

Number	Element or Option	Description
1	Cisco Logo	Click to display the official Cisco web site.
2	Navigation Bar	Displays the primary navigation tabs and the Add Portlet and Change Layout buttons.
3	Portlet	Portlet is a pluggable UI component. For detailed information about the purpose and function of each portlet, see Chapter 2, "Working with Portlets"
4	Add Portlet	Enables you to add portlets to HCM Service Assurance pages. See Adding Portlets, page 1-12
5	Help	Click to see the HCM User Guide.
6	About	Click to display the software version of HCM Service Assurance.
7	Log Out	Click to log out of HCM Service Assurance.
8	Change Layout	Enables you to specify the layout of the portlets. See Managing Screen Layout, page 1-13

Adding Portlets

You must log in as an admin user to add portlets. The Add Portlet button in the Navigation Bar enables you to add portlets to the HCM Service Assurance pages.

To add portlets:

Step 1 Navigate to the page on which you wish to add the portlet.

Step 2 Click the **Add Portlet** button in the Navigation Bar.

The Add Application dialog box appears, displaying a list of portlet categories.

Step 3 Click **Hosted Collaboration Mediation**.

A list of portlets belonging to the Hosted Collaboration Mediation category appears.

Step 4 Click the **Add** button corresponding to the portlet that you want to add. Alternatively, you also drag the portlet to the content area.

The portlet that you select appears in the page that you are currently viewing.

The Add Application dialog box provides options that enable you to search for portlets.

To search for a portlet and then add it to the page:

Step 1 In the Search Applications field, enter the name of the portlet.

The search results corresponding to the criteria that you specify appear.

Step 2 Click the **Add** button corresponding to the portlet that you want to add. Alternatively, you also drag the portlet to the content area.

The portlet that you select, appears in the page that you are currently viewing.

Managing Screen Layout

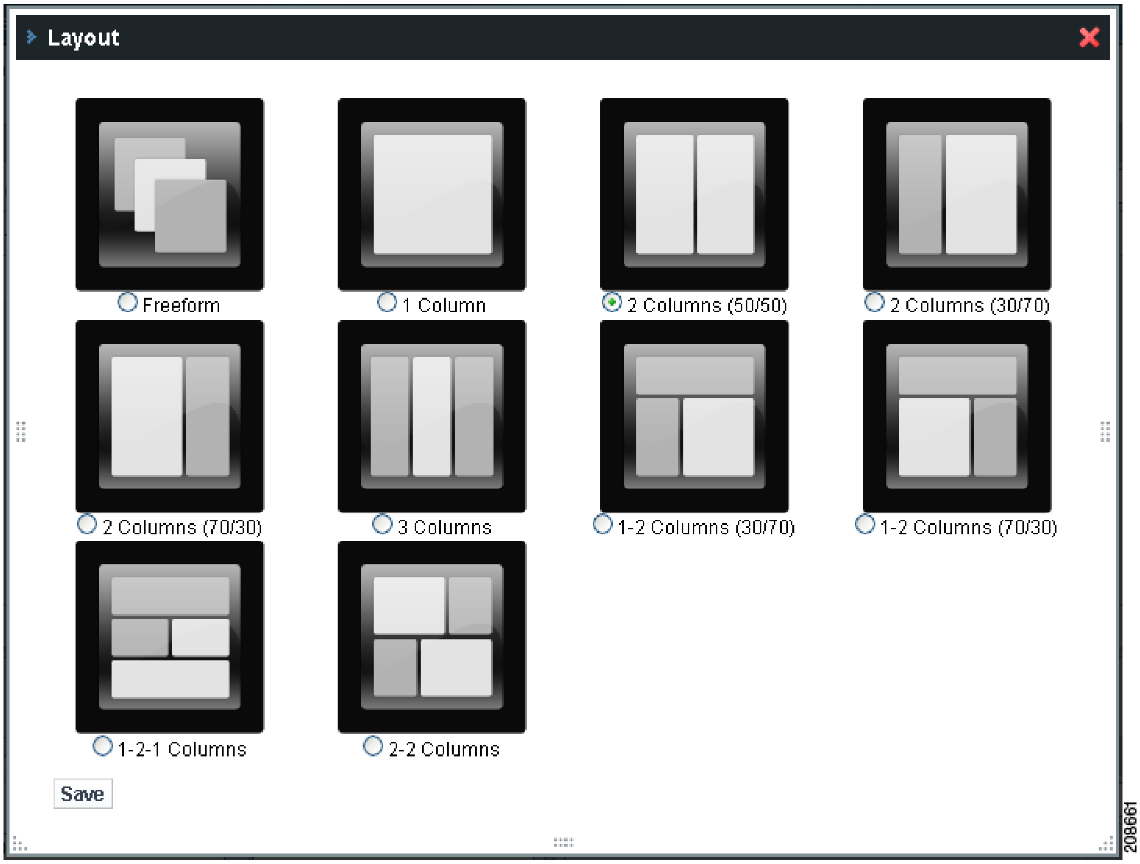
The Change Layout button in the Navigation Bar enables you to manage the layout of portlets that appear in the content area. You can change the layout of portlets, according to a set of available layout templates.

To change the layout of the portlets that appear in the content area:

Step 1 Click the **Change Layout** button in the Navigation Bar.

The Layout dialog box appears, displaying a list of available layout templates. Figure 1-3 shows the Layout dialog box.

Figure 1-3 Layout Dialog Box



○ Freeform
○ 1 Column
● 2 Columns (50/50)
○ 2 Columns (30/70)
○ 2 Columns (70/30)
○ 3 Columns
○ 1-2 Columns (30/70)
○ 1-2 Columns (70/30)
○ 1-2-1 Columns
○ 2-2 Columns

Step 2 Click the radio button corresponding to the layout template that you want to choose.

Step 3 Click **Save**.

The portlets in the content area re-align based on the layout that you selected in the Layout dialog box.

Understanding Portlets

HCM Service Assurance aggregates data from multiple virtualized instances of domain managers and displays summary information using pluggable UI components called portlets. Each portlet acts as an individual application that retrieves data from various domain managers to display information.

You can cross-launch the domain managers that support web-based UI from the portlet. In addition to displaying information, the portlets also act as entities from where the functionality of HCM Service Assurance flows. UI options that enable you to perform various workflow activities appear inside the portlets.

Figure 1-4 shows a sample portlet.

Figure 1-4 Sample Portlet

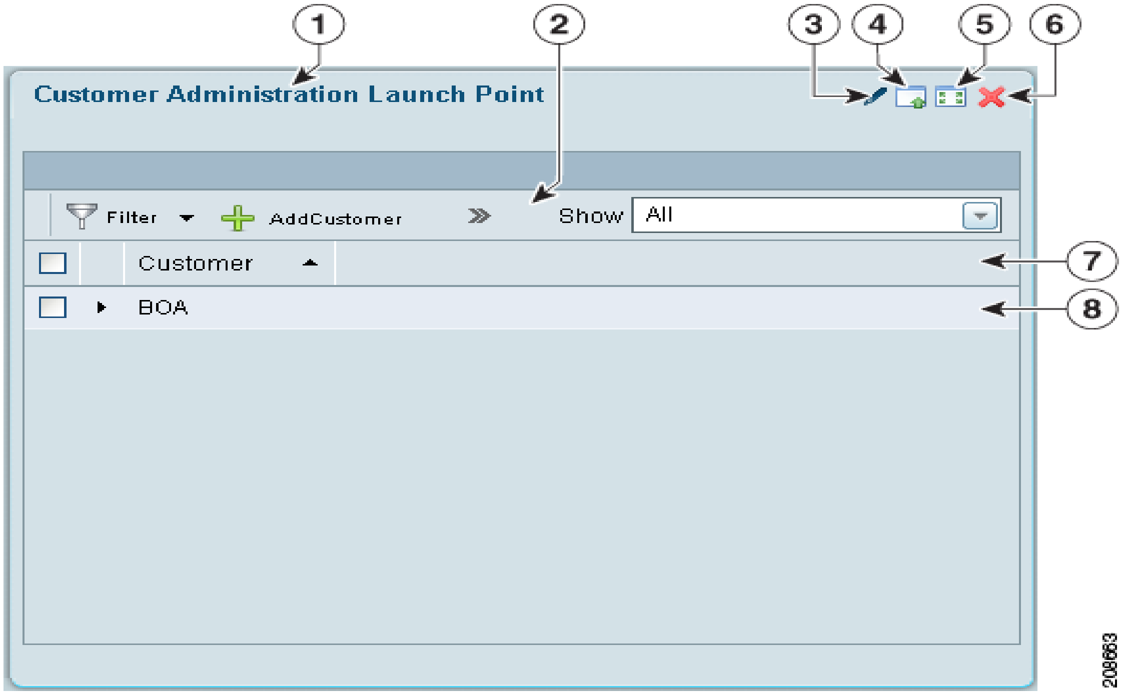


Table 1-3 describes the common UI options that appear in every portlet.

For detailed information about each portlet, see Chapter 2, "Working with Portlets".

Table 1-3 Common UI Options

Number	Description
1	Portlet Title—Displays the title of the portlet. Click **Portlet Title** to edit it.
2	Portlet Toolbar—Displays the various UI options that are available in the portlet. These options differ from portlet to portlet.
3	Look and Feel—Click to change the look and feel of the portlet. See Changing the Look and Feel of the Portlet, page 1-15.
4	Minimize—Click to minimize the portlet.
5	Maximize—Click to maximize the portlet.

Table 1-3 Common UI Options (continued)

Number	Description
6	Remove—Click to remove the portlet.
7	Column Header Row—Displays a check box and the column header for each column in the table.
8	Portlet Table—Information is displayed in tabular format in the portlet.

