CISCO

Administration Guide for Cisco Unity Connection Serviceability Release 12.x

CONTENTS

CHAPTER 1

Introduction to Cisco Unity Connection Serviceability

Introduction to Cisco Unity Connection Serviceability

Understanding Cisco Unity Connection Serviceability

Cisco Unity Connection Serviceability, a web-based troubleshooting tool for Unity Connection, provides the following functionality:

- Displaying Unity Connection alarm definitions that you can use for troubleshooting.

- Enabling Unity Connection traces. You can collect and view trace information in the Real-Time Monitoring Tool (RTMT).

- Configuring the logs to which Unity Connection trace information is saved.

- Managing a cluster and the servers, if a Unity Connection cluster is configured.

> **Note** The Unity Connection cluster feature is not supported for use with Cisco Business Edition.

- Viewing the status of the Unity Connection feature services.

- Activating, deactivating, starting, and stopping the Unity Connection services.

- Generating reports that can be viewed in different file formats.

Depending on the service and component involved, you may perform serviceability-related tasks in both Cisco Unity Connection Serviceability and Cisco Unified Serviceability. For example, you may need to start and stop services, view alarms, and configure traces in both applications to troubleshoot a problem.

Cisco Unity Connection Serviceability supports the functionality that is described in the Administration Guide for Cisco Unity Connection Serviceability. For information on using Cisco Unified Serviceability, see the

Cisco Unified Serviceability Administration Guide, Release 12.x, available at
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Browsers on Administrator Workstations

To access Cisco Unity Connection Serviceability, Cisco Unity Connection Administration, Cisco Unified Serviceability, Disaster Recovery System, and other web applications on the Unity Connection or Cisco Business Edition server, the browser(s) must be set up correctly on an administrator workstation.

Firefox

Do the following tasks to set up Firefox for accessing the Unity Connection web applications.

Step 1 Confirm that the software required for correct browser configuration is installed. See the "Software Requirements-Administrator Workstations" section of the System Requirements for Cisco Unity Connection *Release 12.x*, available at
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.

Step 2 Configure Firefox:

Enable Java.

Enable Java Script > Enable Change Images in Java Script Advanced.

Allow sites to set cookies. (For security purposes, we recommend that you set this to Allow Sites to Set Cookies for the Originating Website Only.)

Microsoft Internet Explorer

Do the following tasks to set up Internet Explorer for accessing the Unity Connection web applications.

Step 1 Confirm that the software required for correct browser configuration is installed. See the "Software Requirements-Administrator Workstations""Software Requirements—Administrator Workstations" section of the System Requirements for Cisco Unity Connection *Release 12.x*, available at
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.

Step 2 Configure Internet Explorer:

Enable Active scripting.

Download and run ActiveX controls.

Enable Java scripting.

Accept all cookies.

Automatically check for newer versions of temporary Internet files.

Enable Medium-High privacy.

Introduction to Cisco Unity Connection Serviceability

Adding the Unity Connection or Cisco Business Edition Server to the List of Trusted Sites (Windows Server 2003 with Internet Explorer 6.0 Only)

If you are running Microsoft Windows Server 2003 and using Internet Explorer version 6.0 to access the Cisco Personal Communications Assistant, add the Unity Connection server to the Trusted Sites list by doing the following procedure

Adding the Unity Connection or Cisco Business Edition Server to the List of Trusted Sites (Windows Server 2003 with Internet Explorer 6.0 Only)

Step 1 Open the Cisco Personal Communications Assistant Sign-In page.

Step 2 On the Internet Explorer File menu, select **Add This Site To** > **Trusted Sites Zone**.

Step 3 In the Trusted Sites dialog box, select **Add**.

Step 4 Select **Close** to close the Trusted Sites dialog box.

Step 5 Restart Internet Explorer.

Accessing Cisco Unity Connection Serviceability

The first time that you sign in to Cisco Unity Connection Serviceability, you use the username and password for the default administrator account that the installer specified for the account during installation. Later, you can use the username and password for any additional administrator accounts that you create.

Step 1 Using a supported web browser, open a browser session.

Step 2 Go to **https://<Cisco Unity Connection server IP address** > **/cuservice**.

Step 3 Enter an applicable username and password, and select **Login**.

After you have logged on to Cisco Unity Connection Serviceability, you can access all applications that appear in the Navigation drop-down box except for Cisco Unified Operating System Administration and Disaster Recovery System without having to sign in to each application.

You cannot access Cisco Unified Operating System Administration or Disaster Recovery System using the Cisco Unity Connection Serviceability username and password. To access these applications from Cisco Unity Connection Serviceability, you must select the Logout link in the upper-right corner of Cisco Unity Connection Serviceability, then select the application from the Navigation drop-down box and select Go.

If you have already logged on to one of the applications that display in the Navigation drop-down box (not Cisco Unified Operating System Administration or Disaster Recovery System), you can access Cisco Unity Connection Serviceability without logging in. From the Navigation drop-down box, select Cisco Unity Connection Serviceability and select Go.

Using Cisco Unity Connection Serviceability Interface

In addition to troubleshooting, generating reports, and doing service-related tasks in Cisco Unity Connection Serviceability, you can do the following tasks:

• To display documentation for a single window, select Help > This Page.

- To display a list of documents that are available with this release of Unity Connection or Cisco Business Edition (or to access the Help index), select Help > Contents.

- To verify the version of Cisco Unity Connection Serviceability running on the server, select Help > About or select the About link in the upper-right corner of the window.

- To go directly to the home page in Cisco Unity Connection Serviceability from a configuration window, select Cisco Unity Connection Serviceability from the Navigation drop-down box.

- To access Cisco Unity Connection Administration or other applications, select the applicable application from the Navigation drop-down box and select Go.

- To sign out of Cisco Unity Connection Serviceability, select the Logout link in the upper-right corner of the window.

- On each Cisco Unity Connection Serviceability configuration page, configuration icons appear that correspond to the configuration buttons at the bottom of the page. (For example, you can select either the Save icon or the Save button to complete the task.)

Using Alarms

Understanding Alarms

Cisco Unity Connection Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with the system. For example, you can use alarms to determine whether there are any ports enabled to set MWIs. Alarm information includes the catalog, name, severity, explanation, recommended action, routing list, and parameters.

You can enable or disable alarms to appear as syslog messages on the local server or on a remote server that you specify. You can also set the severity level that you want to appear.

You use the trace and log central option in the Real-Time Monitoring Tool (RTMT) to collect alarms. You use the SysLog Viewer in RTMT to view alarms.

Alarm Definitions

Alarm definitions describe alarm messages—what they mean and how to recover from them.