Changing the Look and Feel of the Portlet

Using the Look and Feel button in the portlet, you can set or alter the display properties corresponding to each portlet.

To set or alter the display properties corresponding to a portlet:

Step 1 In any portlet, click the **Look and Feel** button.

The Look and Feel dialog box appears.

Step 2 Use the following UI options available in the Look and Feel dialog box to set or alter the display properties, corresponding to the portlet:

- Portlet Configuration
- Text Styles
- Background Styles
- Border Styles
- Margin and Padding
- Advanced Styling
- WAP Styling

Step 3 Click **Save**.

Understanding HCM Service Assurance Roles

A role is associated with a specific job function or functions and provides the necessary permissions to perform these functions. The following types of roles are available for the HCM Service Assurance component:

- Admin, page 1-16
- Operator, page 1-17

Admin

An admin user has all administrative privileges. An admin user can create a user with admin or operator privileges. The username and password details are maintained in the Cisco Secure ACS or LDAP and the HCM database.

The HCM database must be synchronized with the username and password details. You must configure the user in Cisco Secure ACS or LDAP and then map the user in HCM Service Assurance.

Note The default admin username is *portaladmin* and the default password is *admin*.

When you log in as an admin user with the default username and password and provision a Cisco Secure ACS or LDAP user as a SuperAdmin, the default admin user will be disabled and you will not be able to log into the HCM server.

All the portlets will be available for the admin user:

- Customer Cross Launch
- Quick Launch
- Configuration
- User Administration
- Customer Administration Launch Point
- Alarm Summary
- Phone Summary
- Diagnostics Test
- Aggregated Data Center portlet

For detailed information about portlets, see Chapter 2, “Working with Portlets”

Operator

An operator has only monitoring privileges for a customer or a set of customers. An operator cannot add or modify any portlets. The following summary portlets are available for an operator:

- Quick Launch
- Customer Cross Launch
- Alarm Summary
- Phone Summary
- Aggregated Data Center portlet

For detailed information about portlets, see Chapter 2, “Working with Portlets”.

CHAPTER 2

Working with Portlets

Overview

This chapter describes all portlets available in HCM Service Assurance. It includes:

- Understanding the Filtering Option in Portlets, page 2-1
- Administration Portlets, page 2-4
- Service Assurance Portlets, page 2-26
- Diagnostics, page 2-35

Understanding the Filtering Option in Portlets

The Filter option allows you to narrow down the displayed data. Filtering provides a quick and easy way to identify a specific record that matches the given criteria provided by you. The following are the three filtering types:

- Quick Filter, page 2-2
- Filter by Example, page 2-2
- Advanced Filter, page 2-3

The Filter option is available in the following portlets:

- Customer Administration Launch Point
- Customer Cross Launch
- Quick Launch
- User Administration
- Aggregated Data Center
- Alarm Summary
- Phone Summary

Quick Filter

Quick Filter uses commonly used criteria for a given portlet as a set of preset filters. The preset filters list is displayed in the Show drop-down list in the portlet toolbar. The Show drop-down list consists of the following options:

- Manage Preset Filters—Allows you to edit or remove a preset filter. See Managing Preset Filters, page 2-2
- All—Allows you to clear the filter and retrieve the non-filtered data.
- Lists the preset filters.

To filter data in a portlet using the Quick Filter option:

Step 1 Click the **Show** drop-down list.

Step 2 Select one of the preset filters.

To create a preset filter, see Advanced Filter, page 2-3

The data appears according to the preset filter you selected.

Managing Preset Filters

To manage quick filters:

Step 1 Select **Manage Preset Filters** from the Show drop-down list.

The Manage Preset Filters dialog box appears.

Step 2 Select a preset filter.

Step 3 Click **Edit** to edit the preset filter or click **Remove** to remove the preset filter.

Step 4 Click **Cancel** to close the Manage Preset Filters dialog box.

Filter by Example

To filter data in a portlet using the Filter by Example option:

Step 1 Click **Filter** from the portlet toolbar, or click the **Filter** drop-down arrow and then select **Filter by Example.**

A text field appears in the column header. The number of text fields depend on the number of column headers.

Step 2 Enter the filtering criteria in the text field. This field is case sensitive.

The data in the portlet starts filtering as you type.

To clear the filter and retrieve non-filtered data, click the **Close** button that appears in the text field after you type the filtering criteria.

Advanced Filter

To filter data in a portlet using the Advanced Filter option:

Step 1 Click the **Filter** drop-down arrow.

Step 2 Select **Advanced Filter.**

A row appears, in which you can create a rule for filtering and then add the rule as a preset filter.

Step 3 To create a rule and then save the rule as a quick filter:

a. In the first column dropdown, select a filtering option.

Filtering options differ from portlet to portlet. To see the filtering options specific to a portlet, see the Filtering Types and Options table in the corresponding portlet section.

b. Select a relational operator from the second column drop-down list.

Relational operators differ from portlet to portlet. To see the relational operators specific to a portlet, see the Filtering Types and Options table in the corresponding portlet section.

c. Enter the filtering criteria in the text field in the third column.

d. Click **Go.**

The data appears according to the rule.

e. Click **Save** to add this rule as a preset filter.

The Save Preset Filter dialog box appears.

You can also click **Clear Filter** to clear the filter and retrieve the non-filtered data.

f. Enter a name for the quick filter in the Filter Name field.

g. Click **Save**.

The rule is saved as a preset filter and will appear in the Show drop-down list in the portlet toolbar.

Step 4 Click the **Add Criteria** button to create another rule.

You can add multiple rules.

Another row appears where you can create another rule for filtering. Go to Step 3 and follow the steps to create a rule and then save the rule as a preset filter.

You can delete the rule created by clicking the **Remove Criteria** button.

When you create multiple rules, the Match drop-down list appears. This allows you to select a single rule or select all rules. The options in the Match drop-down list are **All** and **Any**.

Administration Portlets

An admin user can view and modify all portlets. The Administration portlets allow you to view all customers and cross-launch CUOM, vCenter, and web pages for customer-centric views. The following are the Administration portlets:

- Customer Administration Launch Point Portlet, page 2-4
- Customer Cross Launch Portlet, page 2-16
- Configuration Portlet, page 2-18
- Quick Launch Portlet, page 2-19
- User Administration Portlet, page 2-21

Customer Administration Launch Point Portlet

To view the Customer Administration Launch Point portlet, go to **Administration > Customer Administration Launch Point.**

The Customer Administration Launch Point portlet allows admin users to configure customer details. As an admin user, you can cross-launch to the domain managers from the portlet. This section includes:

- UI Options, page 2-5
- Filtering Types and Options, page 2-5
- Adding a Customer, page 2-6
- Adding Customer Data in Bulk, page 2-6
- Customer Cross Launch Portlet, page 2-16
- Editing a Customer, page 2-9
- Deleting a Customer, page 2-9
- Viewing a Customer, page 2-10
- Configuring Domain Managers, page 2-10
- Editing Domain Manager Details, page 2-14
- Deleting a Domain Manager, page 2-14
- Viewing Domain Manager Details, page 2-15
- Adding Devices to a Customer, page 2-15

UI Options

Table 2-1 explains the UI options available in the Customer Administration Launch Point portlet.

The UI options in the portlet toolbar appear according to the screen resolution. The screen resolution used is 1024 by 768 pixels.

Table 2-1 Customer Administration Launch Point Portlet UI Options

UI Option	Description
Filter	Allows you to filter the data displayed in the portlet. See Table 2-2 for the list of filtering types and corresponding options available in the portlet.
Add Customer	Allows you to add a new customer.
Edit Customer	Allows you to edit customer details.
Delete Customer	Allows you to delete customer details.
View Customer	Allows you to view customer details.
Add Domain	Allows you to add domain manager credentials.
Edit Domain	Allows you to edit domain manager credentials.
Delete Domain	Allows you to delete domain manager credentials.
View Domain	Allows you to view domain manager credentials.
Customer On-board	Allows you to import customer data using a spreadsheet.

Filtering Types and Options

See Understanding the Filtering Option in Portlets, page 2-1 to understand the Filter option. Table 2-2 lists the filtering types and corresponding options available in the Customer Administration Launch Point portlet.

Table 2-2 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	Customer
Advanced Filter	Filter Dropdown	Customer
	Relational Operators	• Contains • Does not contain • Does not equal • Ends with • Is empty • Is exactly (or equals) • Is not empty • Starts with
	Text Field	Enter the filtering parameters.

Adding a Customer

To add a customer:

Step 1 Click **Add Customer** from portlet toolbar.

The Customer Configuration dialog box appears.

Step 2 Enter the customer name in the **Customer Name** field. This is a mandatory field.

Step 3 (Optional) Enter the description.

Step 4 Click **OK**.

The customer is added successfully.

An error message appears and the customer will not be added if:

- You try to add a duplicate customer.
- You do not enter the customer name in the Customer Name field.

Step 5 Click **Cancel** to close the Customer Configuration dialog box.

Adding Customer Data in Bulk

You can add the details of several customers in a single step. You can add the names of the customers, their credentials and domain manager details in a spreadsheet. You can directly log on to CUOM 8.6, using the same credentials.

Later, if you need to, you can change the credentials for a customer, using the HCM interface. This feature allows you to upload the data of up to 500 customers in a single step. To troubleshoot errors in uploading data, see Appendix A, “Troubleshooting Customer Onboarding Error Messages”.

You must follow these guidelines while you prepare the spreadsheet:

- Every combination of customer name and domain manager name must be unique.
- Fill out the DeviceInfo worksheet before you fill out the DeviceProtocolInfo worksheet.
- You can add AVMs only if you add VMs in the DomainManagers worksheet.
- Device information and IP address must be unique.
- Specify the Admin user and operator user IDs for the domain manager CUOM in the DomainManagers worksheet.