You search the Alarm Message Definitions page for alarm information. When you select an alarm, a description of the alarm information and a recommended action appears on the Alarm Information page. To help with troubleshooting, the definitions include the alarm name, description, severity, explanation, recommended action, routing list, and parameters.

Viewing Alarm Definitions

You can search for and view alarm definitions in *Alarm Message Definitions for Cisco Unity Connection Release 12.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/alarm_messages/12cucalrmmsgdef.html.

Alarm Configurations

This section describes how to enable and disable alarms.

Enabling Alarm

Step 1   In Cisco Unity Connection Serviceability, select **Alarm** > **Configurations**.

Step 2   In the Alarm Configurations window:

> • To enable the system to log the alarms in the application logs area in the SysLog Viewer, under Local Syslogs, check the **Enable Alarm** check box.

Step 3   Under the syslog for which you have enabled alarms, in the Alarm Event Level field, select the severity level that you want.

Step 4   Select **Save**.

Disabling Alarms

Step 1   In Cisco Unity Connection Serviceability, select **Alarm** > **Configurations**.

Step 2   In the Alarm Configurations window, uncheck the applicable **Enable Alarm** check box.

Step 3   Select **Save**.

CHAPTER 3

Using Traces

Using Traces

Understanding Traces

Cisco Unity Connection Serviceability traces help troubleshoot problems in the following ways:

- You can specify the log file parameters for each Unity Connection component, including the maximum number of log files and the maximum file size that can be created when you run traces for a component.

- You can enable micro traces and the level of micro-trace information that you want.

- You can enable macro traces (preselected groups of micro traces) and the level of macro-trace information that you want.

After you have configured the log files and enabled the traces, you collect trace log files in one of the following ways:

- Using the trace and log central option in the Real-Time Monitoring Tool (RTMT). For information, see the "Working with Trace and Log Central" chapter (in the "Tools for Traces, Logs, and Plug-Ins" part) of the Cisco Unified Real-Time Monitoring Tool Administration Guide at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

- Using the command line interface (CLI). For information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Note Enabling macro or micro traces decreases system performance. Enable traces only for troubleshooting purposes.

Configuring Trace Log Files

> **Note** Before trace information can be written to the log files, you must enable micro traces or macro traces that provide the troubleshooting information in the areas that you select.

1. In Cisco Unity Connection Serviceability, select **Trace** > **Configuration**. The Trace Configuration page appears.

2. In the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

3. From the Component drop-down box, select the component for which you want to configure trace log files, and select **Go**.

   The drop-down box displays all components (active and inactive).

4. In the Maximum No. of Files field, enter the maximum number of trace log files that is created for this component.

5. In the Maximum File Size field, enter the size limit (in megabytes) for the trace log files that is created for this component.

6. If you want to return to the default settlings, select **Set Default**. Otherwise, skip to the next step.

7. Select **Save**.

8. If you want the new trace log files to replace the old trace log files for this component, select **Restart Log Files**.

Enabling Micro Traces

Enable micro traces when you are troubleshooting problems with specific Cisco Unity Connection components. For example, if the Alert Central tool in Real-Time Monitoring Tool (RTMT) has notification errors, enable the Notifier trace. However, keep in mind that running traces can affect system performance and hard-disk space.

> **Note** Enabling micro traces decreases system performance. Enable traces only for troubleshooting purposes.

Step 1 In Cisco Unity Connection Serviceability, select **Trace** > **Micro Traces**.

The Micro Traces page appears.

Step 2 In the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3 From the Micro Trace drop-down box, select the micro trace that you want to enable, and select **Go**.

Step 4 Under Micro-Trace Levels, check the check boxes for the micro-trace levels that you want to enable.

Step 5 Select **Save**.

Tip   You may need to enable traces in Cisco Unity Connection Serviceability and Cisco Unified Serviceability to troubleshoot Unity Connection issues. To troubleshoot Unity Connection components, enable traces in Cisco Unity Connection Serviceability. Similarly, to troubleshoot services that are supported in Cisco Unified Serviceability, enable traces in Cisco Unified Serviceability. For information on how to enable traces in Cisco Unified Serviceability, see the Cisco Unified Serviceability Administration Guide at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Available Micro Traces

The Table 1: Micro Traces lists each micro trace that is available, a description of what it analyzes, and the filename of the trace log that it generates.

Table 1: Micro Traces

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
Arbiter	Conversations, ports, and call routing rules that are used for calls	diag_CuCsMgr_*.uc
AudioStore	The audio recording service used by web-based applications that use Media Player to playback or record audio streams	diag_Tomcat_*.uc
AxlAccess	Interaction with the AXL server to get and set phone-related properties	diag_Tomcat_*.uc
BulkAdministrationTool	Bulk Administration Tool that is used for creating, updating, and deleting multiple users or system contacts	diag_Tomcat_*.uc
CCL	The retrieval of meeting information for the calendaring feature	diag_CuCsMgr_*.uc diag_CuGalSvc_*.uc diag_Tomcat_*.uc
CDE	Conversation engine and conversation events	diag_CuCsMgr_*.uc
CDL	Information retrieval from the database	diag_CuCsMgr_*.uc diag_Tomcat_*.uc
CiscoPCA	The Cisco Personal Communications Assistant (Cisco PCA)	diag_Tomcat_*.uc

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
CML	The retrieval of messages from the Cisco Unity Connection message store; the retrieval of messages from an Exchange server (using IMAP) for using Text-to-Speech feature to read email messages	diag_CuCsMgr_*.uc diag_CuNotifier_*.uc diag_Tomcat_*.uc
Common	Low-level activities for components that are shared by Cisco Unity Connection services	<any>
ConfigData	Detection that configuration data has been updated in the database	<any>
ConvRoutingRules	The conversation to which the Arbiter routes calls	diag_CuCsMgr_*.uc
ConvSub	User activities and usage	diag_CuCsMgr_*.uc
CsEws	Exchange Web Services calls from Unity Connection to Exchange for single inbox, calendaring, and text-to-speech	diag_CuCsMgr_*.uc diag_CuMbxSync_*.uc
CsExchangeMbxLocator	Autodiscovery of Exchange mailboxes for single inbox, calendaring, and text-to-speech	diag_CuCsMgr_*.uc diag_CuMbxSync_*.uc
CsMalUmss	Access to the message store by the CML, Notifier, and IMAP server	diag_CuCsMgr_*.uc diag_Tomcat_*.uc
CsMbxSync	Single inbox synchronization	diag_CuMbxSync_*.uc
CsWebDav	Calendar activities in connection with Exchange	diag_CuCsMgr_*.uc diag_CuGalSvc_*.uc diag_Tomcat_*.uc
Cuals	The activities of the web services to add users	diag_Tomcat_*.uc
Cuca	The activities of Cisco Unity Connection Administration	diag_Tomcat_*.uc
CuCESync	Activity related with Survival Remote Site Voicemail (SRSV) processing.	diag_CUCESync_*.uc
CuCcmSynchronizationTasks	Synchronization of the user data from Cisco Unified CM	diag_Tomcat_*.uc