To do this, enter the details of customer in a spreadsheet that contains the columns and create a worksheet for each of the heading in bold. See Table 2-3 for details.

The spreadsheet and the worksheets must be in the order specified below. Follow the naming conventions exactly as mentioned in this document. Every column that contains data must have an appropriate heading as outlined below.

Table 2-3 Customer On Boarding Spreadsheet

Column Name	Description
CustomerInfo	
Customer_Name	Name of the customer

Table 2-3 Customer On Boarding Spreadsheet

Column Name	Description
Description	Description for customer.
Remarks	Remarks, if any.
DomainManagers	
Customer_Name	Name of the customer
DomainManagerType	Domain manager type. This can be any one of the following: • CUOM • UCSM • DCNM-LAN • DCNM-SAN • VCENTER.
ip	IP address of the device
admin_user	Admin username.
admin_pass	Admin password.
operator_user	Operator username.
operator_pass	Operator password.
jtapi_user	Username of Java Telephony API (JTAPI).
jtapi_pass	Password of JTAPI.
jtapi_helperphone1	Helper Phone 1 is one of the alternative phone number used to test the configured customer line.
jtapi_helperphone2	Helper Phone 2 is another alternative phone number used to test the configured customer line.
jtapi_pstn	Number of the public switched telephone network (PSTN).
jtapi_ipsla	IP address of the nearest IP Service Level Agreement (IPSLA) device.
VCenterVMs	
Customer_Name	Name of the customer.
DomainManager	Name of domain manager.
Remarks	Remarks, if any.
DeviceInfo	
customer_name	Name of the customer
deviceip	Device IP.
dns_name	Name of DNS.
private_ip	Private IP address.
private_dns_name	Private DNS name.

Table 2-3 Customer On Boarding Spreadsheet

Column Name	Description
snmpv1v2_ver	Enter version—can be 1,2 or 3.
snmpv1v2_rocomm	Enter read-only community.
snmpv1v2_rwcomm	Enter read-write community.
snmpv3_user	SNMP v3 username.
snmpv3_auth_type	Authorization type—MD5 or SHA.
snmp_auth_pass	Authorization password.
snmpv3_priv_type	Privilege type.
snmpv3_priv_pass	Privilege password.
Remarks	Remarks, if any.
DeviceProtocolInfo	
Customer_Name	Name of the customer.
DeviceIP/DNS	Device IP.
Protocol	Protocol information.
username	Username.
password	Password.
portnumber	Port number.
Remarks	Remarks, if any.

Step 1 Go to **Administration> Customer Administration Launch point.**

Step 2 Click **Customer Onboard.**

A dialog box appears

Step 3 Import the excel sheet that contains the details of customer from this dialog box.

The status of the operation appears.

- If the operation is successful, the following message appears:

```
Validation Success. Please click the On-board status button to get the status.
```

- If the operation fails, the following message appears:

```
Validation Failed. Please click the download link for downloading the error file.
```

Step 4 Click **OK.**

Step 5 Click » to expand menu items.

Step 6 Click on **Onboard Status** to view the status of the operation.

If the operation was not successful, an error message appears. Click Download.

A spreadsheet with errors in Remarks column gets downloaded.

- If the error appeared because of an invalid entry in the spreadsheet, the same file will be updated.
- If the error appeared because of processing problems the file with be prefixed with '*errored*'.

Note If you are viewing using Internet Explorer, the error file has the extension *.zip*. Click **Save**, change the extension to *.xls*, and save it in your local drive.

Editing a Customer

To edit a customer:

Step 1 Select a customer.

Step 2 Click » and select **Edit Customer**.

The Customer Configuration dialog box appears.

Step 3 Edit the description.

You cannot edit the customer name.

Step 4 Click **OK**.

Step 5 Click **Cancel** to close the Customer Configuration dialog box.

Deleting a Customer

To delete a customer:

Step 1 Select a customer. You can select one customer or multiple customers.

Step 2 Click » and select **Delete Customer**.

The following message appears in the dialog box.

```
Are you sure you want to delete the selected customer(s)?
```

Step 3 Click **OK.** To cancel the operation, go to Step 4.

The customer details are deleted from the HCM database.

If the portlet is open, the new data will not be reflected until the server is refreshed or a new session is opened.

An error appears if the customer you are trying to delete has devices associated with CUOM. You have to first manually delete the devices, and then delete the customer. If no devices are associated, the customer is deleted and users are deleted from CUOM.

Step 4 Click **Cancel** to cancel the operation.

Viewing a Customer

To view a customer:

Step 1 Select a customer. You can select only one customer.

Step 2 Click » and select **View Customer**.

The Customer Configuration dialog box appears, displaying the details of the selected customer.

Step 3 Click **Close** to close the Customer Configuration dialog box.

Configuring Domain Managers

You can configure domain managers in the Customer Administration Launch Point portlet. This section includes:

- Configuring CUOM, page 2-10
- Configuring UCSM, page 2-12
- Configuring vCenter, page 2-12
- Configuring DCNM-LAN, page 2-13
- Configuring DCNM-SAN, page 2-13

Configuring CUOM

To be able to add domain manager CUOM, ensure that the super admin credentials are admin/admin. If you specified different credentials, do the following to change them:

Step 1 Go to *HCM_Install_Directory*/thirdparty/jboss/server/default/conf/portal_props/ and change values in the monitor.properties file.

Step 2 Specify the username against SUPER_ADMIN_USER and the password against SUPER_ADMIN_PASSWORD.

Step 3 Restart the server.

To configure CUOM:

Step 1 Select a customer.

Step 2 Click » and select **Add Domain.**

The Add Domain Manager Configuration dialog box appears.

Step 3 Select **CUOM** from the Select Domain Manager Name drop-down list.

Step 4 Enter the following details in the Domain Configuration tab:

- IP Address—IP address of the device.
- Admin Username—CUOM admin username. Mandatory. You cannot provide the username **admin** for admin username since it is the ID of super user of CUOM. Admin user will be created using Network Administrator role.

The username must contain a minimum of five characters. Avoid using special characters; if you must use them, launch CUOM, and go to **Administration > Server Administration (Common Services) > Security > Local User Policy Setup**.

Check **Allow Special Characters in Username.** The special characters that are allowed are listed here within square brackets: [~], [@], [#], [_], [‘], [-], [\], [/], [.], [space].

- Admin Password—CUOM admin password. Mandatory. The username must contain a minimum of five characters.
- Operator Username—CUOM operator username. Optional. Operator user will be created using Network Operator role.

  The username must contain a minimum of five characters. Avoid using special characters; if you must use them, launch CUOM, and go to **Administration > Server Administration (Common Services) > Security > Local User Policy Setup**.

  Check **Allow Special Characters in Username.** The special characters that are allowed are listed here within square brackets: [~], [@], [#], [_], [‘], [-], [\], [/], [.], [space].
- Operator Password—CUOM operator password. Optional. The password must contain a minimum of five characters.

Step 5 Enter the following details in the Diagnostics Configuration tab:

- JTAPI Username—Username of Java Telephony API (JTAPI).
- JTAPI Password—Password of JTAPI.

  JTAPI supports telephony call control and is an extensible API. JTAPI is designed to scale for use in a range of domains. JTAPI can be used from first-party call control in a consumer device, to third-party call control, in large distributed call centers.

  The phone tests that are run as part of batch testing and on-demand testing, take control of a real phone in the network and make a call from one phone to another phone. Phone Tests use JTAPI credentials.

  While running on-demand phone tests, the JTAPI credentials must be provided in the phone test creation page. The JTAPI credentials must be configured in Cisco Unified Communications Manager for Phone Tests in CUOM to work properly.
- Helper Phone 1—Helper Phone 1 is one of the alternative phone number used to test the configured customer line.
- Helper Phone 2—Helper Phone 2 is another alternative phone number used to test the configured customer line.

  Helper Phone 1 and Helper Phone 2 are configured under the same Cisco Unified Communications Manager and are required while running Phone Tests.
- Phone Number—Number of the public switched telephone network (PSTN).
- Nearest IP SLA Device IP—IP address of the nearest IP Service Level Agreement (IPSLA) device.

  IP SLA-based diagnostic tests can measure the performance of WAN links and node-to-node network quality. Phone status tests use IP SLA to monitor the reachability of key phones in the network.

Step 6 Click **Save**.

Step 7 Click **Submit**.

Step 8 Click **Cancel** to close the Add Domain Manager Configuration dialog box.

Configuring UCSM

To configure UCSM:

Step 1 Select a customer.

Step 2 Click » and select **Add Domain**.

The Add Domain Manager Configuration dialog box appears.

Step 3 Select **UCSM** from the Select Domain Manager Name drop-down list.

Step 4 Enter the following details in the Configuration area:

- IP Address—IP address of the device.
- Admin Username—UCSM admin username. Mandatory.
- Admin Password—UCSM admin password. Mandatory.
- Operator Username—UCSM operator username. Optional.
- Operator Password—UCSM operator password.Optional.

Step 5 Click **Save**.

Step 6 Click **Submit**.

Step 7 Click **Cancel** to close the Add Domain Manager Configuration dialog box.

Configuring vCenter

To configure vCenter:

Step 1 Select a customer.

Step 2 Click » and select **Add Domain**.

The Add Domain Manager Configuration dialog box appears.

Step 3 Select **vCenter** from the Select Domain Manager Name drop-down list.

Step 4 Enter the following details in the Domain Configuration tab:

- IP Address—IP address of the device.
- Admin Username—vCenter admin username. Mandatory.
- Admin Password—vCenter admin password. Mandatory.
- Operator Username—vCenter operator username. Optional.
- Operator Password—vCenter operator password. Optional.

Step 5 In the VM Configuration tab, click the **Click here to get VM** button.