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
CuCmDbEventListener	Detection of changes in the Cisco Unified CM database	diag_CuCmDbEventListener_*.uc
CuCsMgr	Main Cisco Unity Connection process; starting and stopping Unity Connection	diag_CuCsMgr_*.uc
CuDbProxy	Database replication for Cisco Unity Connection clusters	diag_CuDbProxy_*.uc
CuEncrypt	Encryption (except for messaging) and the encryption audit logs	<any>
CuESD	The activities of Unity Connection external service diagnostic tools	diag_Tomcat_*.uc
CuFileSync	File replication for Unity Connection clusters	diag_CuFileSync_*.uc
CuGal	The retrieval of calendar and contact information from Exchange	diag_CuGalSvc_*.uc
CuImapSvr	Access to voice messages by IMAP clients	diag_CuImapSvr_*.uc
CuReplicator	Replication for digital networking **Note** We recommend that the Debug Traces and Debug Statistics micro-trace levels be enabled for no more than one hour because they can produce a large number of log entries.	diag_CuReplicator_*.uc
CuService	The activities of Cisco Unity Connection Serviceability	diag_Tomcat_*.uc
CuSlmSvr	The activities of Cisco Smart Software Licensing Services in Cisco Unity Connection	diag_CuSlmSvr_*.uc
CuSnmpAgt	The activities of the Connection SNMP subagent	diag_CuSnmpAgt_*.uc
DataSysAgentTasks	Data SysAgent tasks	diag_CuSysAgent_*.uc
DbEvent	Component notification of database changes	<any>

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
DPAPI	The activities of the diagnostic portal application programming interface web service	diag_Tomcat_*.uc
EWSNotify	Exchange EWS mailbox synchronization notifications	<date in the format yyyy_mm_dd>.stderrout.log.*
FailureConv	Activation of the Failure Conversation when a system error occurs	diag_CuCsMgr_*.uc
Feeder	In Intersite Networking, this micro trace checks the local site change-tracking database for directory changes and responds to poll requests from the remote site gateway Reader task In HTTPS Networking, this micro trace checks the change-tracking database of local subtree in Feeder for directory changes and responds to poll requests from the remote location Reader task.	diag_Tomcat_*.uc
FeedReader	In Intersite Networking, this microtrace periodically polls the remote site gateway for any directory changes since the last poll interval. In HTTPS Networking, this microtrace periodically polls the remote location for any directory changes since the last poll interval.	diag_Tomcat_*.uc
LicenseClient	Functions related to license management	diag_CuCsMgr_*.uc
Logger	Writing traces logs and events	<any>
MessageEventService	Detection of arrival or deletion of messages	diag_Tomcat_*.uc
MiuAdm	Functions in Cisco Unity Connection Administration relating to testing voice messaging ports and generating certificates	diag_Tomcat_*.uc
MiuCall	The process between the Miu and conversations	diag_CuCsMgr_*.uc

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
MiuDatatbase	Media activities relating to accessing the database	diag_CuCsMgr_*.uc
MiuGeneral	Tracking calls through the phone user interface (TUI); call control functions; turning message waiting indicators (MWIs) on and off; notification and outdial functions; basic media or WAV file usage	diag_CuCsMgr_*.uc
MiuIO	Media or WAV file usage with TAPI (circuit-switched or Cisco Unified CallManager) integrations	diag_CuCsMgr_*.uc
MiuMethods	Handing of incoming calls; call control; turning messaging waiting indicators (MWIs) on and off; notification and outdial functions; media or WAV file usage	diag_CuCsMgr_*.uc
MiuSIP	SIP call control	diag_CuCsMgr_*.uc
MiuSIPStack	Low-level SIP interactions for call control	diag_CuCsMgr_*.uc
MiuSkinny	SCCP call control	diag_CuCsMgr_*.uc
MiuTranscode	Low-level media functions relating to transcoding	diag_CuCsMgr_*.uc
Mixer	Low-level activities relating to media and the Text-to-Speech feature	diag_CuMixer_*.uc
Monitor	Monitoring the status of voice messaging ports and call processing during a call; the server-side functions for displaying port status in Real-Time Monitoring Tool	diag_CuCsMgr_*.uc
MTA	Delivery of voice messages to the message store	diag_MTA_*.uc
Notifier	Notification of messages and selected events; turning message waiting indicators (MWIs) on and off	diag_CuCsMgr_*.uc diag_CuNotifier_*.uc
PCAMeetingPlace	Activities of the Cisco Personal Communications Assistant relating to MeetingPlace for the calendar feature	diag_Tomcat_*.u

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
PCAUnifiedCM	Activities of the Cisco Personal Communications Assistant relating to the Cisco Unified Communications Manager integration	diag_Tomcat_*.uc
PhoneManager	The management of IP phone applications	diag_CuCsMgr_*.uc
PhraseServer	The prompts that play and the user DTMF input; the logs are written to a file	diag_CuCsMgr_*.uc
PhraseServerToMonitor	The prompts that play and the user DTMF input; the logs are written to the monitor	diag_CuCsMgr_*.uc
ReportDataHarvester	Conversion of the content in the data log files to entries in the reports database	diag_CuReportDataHarvester_*.uc
ResourceLoader	Using the selected language in the GUI; filling strings with product or message information	<any>
ResourceManager	Monitoring and providing available resources to the Arbiter as needed	diag_CuCsMgr_*.uc
RoutingRules	Call routing decisions	diag_CuCsMgr_*.uc
RSS	RSS feeds that are used for checking voicemail from an RSS client	diag_Tomcat_*.uc
RulesEngine	Evaluation of personal call transfer rules for a user during a call	diag_CuCsMgr_*.uc diag_Tomcat_*.uc
SMTP	SMTP functions	diag_SMTP_*.uc
SocketPoolHelper	Socket connections to the IMAP server	<any>
SRM	Functions related to cluster management	diag_CuSrm_*.uc
SslInit	Initialization procedures for components that use OpenSSL	<any>
SttClient	Detects messages that need to be transcribed; attaches completed transcriptions to original messages	diag_MTA_*.uc

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
SttService	Communication between Cisco Unity Connection and the third-party external transcription service	diag_SttService_*.uc
SysAgent	System Agent component, which schedules system tasks that the administrator enters (such as resynchronizing MWIs)	diag_CuSysAgent_*.uc
TaskRequest	Functions related to the Task Management tool	diag_CuSysAgent_*.uc
TextToSpeech	The activities of the Text to Speech feature	diag_CuCsMgr_*.uc
ThreadPool	The use of threads by the processor	<any>
TimerHelper	The timer used by the Conversation Manager component	<any>
TranscodeWeb	The web server audio format transcoding utilities that transcode the incoming audio streams into the audio format that Cisco Unity Connection uses	diag_Tomcat_*.uc
TRaP	Phone Record and Playback (TRaP), which lets clients use the phone as a recording and playback device	diag_CuCsMgr_*.uc diag_Tomcat_*.uc
UmssSysAgentTasks	Messaging tasks for the System Agent component	diag_CuSysAgent_*.uc
UnityAssistant	The activities of the Messaging Assistant web tool in the Cisco Personal Communications Assistant	diag_Tomcat_*.uc
UnityInbox	The activities of the Messaging Inbox web tool in the Cisco Personal Communications Assistant	diag_Tomcat_*.uc
UnityPCTR	The activities of the Cisco Unity Connection Personal Call Transfer Rules web tool in the Cisco Personal Communications Assistant	diag_CuCsMgr_*.uc

Micro Trace Name	What the Trace Analyzes	Filename of Trace Log
Video	The activities of Video call between Unity Connection and Cisco MediaSense through APIs.	diag_CuCsMgr_*.uc
VirtualQueue	Call queuing	diag_CuCsMgr_*.uc
VMREST	Interactions with Representational State Transfer (REST) API clients	diag_Tomcat_*.uc
VMWS	Interactions with voice messaging web services	diag_Tomcat_*.uc
VUI	The voice user interface	diag_CuCsMgr_*.uc

Enabling Macro Traces

Enable macro traces, which are preselected sets of micro traces, when you are troubleshooting general areas of Unity Connection functionality. For example, if there are MWI problems, enable the Traces for MWI Problems macro trace. However, keep in mind that running traces can affect system performance and hard-disk space.

⚠️

Caution   Enabling macro traces decreases system performance. Enable traces only for troubleshooting purposes.

Step 1   In Cisco Unity Connection Serviceability, select **Trace** > **Macro Traces**.

The Macro Traces page appears.

Step 2   In the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3   Check the check box of the macro trace that you want to enable.

Step 4   Expand the macro trace, and check the check boxes for the levels that you want to enable.

Step 5   Select **Save**.

Tip   You may need to enable traces in Cisco Unity Connection Serviceability and Cisco Unified Serviceability to troubleshoot Unity Connection issues. To troubleshoot Unity Connection components, enable traces in Cisco Unity Connection Serviceability. Similarly, to troubleshoot services that are supported in Cisco Unified Serviceability, enable traces in Cisco Unified Serviceability. For information on how to enable traces in Cisco Unified Serviceability, see the Cisco Unified Serviceability Administration Guide at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Available Macro Traces

Table 2: Macro Traces lists each macro trace that is available, a description of what it analyzes, and the filename of the trace log that it generates.

Table 2: Macro Traces

Macro Trace Name	What the Trace Analyzes	Filename of Trace Log
Call Flow Diagnostics	The flow of a call through Unity Connection	diag_CuCsMgr_*.uc
Message Tracking Traces	Message handing; the objects that handle messages from delivery to deletion	diag_CuSysAgent_*.uc diag_MTA_*.uc diag_CuCsMgr_*.uc diag_CuImapSvr_*.uc diag_Tomcat_*.uc
Call Control (Miu) Traces	Call control functions	diag_CuCsMgr_*.uc
Traces for MWI Problems	Turning message waiting indicators (MWIs) on and off	diag_CuCsMgr_*.uc diag_CuNotifier_*.uc
Traces for Other Notification Problems	Notification and outdial functions	diag_CuCsMgr_*.uc diag_CuNotifier_*.uc
Unity Startup	Unity Connection startup functions	diag_CuCsMgr_*.uc diag_CuNotifier_*.uc
Conversation Traces	Conversation usage	diag_CuCsMgr_*.uc
Voice User Interface/Speech Recognition Traces	Voice user interface (VUI)	diag_CuCsMgr_*.uc
Media (Wave) Traces	Media and WAV file usage	diag_CuCsMgr_*.uc diag_CuMixer_*.uc
Text to Speech (TTS) Traces	The Text to Speech (TTS) feature; also can log traces on other Cisco Unity Connection components that interact with TTS	diag_CuCsMgr_*.uc
Unity Connection Serviceability Web Service	The activity of Cisco Unified Serviceability	diag_Tomcat_*.uc
ViewMail for Outlook	The activity of Cisco Unity Connection ViewMail for Microsoft Outlook clients	diag_CuCsMgr_*.uc diag_CuImapSvr_*.uc diag_MTA_*.uc diag_Tomcat_*.uc
Digital Networking	Digital networking functions	diag_CuReplicator_*.uc

Macro Trace Name	What the Trace Analyzes	Filename of Trace Log
Single Inbox	Single inbox message synchronization	<date in the format yyyy_mm_dd>.stderrout. log.* diag_CuMbxSync_*.uc

Managing Server Status and Ports in a Cisco Unity Connection Cluster

Managing Server Status and Ports in a Cisco Unity Connection Cluster

The Cluster Management page in Cisco Unity Connection Serviceability lets you change the status of servers in a Unity Connection cluster, stop all ports on a server from taking new calls, and restart all ports on a server to take calls.

For the applicable procedures, see the "Configuring Cisco Unity Connection Cluster" chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 12.x*, available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html.

Note The Unity Connection cluster feature is not supported for use with Cisco Business Edition.

Managing Cisco Unity Connection Services

Cisco Unity Connection Services

Cisco Unity Connection has the services described in Table 3: Unity Connection Services.

Table 3: Unity Connection Services

Service	Description
Status Only Services	
Connection DB	This service enables the Unity Connection database and can be deactivated only using the command-line interface (CLI).
Connection Server Role Manager	This service enables the server status when a Unity Connection cluster is configured and can be deactivated only using the command-line interface (CLI).
Connection Serviceability	This service enables the Cisco Unity Connection Serviceability Administration interface and can be deactivated only using the command-line interface (CLI).
Critical Services	
Connection Conversation Manager	This service enables Unity Connection to handle calls. Disabling this service degrades the ability of Unity Connection to function.
Connection Mailbox Sync	This service synchronizes messages between Unity Connection and Exchange.