The available virtual machines (VMs) appear in the Available VM box.

Step 6 Move the VM that you want to add, using the following options:

- >>—Moves all VMs from the Available VM list to the Selected VM list.
- >—Moves a single VM from the Available VM list to the Selected VM list.
- <—Moves a single VM from the Selected VM list to the Available VM list.
- <<—Moves all VMs from the Selected VM list to the Available VM list.

Step 7 Click **Save**.

Step 8 Click **Submit**.

Step 9 Click **Cancel** to close the Add Domain Manager Configuration dialog box.

Configuring DCNM-LAN

To configure DCNM-LAN:

Step 1 Select a customer.

Step 2 Click » and select **Add Domain**.

The Add Domain Manager Configuration dialog box appears.

Step 3 Select **DCNM-LAN** from the Select Domain Manager Name drop-down list.

Step 4 Enter the following details in the Configuration area:

- IP Address—IP address of the device.
- Admin Username—DCNM-LAN admin username. Mandatory.
- Admin Password—DCNM-LAN admin password. Mandatory.
- Operator Username—DCNM-LAN operator username. Optional.
- Operator Password—DCNM-LAN operator password. Optional.

Step 5 Click **Save**.

Step 6 Click **Submit**.

Step 7 Click **Cancel** to close the Add Domain Manager Configuration dialog box.

Configuring DCNM-SAN

To configure DCNM-SAN:

Step 1 Select a customer.

Step 2 Click » and select **Add Domain**.

The Add Domain Manager Configuration dialog box appears.

Step 3 Select **DCNM-SAN** from the Select Domain Manager Name drop-down list.

Step 4 Enter the following details in the Configuration area:

- IP Address—IP address of the device.
- Admin Username—DCNM-SAN admin username. Mandatory.
- Admin Password—DCNM-SAN admin password. Mandatory.
- Operator Username—DCNM-SAN operator username. Optional.
- Operator Password—DCNM-SAN operator password. Optional.

Step 5 Click **Save**.

Step 6 Click **Submit**.

Step 7 Click **Cancel** to close the Add Domain Manager Configuration dialog box.

Editing Domain Manager Details

To edit domain manager details:

Step 1 Select the customer whose domain manager details you want to edit.

Step 2 Select the domain manager that you want to edit from the table in the portlet.

Step 3 Click » and select **Edit Domain**.

The Edit Domain Manager Configuration dialog box appears.

Step 4 Edit the fields that you want to edit.

Step 5 Click **Save**.

Step 6 Click **Submit**.

Step 7 Click **Cancel** to close the Edit Domain Manager Configuration dialog box.

Deleting a Domain Manager

To delete a domain manager:

Step 1 Select the customer whose domain manager you want to delete.

Step 2 Select the domain manager that you want to delete from the table in the portlet.

Step 3 Click » and select **Delete Domain**.

The following message appears in the confirmation window.

```
Are you sure you want to delete the selected domain manager(s)?
```

Note An error message appears if you are trying to delete domain manager CUOM when it has devices associated. You have to first manually delete the devices, and then delete the domain manager. If no devices are associated, domain manager is deleted and users are deleted from CUOM.

Step 4 Click **OK**. To cancel the request, go to Step 5.

Step 5 Click **Cancel** to cancel the operation.

Viewing Domain Manager Details

To view domain manager details:

Step 1 Select the customer whose domain manager details you want to view.

Step 2 Select the domain manager for which you want to see the details.

Step 3 Click » and select **View Domain**.

The View Domain Manager Configuration window appears and you can see the details in the domain manager. These details cannot be changed.

Step 4 Click **Close** to close the View Domain Manager Configuration dialog box.

Adding Devices to a Customer

To add devices to a particular customer:

Step 1 From the Customer Administration Launch Point, check the customer and CUOM against which you want to add devices.

Step 2 Click » and select **Add Devices**.

The **Add Devices** screen appears.

Step 3 Enter device details. If you select the Device Type as SNMP v1 or SNMP v2, the SNMP v3 area gets dimmed.

Step 4 Click **Add**.

Step 5 Click **Cancel.**

Deleting a Device/Editing Device Details

To edit details or delete devices of a particular customer:

Step 1 From the Customer Administration Launch Point, check the customer and CUOM against which you want to delete/edit devices.

Step 2 Select the domain manager for which you want to see the details.

Step 3 Click » and select **Edit/Delete.**

The **Edit Device Configuration** screen appears.

- To delete a device, click **Delete**
- To edit device details, change the device details fields appropriately. If you select the Device Type as SNMP v1 or SNMP v2, the area for enter SNMP v3 details gets dimmed.

Note If some devices that you added earlier are missing, it indicates that the server time and time zonein HCM and CUOM are not synchronized. Run the Network Time Protocol program on both HCM and CUOM.

Step 4 Click **Edit.**

Step 5 Click **Close.**

Customer Cross Launch Portlet

To view the Customer Cross Launch portlet, go to **Administration > Customer Cross Launch.**

The Customer Cross Launch portlet displays the list of customers configured in HCM Service Assurance. Select a customer and then select the cross-launch option. Depending on the option you choose, the corresponding domain manager web page is cross-launched.

You can cross launch an unlimited number of windows for different customers. A single session is used for all CUOM cross-launches for a customer.

Note For the UI options to be enabled, you must select a customer.

Table 2-4 explains the UI options available in the Customer Cross Launch portlet.

The UI options in the portlet toolbar appear according to the screen resolution. The screen resolution used is 1024 by 768 pixels.

Table 2-4 Customer Cross Launch Portlet UI Options

UI Option		Description
Filter		Allows you to filter the data displayed in the portlet. See Table 2-5 for the list of filtering types and corresponding options available in the portlet.
CUOM	Alarms	Allows you to cross-launch the CUOM Alerts and Events page.
	Phones	Allows you to cross-launch the CUOM Phone Inventory page.
	SLV	Allows you to cross-launch the CUOM Service Level View.
	Test	Allows you to cross-launch the CUOM Diagnostics page.
vCenter Alarm		Allows you to cross-launch vCenter Alarms page.
UCSM Alarm		Allows you to cross-launch the UCSM Alarms page.
UCSM Chassis		Allows you to cross-launch the UCSM Chassis page.
DCNM-SAN		Allows you to cross-launch the DCNM-SAN page.

Cross-Launching CUOM

To cross-launch CUOM, you must configure the port number in HCM Service Assurance. For example, if CUOM is installed in port number 443, you must configure the port number in HCM Service Assurance to 443. You can see customer-wise data after cross-launching to CUOM.

To configure the port number in HCM Service Assurance:

Step 1 Navigate to the following directory:

HCM_Root_Directory\thirdparty\jboss\server\default\deploy\ROOT.war\WEB-INF

Step 2 Open the crosslaunch.properties file.

Step 3 Edit the following parameters, as needed:

- CUOM_LOGIN_PROTOCOL
- CUOM_LOGIN_PORTNUMBER
- CUOM_CROSS_LAUNCH_PROTOCOL
- CUOM_CROSS_LAUNCH_PORTNUMBER

Cross-launching to CUOM will fail if:

- You enter invalid CUOM IP address.
- You enter invalid CUOM admin username or password.
- You enter invalid CUOM operator username or password.
- HTTPS support is not enabled in CUOM.

Filtering Types and Options

See Understanding the Filtering Option in Portlets, page 2-1 to understand the Filter option. Table 2-5 lists the filtering types and corresponding options available in the Customer Cross Launch portlet.

Table 2-5 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	Customer

Table 2-5 Filtering Types and Options (continued)

Filter Types	Options	
Advanced Filter	Filter Dropdown	Customer
	Relational Operators	- Contains - Does not contain - Does not equal - Ends with - Is empty - Is exactly (or equals) - Is not empty - Starts with
	Text Field	Enter the filtering parameters.

Configuration Portlet

To view the Configuration portlet, go to **Administration > Configuration.**

The Configuration portlet allows the admin user to update configuration parameters. This section includes:

- Configuring Polling Interval, page 2-18
- Configuring Portlet Refresh Frequency, page 2-19

Configuring Polling Interval

To configure polling interval:

Step 1 Go to **Configuration > Polling Configuration.**

Step 2 Select the domain manager from the Domain Manager drop-down list.

Step 3 Enter the value for the **Polling Interval** field.

Step 4 Click **Save**.

Step 5 Click **Submit**.

Configuring Portlet Refresh Frequency

To configure the refresh frequency of a portlet:

Step 1 Go to **Configuration > Portal Configuration.**

Step 2 Select the portlet from the Portlet drop-down list.

Step 3 Enter the value for the **Refresh Frequency** field.

Step 4 Click **Save**.

Step 5 Click **Submit**.

Quick Launch Portlet

To view the Quick Launch portlet, go to **Administration > Quick Launch.**

The Quick Launch portlet allows the admin user to navigate to different URLs. This section includes:

- Filtering Types and Options, page 2-20
- Adding a URL, page 2-20
- Editing a URL, page 2-21
- Deleting a URL, page 2-21

Table 2-6 lists the Quick Launch portlet UI options.

The UI options in the portlet toolbar appear according to the screen resolution. The screen resolution used is 1024 by 768 pixels.

Table 2-6 Quick Launch Portlet UI Options

UI Option	Description
Filter	Allows you to filter the data displayed in the portlet. See Table 2-7 for the list of filtering types and corresponding options available in the portlet.
Add	Allows you to add a new URL.
Edit	Allows you to edit an existing URL.
Delete	Allows you to delete an existing URL.

Filtering Types and Options

See Understanding the Filtering Option in Portlets, page 2-1 to understand the Filter option. Table 2-7 lists the filtering types and corresponding options available in the Quick Launch portlet.