Service	Description
Connection Message Transfer Agent	This service enables the delivery of messages to the message store. Disabling this service degrades the ability of Unity Connection to function.
Connection Mixer	This service enables the audio (media stream) for calls, recorded messages, and Text-to-Speech (TTS). Disabling this service degrades the ability of Unity Connection to function.
Connection Notifier	This service enables notification of messages, such as turning message waiting indicators (MWIs) on and off. Disabling this service degrades the ability of Unity Connection to function.
Connection Smart License Manager Server	This service manages all the Cisco Smart Software Licensing operations on Cisco Unity Connection.
Base Services	
Connection Administration	This service enables Cisco Unity Connection Administration and the settings that are saved in the interface.
Connection DB Event Publisher	This service enables notifying Unity Connection components of changes to the Unity Connection database.
Connection SNMP Agent	This service enables the Simple Network Management Protocol (SNMP) that uses the Cisco-Unity-MIB. For more information on SNMP, see the "Simple Network Management Protocol" chapter of the *Cisco Unified Serviceability Administration Guide* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/serviceadministration/guide/cucm_service_admin.html
Optional Services	
Connection Access Layer	This service enables the sharing of user data between Unity Connection and other servers using Cisco Unity Access Layer (CUAL), a HTTP/SOAP web service. For example, this service can be used by Cisco Business Edition or by Digital Networking with Cisco Unity.
Connection Branch Sync Service	This service enables Survivable Remote Site Voicemail (SRSV) feature.
Connection CM Database Event Listener	This service enables the detection of changes in the Cisco Unified Communications Manager database.

Service	Description
Connection Database Proxy	This service allows tools that are not installed on the Unity Connection server (COBRAS, User Data Dump, Distribution List Builder, and so on) to gain direct access to the Unity Connection database via ODBC from a Windows client on the network.
	The service is disabled by default. To use any of these tools, you must enable the service, configure the time out for the service, and create a user that has the remote admin role. For more information, see the help file for the applicable tool.
Connection Diagnostic Portal Service	This service enables access to data on Unity Connection by the Diagnostic Portal in the Real-Time Monitoring Tool (RTMT).
Connection Digital Networking Replication Agent	This service enables the replication of data between Unity Connection servers for Digital Networking.
Connection Directory Feeder	For Intersite Networking, this service checks the local site change-tracking database for directory changes and responds to poll requests from the remote site gateway Reader task.
Connection File Syncer	This service enables the replication of files for Unity Connection clusters.
Connection Groupware Caching Service	This service enables Unity Connection to cache calendar data (from Exchange, MeetingPlace, or MeetingPlace Express servers) and to cache Exchange contacts.
Connection HTTPS Directory Feeder	This service checks the change-tracking database of its own and the associated local subtree locations for directory changes and responds to poll requests from the remote location Reader task.
Connection IMAP Server	This service enables access to data on Unity Connection by IMAP clients.
Connection Inbox RSS Feed	This service enables RSS feeds for checking voicemail from RSS clients.
Connection Integrated Mailbox Configuration	This service enables sharing of user data between Unity Connection and Cisco Unified Communications Manager.
Connection Jetty	This service enables Java web clients.
Connection Message Event Service	This service enables access to voice message data on Unity Connection by Cisco Unified Mobility Advantage.

Service	Description
Connection Personal Communication Assistant	This service enables access to data on Unity Connection by the Cisco Personal Communications Assistant (Cisco PCA).
Connection Realtime Monitoring APIs	This service enables access to data on Unity Connection by Real-Time Monitoring Tool (RTMT).
Connection Reports Data Harvester	This service enables conversion of data in log files to entries in the reports database, which is used to generate reports.
Connection REST Service	This service enables Representational State Transfer (REST) API clients.
Connection SMTP Server	This service enables access to data on Unity Connection by an SMTP server.
Connection SpeechView	This service enables the SpeechView feature and communicates with the third-party external transcription service.
Connection System Agent	This service enables schedules system tasks (such as re-synchronizing MWIs) that the administrator can enter in Cisco Unity Connection Administration.
Connection Voicemail Web Service	This service enables access to data on Unity Connection through Voicemail Web Service (VMWS) by Cisco Unified Communications Widgets such as Visual Voicemail.
Connection Voice Recognition Transport	This service enables generation and placement of dynamic grammars that are used by the speech-recognition engine for the voice user interface (VUI).
Connection Voice Recognizer	This service is the speech-recognition engine that enables voice recognition for the voice user interface (VUI).

Managing Services in Control Center

Control Center in Cisco Unity Connection Serviceability lets you do the following tasks:

- Activate and deactivate Unity Connection services in the Optional Services section.

- Start and stop all Unity Connection services except the services in the Status Only Services section.
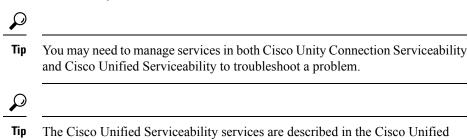
Stopping Unity Connection services in the Critical Services section may cause calls in progress to be dropped and degrades the normal function of the Unity Connection or Cisco Business Edition server.

When a Cisco Unity Connection cluster is configured, stopping a service in the Critical Services section for the server with Primary status causes the status for the servers in the cluster to change.

• View the status the status of Unity Connection services.

• Refresh the status of Unity Connection services.

Tip   You may need to manage services in both Cisco Unity Connection Serviceability and Cisco Unified Serviceability to troubleshoot a problem.

Tip   The Cisco Unified Serviceability services are described in the Cisco Unified Serviceability Administration Guide.

This section contains five procedures; do the applicable procedure to activate, deactivate, start, or stop Unity Connection services, or to refresh the status of services. You can activate, deactivate, start, and stop only one service at a time.

Activating a Service in Control Center

Step 1   In Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 2   From the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3   Under Optional Services, locate the service that you want to activate.

Step 4   In the Change Activate Status column, select **Activate**.

Deactivating a Service in Control Center

Step 1   In Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 2   From the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3   Under Optional Services, locate the service that you want to deactivate.

Step 4   In the Change Activate Status column, select **Deactivate**.

Starting a Service in Control Center

Step 1   In Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 2   From the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3   Locate the service that you want to start.

Note Services that are deactivated must be activated before they can be started.

Step 4 In the Change Service Status column, select **Start**.

Stopping a Service in Control Center

Step 1 In Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 2 From the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3 Locate the service that you want to stop.

Note Services in the Status Only Services section cannot be started or stopped in Cisco Unity Connection Serviceability. You must use the command-line interface (CLI) to start or stop these services.

When a Unity Connection cluster is configured, stopping a service in the Critical Services section for the server with Primary status causes the status for the servers in the cluster to change. To prevent the status change when the service is stopped, in Cisco Unity Connection Administration, you must uncheck the Automatically Change Server Status When the Publisher Server Fails check box on the System Settings > Advanced > Cluster Configuration page.

Step 4 In the Change Service Status column, select **Stop**.

Note Stopping Unity Connection services in the Critical Services section may cause calls in progress to be dropped and degrades the normal function of the Unity Connection or Cisco Business Edition server.