Table 2-7 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	• Description • URL
Advanced Filter	Filter Dropdown	• Description • URL
	Relational Operators	• Contains • Does not contain • Does not equal • Ends with • Is empty • Is exactly (or equals) • Is not empty • Starts with
	Text Field	Enter the filtering parameters.

Adding a URL

To add a URL:

Step 1 Click **Add** from the portlet toolbar.

Step 2 Enter the following details:

a. Description—Description of the URL.

b. URL—URL of the page that you are adding.

Note You can add a maximum of 20 URLs.

Step 3 Click **OK**.

The URL is added successfully. This URL will be launched in a different window.

Step 4 Click **Cancel** to close the Quick Launch Point dialog box.

Editing a URL

To edit a URL:

Step 1 Select the Quick Launch row that you want to edit.

Step 2 Click **Edit** from the portlet toolbar.

You cannot edit the Description field.

The Quick Launch Point dialog box opens.

Step 3 Edit the **URL**.

Step 4 Click **OK**.

Step 5 Click **Cancel** to close the Quick Launch Point dialog box.

Deleting a URL

To delete a URL:

Step 1 Select the Quick Launch row that you want to delete. You can select single or multiple rows.

Step 2 Click » and select **Delete**.

The following message appears in the dialog box.

```
Are you sure you want to delete the selected link(s)?
```

Step 3 Click **OK**.

The selected URL is deleted from the Quick Launch portlet and HCM database.

Step 4 Click **Cancel** to cancel the operation.

User Administration Portlet

To view the User Administration portlet, go to **Administration > User Administration.**

The User Administration portlet allows you to manage users and assign specific customers per user. The User Administration portlet manages the admin and operator user details. You can assign privileges and map customers to the user.

You must create a user ID in the Cisco Secure ACS server and then map the new user in the User Administration portlet. The User Administration portlet allows the admin user to create a user with operator or admin credentials. For all admin users, the following details are displayed:

- User ID
- Customers
- Privilege

It includes the following sections:

- UI Options, page 2-22
- Filtering Types and Options, page 2-23
- Adding a User, page 2-24
- Editing a User, page 2-25
- Deleting a User, page 2-25
- Viewing a User, page 2-26

UI Options

Table 2-8 lists the User Administration portlet UI options.

The UI options in the portlet toolbar appear according to the screen resolution. The screen resolution used is 1024 by 768 pixels.

Table 2-8 User Administration Portlet UI Options

UI Option	Description
Filter	Allows you to filter the data displayed in the portlet. See Table 2-9 for the list of filtering types and corresponding options available in the portlet.
Add	Allows you to add a new user.
Edit	Allows you to edit user details.
Delete	Allows you to delete user details.
View	Allows you to view user details.

Filtering Types and Options

See Understanding the Filtering Option in Portlets, page 2-1 to understand the Filter option. Table 2-9 lists the filtering types and corresponding options available in the User Administration portlet.

Table 2-9 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	• User ID • Customers • Privilege
Advanced Filter	Filter Dropdown	• User ID • Customers • Privilege
	Relational Operators	• Contains • Does not contain • Does not equal • Ends with • Is empty • Is exactly (or equals) • Is not empty • Starts with
	Text Field	Enter the filtering parameters.

Adding a User

To add a user:

Step 1 Click **Add** from the portlet toolbar.

The User Configuration dialog box opens. See Table 2-10 for the UI options.

Note You must be logged in as an admin user to add users.

Step 2 Enter the following details:

a. Used ID—Enter the user ID for the user. This is a mandatory field.

b. Privilege—Select the privilege. The following two options are available:

- Admin—Admin has access to all of the portlets. Admin can create another user with admin or operator privileges. By default, all customers will be selected for this user.
- Operator—Operator has access to all of the portlets except Customer Administration Launch Point and User Management.
- Password— Password to be associated with the user ID. If you are using ACS for authentication, the password you specify must be the one that you mentioned at the time of installation.
- Email ID—Enter an email address for the username. User will not be added if you provide duplicate email ID.
- First Name—Enter the user's first name
- Last Name—Enter the user's last name.

c. Available Customers—Lists all added customers. Select the customers that you want to map to the user. Click the arrow to move the selected customers to the Selected Customers list.

d. Selected Customers—Lists all selected customers.

Step 3 Click **OK**.

The user is added successfully.

You cannot add users to whom there are no customers assigned.

Step 4 Click **Cancel** to close the User Configuration dialog box.

Table 2-10 lists the UI options in the User Configuration dialog box.

t

Table 2-10 User Configuration Dialog Box UI Options

UI Option	Description
>>	Allows you to move all of the customers from the Available Customers list to the Selected Customers list.
>	Allows you to move a single customer or multiple selected customers from the Available Customers list to the Selected Customers list.

Table 2-10 User Configuration Dialog Box UI Options (continued)

UI Option	Description
<	Allows you to move a single customer or multiple selected customers from the Selected Customers list to the Available Customers list.
<<	Allows you to move all of the customers from the Selected Customers list to the Available Customers list.

Editing a User

To edit a user:

Step 1 Select a user.

Step 2 Click **Edit** from the portlet toolbar.

The User Configuration dialog box appears.

Step 3 Modify the user details.

You cannot edit the user ID.

Step 4 Click **OK**.

The user details are updated successfully.

Step 5 Click **Cancel** to close the User Configuration dialog box.

Note Admin users cannot edit their own user IDs.

Deleting a User

To delete a user:

Step 1 Select a user. You can select multiple users.

Step 2 Click » and select **Delete**.

Step 3 The following message appears in the dialog box..

```
Are you sure that you want to delete the selected user(s)?
```

Step 4 Click **OK**

The selected user is deleted successfully from the User Administration portlet and HCM database.

Step 5 Click **Cancel** to cancel the operation.

Note Admin users cannot delete their own user IDs.

Viewing a User

To view a user:

Step 1 Select a user. You can select only one user.

Step 2 Click » and select **View**.

The user details are displayed in the User Configuration dialog box.

You cannot edit user details using the View User option.

Step 3 Click **Close** to close the User Configuration dialog box.

Service Assurance Portlets

The Service Assurance portlets are summary portlets and are available to all users. The Service Assurance portlets display the alarms by customers, alarms by domain managers, and phone summaries

The following are the Service Assurance portlets:

- Aggregated Data Center Portlet, page 2-26
- Alarm Summary Portlet, page 2-27
- Phone Summary Portlet, page 2-33

Aggregated Data Center Portlet

To view the Aggregated Data Center portlet:

Step 1 Choose **Dashboard > Aggregated Data Center.**

The Aggregated Data Center portlet appears

Step 2 Use this portlet to view alarms of DCNM-SAN, DCNM-LAN, and UCSM Chassis. You can also cross-launch the domain managers DCNM-SAN and UCSM Chassis.

The portlet also displays the alarms for these domain managers.

To know more about the details displayed in this pane, see Domain Manager Specific Alarms.

This section covers the following topics:

- Filtering Types and Options, page 2-27
- Understanding the Alarm Summary Information, page 2-28
- Understanding the Color Scheme Used and Alarm Status, page 2-29
- Understanding Domain Manager Specific Alarms, page 2-30
- Understanding Alarm Mapping, page 2-31

Alarm Summary Portlet

To view the Alarm Summary portlet, choose **Dashboard > Alarm Summary.**

The Alarm Summary portlet displays the alarms by customers and alarms by domain managers. The Alarm Summary portlet lists all of the customers that administration supports.

When you add or delete a customer, the Alarm Summary portlet information is updated to reflect the status.

This section covers the following topics:

- Filtering Types and Options, page 2-27
- Understanding the Alarm Summary Information, page 2-28
- Understanding the Color Scheme Used and Alarm Status, page 2-29
- Understanding Domain Manager Specific Alarms, page 2-30
- Understanding Alarm Mapping, page 2-31

Filtering Types and Options

The Filter option is available in the portlet. See Understanding the Filtering Option in Portlets, page 2-1 to understand the Filter option.

When you select the Filter by Example option to filter data, search fields appear in all columns and you must enter alphabetical or numerical data in these fields. If you enter alphabetical or numerical data in the search fields in the First column and the Summary column, no data will be displayed because both columns display graphical data.

If you select the Advanced Filter option, do the following:

Step 1 Select **Summary** in the Filter dropdown list.

Step 2 Select any one of the relational operators.

Step 3 Enter alphabetical or numerical data in the Text Field.

Step 4 Click **Go.**

No data will be displayed because the Summary column displays only graphical data.

To understand the color scheme used in HCM Dashboard, see Table 2-13 and to understand the icons used in HCM Service Assurance, see Table 2-14.

Table 2-11 lists the filtering types and corresponding options available in the Alarm Summary portlet.

Table 2-11 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	• Customer • Critical • Warning • Information • Cleared • RequireAck • Total
Advanced Filter	Filter Dropdown	• Customer • Critical • Warning • Information • Cleared • RequireAck • Total
	Relational Operators	• Does not equal • Is exactly (or equals) • Is greater than • Is greater than or equal to • Is less than • Is less than or equal to
	Text Field	Enter the filtering parameters.

Understanding the Alarm Summary Information

The Alarm Summary portlet displays the information for each customer or domain manager in tabular format. The total number of critical, warning, and cleared alarms are displayed in the Information Bar in the portlet. Table 2-12 describes the columns in the Alarm Summary portlet.

Table 2-12 Alarm Summary Information

Column Header	Description
Customer/Domain Manager	Displays the name of the customer or domain manager.
Summary	The colors in this column represent the different alarms for a customer. For example, if there are only critical alarms for a customer, the table cell will be in red. See Table 2-13 to understand the color scheme used in HCM Service Assurance.
Critical	Displays the number of critical alarms for each customer.