A service that is not activated cannot be started or stopped.

Step 5 If you are prompted that the cluster server status changes, select **OK**.

Refreshing Service Status in Control Center

Step 1 In Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 2 From the Server drop-down box, select the applicable Unity Connection or Cisco Business Edition server, and select **Go**.

Step 3 Select **Refresh**.

The status information is updated to reflect the current status.

Using Reports

Understanding Reports

Cisco Unity Connection Serviceability lets you gather information about system configuration and call handlers into reports.

Table 4: Reports Available in Cisco Unity Connection Serviceability describes the reports that you can generate in Cisco Unity Connection Serviceability.

Table 4: Reports Available in Cisco Unity Connection Serviceability

Report Name	Description of Output
Phone Interface Failed Logon	Includes the following information for every failed attempt to sign in to Unity Connection by phone: • Name of user, alias, caller ID, and extension of user who failed to sign in. • Date and time the failed logon occurred. • Whether the maximum number of failed sign-ins has been reached for the user.

Report Name	Description of Output
Users	Includes the following information for each user: • Last name, first name, and alias. • Information that identifies the Unity Connection or Cisco Business Edition server associated with the user. • Billing ID, class of service, and extension. • Whether the account is locked. • Whether the user has enabled personal call transfer rules.
Message Traffic	Includes totals for the following traffic categories: • Voice. • Fax. • Email. • Non-delivery receipt (NDR). • Delivery receipt. • Read receipt. • Hourly totals. • Daily totals.
Port Activity	Includes the following information for voice messaging ports: • Name. • Number of inbound calls handled. • Number of outbound MWI calls handled. • Number of outbound AMIS calls handled. • Number of outbound notification calls handled. • Number of outbound TRaP calls handled. • Total number of calls handled.

Report Name	Description of Output
Mailbox Store	Includes the following information about the specified mailbox stores: • Mail database name. • Display name. • Server name. • Whether access is enabled. • Mailbox store size. • Last error. • Status. • Whether the mail database can be deleted.
Dial Plan	Includes a list of the search spaces configured on the Unity Connection or Cisco Business Edition server, with an ordered list of partitions assigned to each search space. If the server is part of a Digital Network, also lists the search spaces and associated partition membership on every other Unity Connection location on the network.
Dial Search Scope	Includes a list of all users and their extensions in the specified partition that is configured in the Unity Connection directory. If a partition is not specified, lists all users and their extensions for all partitions that are configured in the directory.
User Phone Login and MWI	Includes the following information about phone logins, MWI activity, and message notifications to phone devices per user: • Name, extension, and class of service. • Date and time for each activity. • The source of each activity. • Action completed (for example, Login, MWI On or Off, and Phone Dialout). • Dial out number and results (applicable only for message notifications to phone devices). • The number of new messages for a user at time of login.

Report Name	Description of Output
User Message Activity	Includes the following information about messages sent and received, per user: • Name, extension, and class of service. • Date and time for each message. • Type of message. • Action completed (for example, new message, message saved, and so on). • Information on the message sender.
Distribution Lists	Includes the following information: • Name and display name of the list. • Date and time the list was created. (Date and time are given in Greenwich Mean Time.) • A count of the number of users included in the list. • If the Include List Members check box is checked, a listing of the alias of each user who is a member of the list.
User Lockout	Includes user alias, the number of failed logon attempts for the user, credential type (a result of "4" indicates a logon attempt from the Unity Connection conversation; a result of "3" indicates a logon attempt from a web application), and the date and time that the account was locked. (Date and time are given in Greenwich Mean Time.)
Unused Voicemail Accounts	Includes user alias and display name, and the date and time that the user account was created. (Date and time are given in Greenwich Mean Time.)
Transfer Call Billing	Includes the following information for each call: • Name, extension, and billing ID of the user. • Date and time that the call occurred. • The phone number dialed. • The result of the transfer (connected, ring-no-answer (RNA), busy, or unknown).

Report Name	Description of Output
Outcall Billing Detail	Includes the following information, arranged by day and by the extension of the user who placed the call: • Name, extension, and billing ID. • Date and time the call was placed. • The phone number called. • The result of the call (connected, ring-no-answer (RNA), busy, or unknown). • The duration of the call in seconds.
Outcall Billing Summary	Arranged by date and according to the name, extension, and billing ID of the user who placed the call, and is a listing of the 24 hours of the day, with a dialout time in seconds specified for each hour span.
Call Handler Traffic	Includes the following information for each call handler, in rows for each hour of a day: • Total number of calls. • Number of times each key on the phone keypad was pressed. • Extension. • Invalid extension. • Number of times the after greeting action occurred. • Number of times the caller hung up.
System Configuration	Includes detailed information about all aspects of the configuration of the Unity Connection system.
SpeechView Activity Report By User	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for a given user during a given time period. If the report is run for all users, then the output is broken out by user.
SpeechView Activity Summary Report	Includes the total number of transcribed messages, failed transcriptions, and truncated transcriptions for the entire system during a given time period. When messages are sent to multiple recipients, the message is transcribed only once, so the transcription activity is counted only once.

Report Name	Description of Output
HTTPS Networking Sync Error Report	(Applicable only for HTTPS Networking) Includes the following information associated with the directory objects that does not synchronize during directory synchronization: • Creation Date • Failed ObjectId • USN • Object Type • Location Display Name • HTTP(S) Link • Error Message

Setting Report Configuration Parameters

Cisco Unity Connection is automatically set to gather and store data from which you can generate reports. The parameters listed in this section can be adjusted, depending on the report output that you want to generate. All report parameter settings are found on the System Settings > Advanced > Reports page in Cisco Unity Connection Administration.

Reports data is gradually written over, depending on the parameters you set for retention of data. We recommend that if you want to keep reports for historical purposes, you develop a schedule for regularly generating reports, and save them in a location separate from the Unity Connection or Cisco Business Edition server.

- **Milliseconds Between Data Collection Cycles**—Set by default to 30 minutes (1,800,000 milliseconds). This setting controls the amount of time Unity Connection waits between cycles of gathering report data.

- **Days to Keep Data in Reports Database**—Set by default to 180 days. Note that even if you specify more than this number of days in the time range for the report you are generating, the number of days of data is limited by what you set here.

- **Maximum Records in Report Output**—Set by default to 25,000 records. The maximum value allowed for this field is 30,000 records. If the report you want to generate exceeds the maximum number of records allowed, you can generate the report in pieces (for example by reducing the date range or number of user accounts included in each iteration).

  Note The Maximum Records in Report Output setting for the User Message Activity Report has been restricted to 15,000 records—rather than the default of 25,000 records—because of the size of the report.

- **Minimum Records Needed to Display Progress Indicator**—Set by default to 2,500 records. The maximum value allowed for this field is 10,000 records. The purpose of the progress indicator is to warn you if the report you request is large and likely to take a long time to complete. In Unity Connection,

reports are generated from within a browser, and the browser session must be kept open while the report is being generated. Depending on the size of the database, and the type of report being generated, a report can take a long time to generate; meanwhile, you are unable to use the browser, and must keep the Connection Administration session open.

Generating and Viewing Reports

When you generate a report, you can specify some or all of the following:

- The objects (for example, user accounts or call handlers) to include in the report.

- The date and time range to include.

- The sort order for the data in the report.

You can select one of the following file formats for the report:

Web page	HTML file. Report output appears in your web browser.
	Select this format to quickly view a small report.
	For archiving purposes, we recommend that you generate PDF reports.
Comma-delimited file	Text file (also known as a comma-separated, or CSV, file). Report output appears as a string of data, separated by commas.
	Select this format if you want to view or print the information in another application, for example, a spreadsheet application.
PDF file	Report output appears as a PDF that can be printed and saved.
	We recommend that you select this format if you plan to archive reports.

Note A "**Checksum (SHA512) for Generated PDF or CSV Report**" link appears at the end of the page. After clicking the link, the SHA-512 checksum value is displayed for the report to check the integrity of the file.

The best time to generate reports is when the system is not busy: after regular business hours when Unity Connection is not processing many calls, or when there are no other processes running (for example, before or after a full backup). Requests to generate reports are queued. If multiple reports are generated at one time (from separate browsers), the reports wait in line and only one is processed at a time.

Caution Generating large reports when the system is busy uses system resources and could potentially result in slower response time for system users.

Note that reports cannot be scheduled in advance. If you shut down the Unity Connection or Cisco Business Edition server, or close the Connection Administration browser session while reports are being generated, the report generation is canceled.

Generating and View a Report

Step 1   In Cisco Unity Connection Serviceability, select **Tools** > **Reports**.

Step 2   On the Serviceability Reports page, select the name of the report that you want to generate.

Step 3   Select the applicable file format for the report output.

Step 4   If the fields are available, set a date range by selecting the beginning and ending month, day, year, and time.

Step 5   Set other parameters, as applicable.

Step 6   Select **Generate Report**.

Step 7   View the report output, depending on the file format you select in Step 3:

Web Page	Output appears in your browser window.
Comma-delimited File	File download dialog box opens, asking if you want to open or save the file.
PDF File	File download dialog box opens, asking if you want to open or save the file.

CHAPTER 7

Using the Voice Network Map Tool

This chapter provides information on using the Voice Network Map Tool in Cisco Unity Connection Serviceability.

Understanding the Voice Network Map Tool

The Voice Network Map tool provides a consolidated visual representation of the health of the locations in a Unity Connection site. (The tool also identifies any location in the site that acts as an intersite gateway, but does not display health information about other sites.)

With the tool, you can quickly locate replication problems in a site, and get information about the status of replication between any two locations in the site.

The tool includes a site display, a data display, and a key that explains the meaning of the icons that you may see in the site display.

The site display includes an icon for each location in the Unity Connection site. The icon itself gives you an indicator of the health of the location (or, in some cases, indicates that the tool is unable to gather data from the location).

The data display shows information about the pair of locations that you select in the site display. This information includes whether one location is currently pulling or pushing directory information with the other, and information about the USN, or sequence numbers, of replication messages sent to and from a location. (When two locations are fully synchronized, the Last USN Sent and Last USN Acknowledged values for the location that is sending replication updates equal the Last USN Received value for the location that is receiving updates. During replication, it is normal for the Last USN Acknowledged value to lag behind the Last USN Sent value.) You can also find the push/pull state and USN information in Cisco Unity Connection Administration, but the Voice Network Map tool simplifies access to the information by providing it all in one visual display.

Use the key for more information about the icons in the site display. Move the pointer over an icon in the key to see the information about it. You can view additional icons by selecting the (More) link.

Tip Right-click a location icon for options to access Cisco Unity Connection Serviceability or Cisco Unity Connection Administration for that location. If the location is a gateway to an intersite link, you can also view a map of the servers in the remote site.

Configuring Remote Access to Other Unity Connection Locations in a Unity Connection Site

In order for the Voice Network Map tool to collect the data that it needs from other locations in the Unity Connection site, the location on which you use the tool must have sign-in information for other locations in the site. The sign-in information is not replicated between locations in the site, so if you intend to use the Voice Network Map tool on multiple locations in the site, do the procedure in this section on each location on which you use the tool.

Note The sign-in information is also used when editing objects across the network in Bulk Edit mode in Unity Connection Administration. Changes you make to the sign-in information also affect access to Bulk Edit mode.

Step 1 In Cisco Unity Connection Administration, expand **Networking**, then select **Unity Connection Location Passwords**.

Step 2 On the Search Enterprise Administration Passwords page, select a Unity Connection location from the list.

Step 3 In the Alias field, enter the username for the account you use to sign in to the remote server. The account must have the System Administrator role.

Step 4 In the Password field, enter the password for the account you use to sign in to the remote server.

Step 5 Select **Add New**.

Step 6 Select **Save**.

Tip You may want to configure remote access only on an as-needed basis. When remote access is no longer needed, you can delete the sign-in information by checking the check box next to the applicable account on the Search Enterprise Administration Password page, and selecting Delete Selected.

Step 7 Repeat Step 2 through Step 6 as necessary to configure remote access to additional locations in the Unity Connection site.

Viewing Replication Status Information in the Voice Network Map Tool

To use the Voice Network Map Tool, you must have configured remote access to other locations in the Unity Connection site so that the tool can collect the data it needs. See the Configuring Remote Access to Other Unity Connection Locations in a Unity Connection Site.

Step 1 In Cisco Unity Connection Serviceability, from the Tools menu, select **Voice Network Map**.

Step 2 On the Voice Network Map page, select the first location for which you would like to view replication status information.

Step 3 To see the replication state and data about USN messages sent, received, and acknowledged between the location you selected in Step 2 and another location, move the pointer over the second location.

> **Tip** You can quickly change the second location by moving the pointer to a new location. Alternatively, to "lock" the information display to a pair of locations, press the Control key and select the second location. To release the lock, repeat the action of pressing the Control key and selecting the second location.

Step 4 To change the first location, select a new location, then repeat Step 3.

Step 5 The tool periodically updates the display information based on the update interval you specify. To change the update interval:

a) Select the **Config** tab.

b) In the Update Interval field, enter a value for the frequency at which the display information updates. The minimum value is 15 seconds, and the default value is 30 seconds. Note that the interval is reset to the default each time the Tomcat service is restarted.

c) Select **Save**.