Table 2-12 Alarm Summary Information (continued)

Column Header	Description
Warning	Displays the number of warning alarms for each customer.
Information	Displays the number of informational alarms for each customer.
Cleared	Displays the number of cleared alarms for each customer.
RequireAck	Displays the number of alarms that require acknowledgement for each customer.
Total	Displays the total of alarms for each customer.

Understanding the Color Scheme Used and Alarm Status

The Alarm Summary portlet shows different alarms with different colors. Table 2-13 lists the colors used and the corresponding alarm status.

Table 2-13 Color and Alarm Status

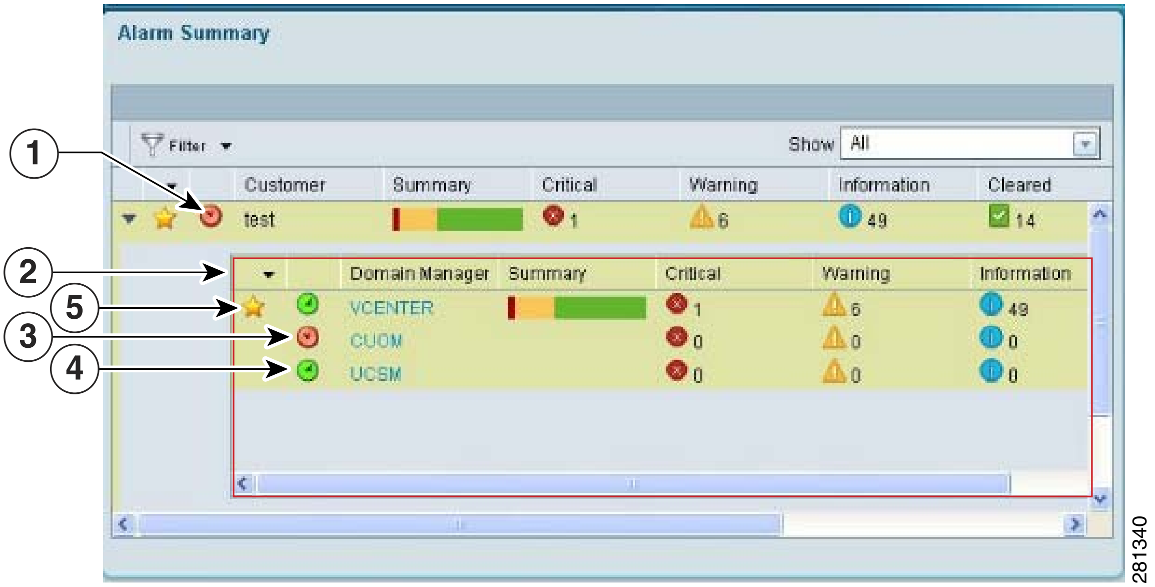
Color	Alarm Status
Red	Critical
Yellow	Warning
Blue	Informational
Green	Cleared

Understanding Domain Manager Specific Alarms

HCM Dashboard displays domain manager specific alarms for each customer in the Alarm Summary portlet. The table in the Alarm Summary portlet is a tree table and supports the display of hierarchical information.

See Figure 2-1 and Table 2-14.

Figure 2-1 Domain Manager Specific Alarms



Show: All

Customer	Summary	Critical	Warning	Information	Cleared
test		1	6	49	14

Domain Manager	Summary	Critical	Warning	Information
VCENTER		1	6	49
CUOM		0	0	0
UCSM		0	0	0

You must click the node (see number 1 in Figure 2-1 and Table 2-14) to expand and collapse the domain manager-specific alarms table. When the node is expanded, another table displays the domain manager specific alarms.

Table 2-14 Domain Manager Specific Alarms

Number	Description
1	Node—Allows you to expand and collapse the domain manager specific alarms table.
2	Domain Manager-specific alarms table.
3	Red Icon—If data is collected for the previous interval or if the data is invalid, a red icon is displayed.
4	Green Icon—If data is collected for the current time interval, a green icon is displayed.
5	Star—If the data has changed since the last poll.

The following list explains the domain manager-specific alarms table:

- UCSM—If you enter wrong UCSM credentials or if the UCSM server is down or if UCSM is unable to trace the MAC address for the VMs, the data collected for the previous interval and a red icon is displayed in the domain manager-specific alarms table.

- vCenter—If you enter wrong VM credentials or if the VM server is down or if no VMs are configured for the customer in vCenter, the data collected for the previous interval and a red icon is displayed in the domain manager-specific alarms table.
- CUOM, DCNM-LAN, DCNM-SAN—If you enter wrong credentials or if the server is down, the data collected for the previous interval and a red icon is displayed in the domain manager-specific alarms table. You can also view the alarms generated on CUOM, based on customers.

In the domain manager specific alarms table, click the domain manager to cross-launch the respective pages:

- UCSM—Launches a new window in HCM Service Assurance which displays a list of UCSM alarm and chassis details.
- vCenter—Cross-launches the vCenter Login page. After you enter the credentials in the login page, the vCenter Alarms page is displayed.
- CUOM—Cross-launches the CUOM Alarms and Events page.
- DCNM-SAN—Cross-launches the DCNM-SAN page.

Understanding Alarm Mapping

HCM Dashboard and the domain managers categorize the alarms differently. This section explains how HCM Dashboard alarms are mapped with the various domain managers. It includes the following topics:

- vCenter and HCM Service Assurance Alarm Mapping, page 2-31
- UCSM and HCM Service Assurance Alarm Mapping, page 2-32
- CUOM and HCM Service Assurance Alarm Mapping, page 2-32
- DCNM-LAN, DCNM-SAN and HCM Service Assurance Alarm Mapping, page 2-32

vCenter and HCM Service Assurance Alarm Mapping

Table 2-15 maps vCenter and HCM Dashboard alarms. RequireAck severity will be mapped to zero in HCM Service Assurance because HCM Service Assurance cannot fetch RequireAck alarms from vCenter.

Table 2-15 vCenter Alarm Mapping

vCenter Severity	HCM Service Assurance Severity
Gray—Unknown status	Information
Green—Entity is OK	Cleared
Red—Entity has a problem	Critical
Yellow—Entity might have a problem	Warning

UCSM and HCM Service Assurance Alarm Mapping

Table 2-16 maps UCSM and HCM Dashboard alarms. RequireAck severity will be mapped to zero in HCM Service Assurance because HCM Service Assurance cannot fetch RequireAck alarms from UCSM.

Table 2-16 UCSM and HCM Service Assurance Alarm Mapping

UCSM Severity	HCM Service Assurance Severity
Critical	Critical
Major	Critical
Warning	Warning
Minor	Warning
Info	Information
Cleared	Cleared

CUOM and HCM Service Assurance Alarm Mapping

Table 2-17 maps CUOM and HCM Dashboard alarms.

Table 2-17 CUOM and HCM Service Assurance Alarm Mapping

CUOM Severity	HCM Service Assurance Severity
Critical	Critical
Warning	Warning
Information	Information
Cleared	Cleared
RequireAck	RequireAck

DCNM-LAN, DCNM-SAN and HCM Service Assurance Alarm Mapping

Table 2-18 maps DCNM-LAN, DCNM-SAN and HCM Dashboard alarms.

Table 2-18 DCNM-LAN, DCNM-SAN and HCM Service Assurance Alarm Mapping

DCNM-LAN and DCNM-SAN Severity	HCM Service Assurance Severity
Critical	Emergency + Critical
Warning	Error + Alert + Warning
Information	Notice + Information + Debug

Table 2-18 DCNM-LAN, DCNM-SAN and HCM Service Assurance Alarm Mapping (continued)

DCNM-LAN and DCNM-SAN Severity	HCM Service Assurance Severity
Cleared	Default value 0, since this is not returned by the domain managers.
RequireAck	Default value 0, since this is not returned by the domain managers.

Phone Summary Portlet

To view the Phone Summary portlet, go to **Dashboard > Phone Summary.**

The Phone Summary portlet displays the number of configured phones, registered phones, and unregistered phones for each customer.

The Filter option is available in the portlet. See Understanding the Filtering Option in Portlets, page 2-1 for details about the Filter option.

When you select the Filter by Example option to filter data, search fields appear in all columns and you must enter alphabetical or numerical data in these fields.

The First column displays only graphical data. If you enter alphabetical or numerical data in the search field in the First column, no data will be displayed.

To understand the icons used in HCM Service Assurance, see Table 2-14.

Table 2-19 lists the filtering types and corresponding options available in the Phone Summary portlet.

Table 2-19 Filtering Types and Options

Filter Types	Options	
Filter by Example	Column Header Text Field	• Customer • Configured • Registered • Unregistered

Table 2-19 Filtering Types and Options (continued)

Filter Types	Options	
Advanced Filter	Filter Dropdown	• Customer • Configured • Registered • Unregistered
	Relational Operators	• Does not equal • Is exactly (or equals) • Is greater than • Is greater than or equal to • Is less than • Is less than or equal to
	Text Field	Enter the filtering parameters.

The Phone Summary portlet displays the following details for each customer:

- Customer—Name of the customer.
- Configured—Registered + Unregistered + Disconnected + Phones in Survivable Remote Site Telephony (SRST) mode.
- Registered—Number of registered phones for each customer.
- Unregistered—Number of unregistered phones. The Unregistered column in the Phone Summary table contains a red exclamatory mark, if the number of unregistered phones exceeds 10% of the configured phones.

Click the customer name to cross-launch the CUOM Phone Inventory page. When you add or delete a customer, the Phone Summary portlet information is updated to reflect the status.

Note The phone count displayed in the Phone Summary portlet and the phone count displayed in the CUOM Phone Inventory page that is cross-launched, might differ if there are Unknown phones in the network. For more information about Unknown Phones, see Unknown Phones, page 2-34.