Step 6 To pause periodic updates so that the current data continues to display, select the **Pause** tab. The tab label changes to **Resume**, which you select to have the tool resume periodic updates.

Step 7 To do an immediate update of replication information without waiting for the next update interval, select the **Update** tab.

CHAPTER 8

Using the Voice Network Map Tool in HTTPS Networking

Understanding the Voice Network Map Tool in HTTPS Networking

The Voice Network Map tool provides a consolidated visual representation of the health of the locations in an HTTPS Cisco Unity Connection network.

With the tool, you can quickly locate replication problems in a network, and get information about the status of replication between any two or more locations in the network.

The tool includes a network display, a data display, and a key that explains the meaning of the icons that you may see in the network display.

The network display includes an icon for each location in the HTTPS network. The icon itself gives you an indicator of the health of the location (or, in some cases, indicates that the tool is unable to gather data from the location). For example, if the password for a particular location is not set, then the corresponding message is displayed when you hover the mouse on the location in the network display.

The data display shows the information about the pair of locations that you select in the network display. This information includes Host Address, Display Name, Last Sync Time, Replication Set, Max USN, Last USN and the SYNC MODE between two locations in the network. For more information on the fields associated with directory synchronization, navigate to the corresponding page on Cisco Unity Connection Administration and see Help > This Page.

Use the key for more information about the icons in the network display. Move the pointer over an icon in the key to see the information about it. You can view additional icons by selecting the (More) link.

Tip Right-click a location icon for options to access Cisco Unity Connection Serviceability or Cisco Unity Connection Administration for that location.

Configuring Remote Access to Other Unity Connection Locations in an HTTPS Network

In order for the Voice Network Map tool to collect the data that it needs from other locations in an HTTPS network, the location on which you use the tool must have sign-in information for other locations in the HTTPS network. The sign-in information is not replicated between locations in the network, so if you intend to use the Voice Network Map tool on multiple locations in the network, do the procedure in this section on each location on which you use the tool.

> **Note** The sign-in information is also used when editing objects across the network in Bulk Edit mode in Unity Connection Administration. Changes you make to the sign-in information also affect access to Bulk Edit mode.

Step 1 In Cisco Unity Connection Administration, expand **Networking**, then select **Unity Connection Location Passwords**.

Step 2 On the Search Enterprise Administration Passwords page, select a Unity Connection location from the list.

Step 3 In the Alias field, enter the username for the account you use to sign in to the remote server. The account must have the System Administrator role.

Step 4 In the Password field, enter the password for the account you use to sign in to the remote server.

Step 5 Select **Add New**.

Step 6 In Stored Enterprise Administration Passwords, check the check box corresponding to the Unity Connection location for which you want to configure the remote access.

Step 7 Select **Save**.

> **Tip** You may want to configure remote access only on an as-needed basis. When remote access is no longer needed, you can delete the sign-in information by checking the check box next to the applicable account on the Search Enterprise Administration Password page, and selecting Delete Selected.

Step 8 Repeat Step 2 through Step 7 as necessary to configure remote access to additional locations in the HTTPS network.

Viewing Replication Status Information in Voice Network Map Tool

To use the Voice Network Map Tool, you must have configured remote access to other locations in the HTTPS network so that the tool can collect the data it needs. See the Configuring Remote Access to Other Unity Connection Locations in an HTTPS Network.

Step 1 In Cisco Unity Connection Serviceability, from the Tools menu, select **Voice Network Map**.

Step 2 On the Voice Network Map page, select the first location for which you would like to view replication information.

Step 3   To see the replication information, such as replication set and Last USN associated with the remote location that you selected in Step 2 and another location, move the pointer over the second location.

You can also view the directly and indirectly connected locations with respect to the reference location in an HTTPS network using VNMAP tool.

- If you hover the pointer on any location in the network display without selecting the location, the following information is displayed in data display section:

    - Host Address

    - Display Name

    - Retry Queue Size

    Tip   You can quickly change the second location by moving the pointer to a new location. Alternatively, to "lock" the information display to a pair of locations, press the Control key and select the second location. To release the lock, repeat the action of pressing the Control key and selecting the second location.

Step 4   To change the first location, select a new location, then repeat Step 3.

Step 5   The tool periodically updates the display information based on the update interval you specify. To change the update interval:

- Select the **Config** tab.

- In the Update Interval field, enter a value for the frequency at which the display information updates. The minimum value is 15 seconds, and the default value is 30 seconds. Note that the interval is reset to the default each time the Tomcat service is restarted.

- Select **Save**.

Step 6   To pause periodic updates so that the current data continues to display, select the **Pause** tab. The tab label changes to **Resume**, which you select to have the tool resume periodic updates.

Step 7   To do an immediate update of replication information without waiting for the next update interval, select the **Update** tab.

I N D E X

A

about **1, 35, 39**
    Cisco Unity Connection Serviceability **1**
    Voice Network Map tool **35, 39**
accessing **3, 4**
    Cisco Unity Connection Serviceability **3**
    Help **4**
activating services **24**
administrator workstations, configuring browsers on **2**
alarms **5, 6**
    configurations **6**
    definitions **5**
    enabling **6**
    overview **5**
    searching for definitions in database **5**
    severity **6**
    viewing definitions **5**

B

browsers, configuring on administrator workstations **2**

C

Call Handler Traffic report, description **31**
Cisco Unified Real-Time Monitoring Tool. See<Default ¶ Font>
         RTMT **5**
configuring **2, 36, 40**
    browsers on administrator workstations **2**
    remote access to other Connection locations in a Connection site,
        for Voice Network Map tool **36, 40**
Control Center **21, 24**
    list of services **21**
    using to manage services **24**

D

database, searching for alarm definitions **5**
deactivating services **24**
diagnostic traces, overview **7**
Dial Plan report, description **29**
Dial Search Scope report, description **29**
Distribution Lists report, description **30**

F

feature services **21, 24**
    list of **21**
    starting, stopping, restarting and refreshing **24**
finding version **4**
Firefox, configuring on administrator workstations **2**
functionality in Cisco Unity Connection Serviceability **1**

G

generating reports **33**

H

Help, accessing **4**

I

interface, using **3**
Internet Explorer, configuring on administrator workstations **2**

M

macro traces **16**
    enabling **16**
    list of **16**
Mailbox Store report, description **29**
managing **19**
    ports in a Cisco Unity Connection cluster **19**
    server status in a Cisco Unity Connection cluster **19**
Message Traffic report, description **28**
micro traces **8, 9**
    enabling **8**
    list of **9**

O

Outcall Billing Detail report, description **31**
Outcall Billing Summary report, description **31**

P

parameters, setting for reports **32**