Unknown Phones

Phones in the Unknown state are the phones that are not registered with the Cisco Unified Communications Manager (CallManager) in the last 24 hours. Unknown phones include:

- Phones that are configured, but not available in the network yet.
- Phones that were registered earlier, but are no longer available in the network.

Diagnostics

The Diagnostics tab lists the Diagnostics Test portlet. For details see Diagnostics Test, page 2-35

Diagnostics Test

To view the Diagnostics Test portlet, go to **Diagnostics > Diagnostics Test.**

You can use the Diagnostic Test portlet to initiate different tests to verify a given phone IP. The following options are available in the Diagnostics Test portlet:

- Customer—Allows you to select a customer from the drop-down list.
- Test—Allows you to select the type of test. The options are:
  - Basic, page 2-35
  - Advanced, page 2-37
- Phone No—Allows you to enter the phone number that has to be tested.
- Type—Allows you to select the type of Advanced test. The options are:
  - Synthetic, page 2-37
  - Node-to-Node (N-2-N), page 2-38

If you enter wrong CUOM credentials for the customer or if the CUOM server is down, the Diagnostics Test will timeout and an error message will be displayed. The default timeout value is four minutes. You can configure the timeout value in the portal.properties file available in the *HCM_Root_Directory*\thirdparty\jboss\server\default\deploy\ROOT.war\WEB-INF directory.

You must make sure that the time and time zone of the HCM Service Assurance server and the CUOM server are the same.

Phone Status Tests

Phone status testing uses Cisco IOS IP SLA technology to monitor the reachability of key phones in the network. A phone status test consists of the following:

- A list of IP phones to test, selected by you.
- A testing schedule that you configure.
- IPSLA-based pings from an IP SLA-capable device (for example, a switch, a router, or a voice router) to the IP phones. IPSLA-based pings can also be from CUOM to the IP phones.

Basic

To run a Basic test:

Step 1 Select a customer from the Customer drop-down list.

Step 2 Select the test as **Basic** from the Test drop-down list.

Step 3 Enter the phone number that has to be tested.

Step 4 Click ⇨.

The tests are run sequentially and the test results are displayed in the portlet in a tabular format.

After you start the Basic test, a spin indicator shows that the Basic test is in progress.

While the test is in progress:

- You cannot initiate another Basic test until the first test is complete.
- You will still be able to navigate to other tabs. However, if you return to the Basic test tab, the test stops. You must initiate a new test.
- You will be able to resize the Diagnostics Test portlet. However, the test stops and you must initiate a new test.

Table 2-20 lists the Basic tests and description.

Table 2-20 Basic Tests and Description

Test	Description
Call Hold	Takes control of two phones and performs the following: • Places a call from phone A to phone B. • Puts phone B call on hold. • Disconnects the call.
Call Forward	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Forwards the call to phone C from phone B. • Verifies that the call is received by phone C. • Disconnects the call.
Call Park	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Has phone B park the call. The call disappears from phone B and a message is displayed to inform you where the call is parked (for example, Call Park at 80503). • Has phone C dial the number where the call is parked. The parked call is transferred to the phone that you made the call from. • Disconnects the call.
Call Conference	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Places a conference call from phone A to phone C. • Disconnects the call.

Table 2-20 Basic Tests and Description (continued)

Test	Description
Call Transfer	Takes control of three phones and performs the following: • Places a call from phone A to phone B. • Has phone B transfer the call to phone C. • Has phone C accept the call. • Disconnects the call.
Call Test	Takes control of a phone and places a call to a given number. The call can be from a real phone to a number, in which case, the test controls only the caller. Alternatively, the call can be from one real phone to another, in which case the test controls both the caller and the receiver.

The Basic Test fails and an error message is displayed if you:

- Enter an invalid:
  - Phone number.
  - JTAPI username.
  - JTAPI password.
  - Nearest IP SLA Device IP.
- Did not enter the details in the mandatory fields.

Advanced

For advanced diagnostic tests such as synthetic tests and node-to-node (N-2-N) tests, the portlet cross-launches to the CUOM Diagnostics web page. You have to manually enter the parameters in the CUOM Diagnostics web page to run the test.

Synthetic

You can configure synthetic tests to be run on a periodic basis. You should manually enter the parameters in the CUOM Create Synthetic Test web page, to run the test. A synthetic test uses voice applications and analyzes the behavior of the system.

CUOM monitors the information returned from the synthetic test and generates events based on the results. Synthetic tests verify whether a voice application can service requests from a user. Synthetic tests are used to measure the availability of voice applications.

For example, you can use a synthetic test to verify whether phones can register with a Cisco Unified Communications Manager.

To create a synthetic test:

Step 1 Select a customer from the customer drop-down list.

Step 2 Select the test as **Advanced** from the Test drop-down list.

Step 3 Select **Synthetic** from the Type drop-down list.

Step 4 Click ⇨.

The Create Synthetic Test page is cross-launched.

Step 5 Select the **Test Type** in the Create Synthetic Test page.

Step 6 Enter the details in the Create Synthetic Test page.

Step 7 Click **Create**.

For more information, see *Creating Synthetic Tests* section of the *User Guide for Cisco Unified Operations Manager*.

Node-to-Node (N-2-N)

Node-to-node (N-2-N) tests monitor the response time and availability of multiple-protocol networks on both an end-to-end and hop-by-hop basis. You should manually enter the parameters in the CUOM Create Node-to-Node Test page to run the test.

After collecting the data, you can use the CUOM graphing function to examine changes in network performance metrics.

You can select, display, and chart network performance data in real time. You can also configure N-2-N tests to trigger events if certain thresholds are crossed. These events appear in the Monitoring Dashboard.

To create an N-2-N test:

Step 1 Select a customer from the Customer drop-down list.

Step 2 Select the test as **Advanced** from the Test drop-down list.

Step 3 Select **N-2-N** from the Type drop-down list.

Step 4 Click ⇨.

The Create Node-to-Node Test page is cross-launched.

Step 5 Select the **Test Type** in the Create Synthetic Test page.

Step 6 Enter the details in the Create Node-to-Node Test page.

Step 7 Click **OK**.

For more information, see *Creating a Single Node-To-Node Test* section of the *User Guide for Cisco Unified Operations Manager*.

APPENDIX A

Troubleshooting

This appendix offers troubleshooting steps to help solve problems while using HCM Service Assurance. This appendix includes the following troubleshooting information:

Overview

Troubleshooting involves:

1. Identifying the source of the problem—Which devices, links, interfaces, hosts, or applications have the problem?
2. Locating the problem on the network—On what VLAN, subnet, or segment is the problem occurring?
3. Comparing current network performance against an established baseline—Is the performance better or worse?
4. Finding out when the problem started—When did you first see the problem? Is it recurring?
5. Determining the extent of the problem—How widespread is the problem? Is it getting worse?

Troubleshooting HCM Service Assurance

You can use HCM Service Assurance server log files to troubleshoot your system. See Log Files, page A-7 for a list of server logs.

Frequently Asked Questions

The following are FAQs about HCM Service Assurance:

Q. Can I use the sort option in all columns in portlets?

A. No. You cannot use the sort option in all columns in portlets. You cannot sort the Customers and the Privilege columns in the User Administration portlet.

Note You can sort the User ID column in the User Administration portlet.

Q. Can I change the collection interval?

A. Yes. The default collection interval is five minutes for CUOM, UCSM, and vCenter. You can configure the collection interval in the Configuration portlet.

Q. What is the default refresh frequency for all portlets?

A. The default refresh frequency for all portlets is five minutes. You can configure the refresh frequency of a portlet in the Configuration portlet. For more information, see Configuring Portlet Refresh Frequency, page 2-19

The Refresh option is not available for the Diagnostics Test portlet.

Q. How long will HCM Service Assurance take to reflect the newly added customer details?

A. For the Alarm Summary and Phone Summary portlets, a new customer is reflected after the collection interval.

Q. What is the default timeout value for the diagnostics test execution?

A. The default timeout value for the diagnostics test is four minutes. It can be configured in the portal.properties file in the JBOSS_HOME\server\default\deploy\ROOT.war\WEB-INF directory.

You must restart the HCM server after you change the timeout value.

Q. How can I configure the session timeout value in HCM Service Assurance?

A. You can configure the session timeout value in the web.xml file. The default session timeout value is 60 minutes. For more information, see Configuring Session Timeout Value, page 1-7.

Q. Why is the UCSM blade failure alarm not shown in HCM Service Assurance?

A. UCSM blade failure alarm will not be shown in HCM Service Assurance if:

- VMware HA is enabled and the UCS blade on which the monitored VM resides, fails.
- VMware HA moves the VM to another UCS blade.

To resolve this problem:

1. Configure VMware HA alarm in vCenter.

   This alarm is generated when a VM is moved by VMware HA.

   HCM Service Assurance displays this alarm in vCenter alarms for the corresponding VM.

2. Check for UCSM alarms whenever VMware HA alarm is generated for a VM.

Q. Why is the red icon displayed in the Domain Manager Specific Alarms table, even after configuring UCSM for a customer with valid UCSM host IP address and credentials?

A. You must check whether vCenter is configured for the same customer. If vCenter is not configured, you must configure vCenter. For configuring vCenter, see Configuring vCenter, page 2-12.

Q. Why is Diagnostics Test not working, even after configuring CUOM correctly?

A. Check the IP address that you entered in the `WSN_CONSUMER_IPADDRESS` field in the monitor.properties file. If the IP address is wrong, edit the `WSN_CONSUMER_IPADDRESS` field and enter the correct IP address.

The monitor.properties file is available in the *HCM_Root_Directory*/thirdparty/jboss/server/default/conf/portal_props directory. You must clear the browser cache before logging into HCM Service Assurance.

Q. Sometimes there is a discrepancy between the count shown in HCM Service Assurance and the count shown in the corresponding domain manager page that is cross-launched. Why does this discrepancy exist?

A. HCM Service Assurance collects data based on the collection frequency. If the count changes after data collection, the updated count is reflected in HCM Service Assurance only during the next collection. The domain manager page, which is cross-launched, displays the most-current count.

Q. Sometimes the fault time indicator, time stamp and alarm count displayed in the Aggregated Data Center does match with the data dislayed in the details box. Why does this happen?

A. Fault count indicator, time stamp, and alarm count that is displayed in the Aggregated Data Center portlet pane do not reflect the updated data automatically after polling. The time stamp, fault count indicator, and alarm count that is displayed next to the IP address indicate the updated data, after polling. As a workaround, to sync up the alarm count, refresh manually or wait for an auto-refresh.

Q. Some devices that I added are missing from the Devices drop-down list in Edit/Delete Devices screen. Why does this happen?

A. The server time of HCM and CUOM are not synchronized. Run the Network Time Protocol (NTP) program on both CUOM and HCM.

Q. Why am I not able to add domain manager CUOM?

A. The super admin credentials that you specify for CUOM must always be admin/admin. If you specified different credentials, change them at the following path.

Go to *HCM_Install_Directory*/thirdparty/jboss/server/default/conf/portal_props/ and change values in the monitor.properties file. Specify the username against SUPER_ADMIN_USER and the password against SUPER_ADMIN_PASSWORD. Restart HCM server.

Error Messages

This section describes the HCM Service Assurance error messages and recommended solutions.

Error Message `Authentication failed, please try again.`

Recommended Action You have entered an invalid password in the HCM login page. Enter a valid password.

Error Message `Please enter a valid log-in.`

Recommended Action Check whether you entered a valid username in the HCM login page.

Error Message `Fields cannot be empty. Please enter details to continue.`

Recommended Action Enter details in the mandatory fields in the Add Customer dialog box. For more information, see Adding a Customer, page 2-6

Error Message `Please select the customer(s) required.`

Recommended Action Select a customer from the Available Customers list in the User Configuration dialog box when you create a user. For more information, see Adding a User, page 2-24

Error Message `Please select any one of the customer.`

Recommended Action Select a customer and then select the cross-launch option in the Customer Cross Launch portlet.

Error Message `Invalid URL!! Please enter a valid URL.`

Recommended Action Enter a valid URL in the Add dialog box. The URL must start with either http:// or https://. For more information, see Adding a URL, page 2-20.

Troubleshooting Customer Onboarding Error Messages

Validation Errors

The following errors appear during validation because of incorrect entries in the Customer Onboard spreadsheet. You can download a spreadsheet that contains a list of errors The name of file is prefixed with ‘errored’. The errors are listed in the Remarks column.

If you added devices to a particular customer in CUOM, and the operation was partially successful, delete manually all the devices that were added to CUOM. Correct the entries in the spreadsheet and thentry again.

Note Association between customer and user will be seen only after you move the added devices to Monitored/Partially Monitored state. If device addition fails, the mapping will not be shown.

Error Message `Please add <`*`Missing_Sheet name`*`> sheet(s) to proceed Customer on-boarding.`

Recommended Action Check whether all pre-defined sheets are present (CustomerInfo, DomainManagers, VCenterVMs, DeviceInfo, DeviceProtocolInfo). You must add the missing sheet in the main Customer Onboard spreadsheet. If the sheet is present, the name you specified for the sheet is incorrect. Correct the name of the worksheet.

Error Message `Invalid Domain Manager.`

Explanation Name of the domain manager specified is incorrect.

Recommended Action Change the name of the domain manager specified in the DomainManagers sheet to any pre-defined Domain Manager type specified in Table 2-3Customer On Boarding Spreadsheet, page 2-6.

Error Message `Duplicate Customer.`

Explanation The name of the customer has to be unique. You have duplicate entries for a certain customer in the CustomerInfo sheet.

Recommended Action Change one of the names to a unique name.

Error Message `Duplicate Customer DM combination.`

Explanation Duplication of a customer-domain manager combination. There can be only one instance of a particular combination of customer and a domain manager. A customer name can be associated with a domain manager only once.

Recommended Action Specify a unique customer-domain manager combination.

Error Message `Admin username or password is empty.`

Explanation Either the admin username or password is blank for a domain manager in DomainManagers sheet.

Recommended Action Provide the necessary data.

Error Message `Invalid Auth Type.`

Recommended Action Specify the device authentication type as either MD5 or SHA in DeviceInfo sheet.

Error Message `DeviceInfo not found for customer device combination.`

Explanation Details of device not found in the DeviceInfo sheet, but entry exists in the DeviceProtocolInfo sheet.

Recommended Action Specify details of the device in the DeviceInfo sheet.

Processing Errors

The following section explains the errors that occured during processing the request to add the data to the database. An error message appears and you can download a spreadsheet. The name of file is prefixed with '*errored*'. The errors are listed in the Remarks column.

Error Message `Error while adding Admin User in DomainManagers sheet.`

Explanation The admin user or operator user that you have entered against CUOM is already present in the database.

Recommended Action Add a different user.

Error Message `Exception will be shown in the respective sheet [CustomerInfo/DomainManagers].`

Explanation An exception occured while adding customer or domain manager to the database. This error may also occur if the database is down.

Recommended Action Bring the database up.

Error Message `Customer already exists for <`*`customer name`*`> in CustomerInfo sheet.`

Explanation Customer name already exists in database.

Recommended Action Specify a different customer name.

Error Message `Exception will be shown in the DomainManagers sheet and DeviceInfo sheet.`

Explanation For example, errors in DeviceInfo sheet:

```
RequestId[AddDevice_distinct IP Address],Reason[Device[IP Address] already exists
in the system.]

For example, errors in DomainManager sheet

Device addition failed for customer: customer_name

Following devices got error while adding to CUOM - <device_IP_address>
```

Recommended Action Add a device with unique IP address.

Error Message `Exception will be shown in the DomainManagers sheet and DeviceInfo sheet.`

```
Error in DomainManagers sheet:

Device addition failed for customer: customer_name

Following devices got error while adding to CUOM - <Device IP address>

Error in DeviceInfo sheet:

RequestId[AddDevice IP Address],Reason[The server has received more requests than
supported.]

WSDoAllReceiver: security processing failed.
```

Recommended Action Try again, later.

Error Message `Error while adding Admin User for Customer <`*`Error Message`*`>.`

Explanation The exact error message from CUOM will be appended with this error message. This exception appears when there is an error while adding admin user or operator user to CUOM .

Recommended Action See CUOM user documents for details.

Log Files

The log file logs details of all report generation requests and user authorization requests. This helps you to debug the application.

HCM Service Assurance maintains separate log files for UI, Schedulers, CUOM, synchronous and notification Web Services components. The log files are stored in JBOSS_HOME\server\default\log\msdtportal directory.

The following log files are available:

- msliferay.log—UI
- msscheduler.log—Scheduler
- mswsomclient.log—Web services OM logs
- mswsnotifyclient.log—Web services OM notification
- mswsvcclient.log—Web services vCenter logs
- mswsucsmclient.log—Web services UCSM logs
- msdcnmlanclient.log—Web services DCNM-LAN
- msdcnmsanclient.log—Web services DCNM-SAN

Note The default size of a log file is 10 MB. A separate log file is created when the first log file exceeds 10 MB. A maximum of two log files are maintained and older log files are recycled.

Configuration Files

The configuration file allows you to configure properties in HCM Service Assurance. HCM Service Assurance maintains separate configuration files for CUOM, UCSM, vCenter, Schedulers, ACS, cross-launch and portal properties.

Note You must restart the HCM server after you modify the values in the configuration file.

The following configuration files are available in *HCM_Install_Directory*\thirdparty\jboss\server\default\conf\portal_props directory:

- monitor.properties—CUOM Web services configuration
- ucsm.properties—UCSM Web services configuration
- vcenter.properties—vCenter Web services configuration
- msscheduler-config.xml—Thread and polling configuration
- dcnmsan.properties—DCNM-SAN web services configuration
- dcnmlan.properties—DCNM-LAN web services configuration

The following configuration files are available in *HCM_Install_Directory*\jboss\server\default\deploy\ROOT.war\WEB-INF directory:

- acs.properties—ACS configuration
- crosslaunch.properties—Cross-launch port and protocol configuration
- portal.properties—Diagnostics timeout configuration
- dcnmsan.properties—DCNM-SAN web services configuration
- dcnmlan.properties—DCNM-LAN web services configuration

GLOSSARY

A

ACL	access control list
ACS	Access Control Server
API	application program interface
AS	application server
ASCII	American Standard Code for Information Interchange

C

Cisco IOS	Cisco Internetwork Operating System
CLI	command-line interface
CPU	central processing unit
CUOM	Cisco Unified Operations Manager

G

GUI	graphical user interface

H

HCM	Hosted Collaboration Mediation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

I

IP	Internet Protocol
IP SLA	IP Service Level Agreement

J

JTAPI	Java Telephony API

L

LAN	local area network

M

MAC	Media Access Control
MSP	Managed Service Provider

N

N-2-N	none-to-node
NAT	Network Address Translation
NBI	Northbound Interface
NE	network element
NMS	network management system
NOC	Network Operations Center

O

OS	1. operating system 2. operations system

P

PDU	protocol data unit
PSTN	public switched telephone network

Q

QoS	quality of service

R

RAM	random-access memory
RIP	Routing Information Protocol

S

SLV	Service Level View
SID	Shared Information/Data Model
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

T

TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

U

UCSM	Unified Computing System Manager
UI	user interface
URL	Uniform Resource Locator

V

VLAN	virtual local area network
VoIP	Voice over IP

W

WAN	wide area network
WAP	Wireless Application Protocol

X

XML	Extensible Markup Language

INDEX