Design Guide for Cisco Unity Connection 11.x

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

CONTENTS

CHAPTER 15

CHAPTER 16

CHAPTER 1

Cisco Unity Connection Overview

Cisco Unity Connection Overview

Introduction

Cisco Unity Connection is a feature-rich voice messaging platform that runs on the same Linux-based Cisco Unified Communications Operating System used by Cisco Unified Communications Manager. Unity Connection scales to support enterprise organizations with up to 100,000 users.

Flexible User Interface

There are two ways in which users can interact with Unity Connection by phone:

- Phone keypad keys—Users press keys on any touchtone phone to respond to prompts or select menu options.
- Voice commands—Users speak into the phone handset, headset, or speaker phone, and Unity Connection responds to their voice commands.

Note Users who are configured for the voice-recognition conversation have the option to press keys on the phone keypad for a primary set of commands rather than say a voice command.

The users can also press a key to toggle between the voice-recognition and touchtone conversations (by default, users press 9 to toggle between conversations, though you can use the Custom Keypad Mapping tool to assign a different key or keys). If users are assigned to the voice-recognition conversation and press 9 while in the main menu, they are switched to the touchtone conversation, and vice versa.

The Unity Connection conversations can be customized both by administrators and by end users to maximize company and individual productivity. Users can configure the system to manage calls and messages in the way that is most comfortable and convenient for them, which makes messaging more efficient for "power users" and occasional voicemail users alike. In addition, for users who are accustomed to third-party voicemail conversations, Unity Connection offers multiple conversation keypad mappings that can be further customized, as well as the option to create a new conversation using the Custom Keypad Mapping tool.

To maximize the productivity of mobile workers, consider enabling the speech-activated voice command interface. This interface allows users to browse and manage voice messages and to call other Unity Connection users or personal contacts using simple, natural speech commands.

The phone interface also allows for access to Microsoft Exchange calendars, contacts, and emails, and to Cisco Unified MeetingPlace.

Note Microsoft Exchange calendars and Cisco Unified MeetingPlace cannot be configured simultaneously for a Connection user.

Automated Attendant Functionality

Unity Connection includes a full-featured automated attendant that is customizable to suit the needs of your organization. Unity Connection provides a number of different call management elements that you can combine to customize how your system handles calls and collects input from callers. You can use the default configuration to play a company greeting to callers, allow them to enter user extensions or reach a directory of users, or reach an operator. You can also add and customize elements to create complex audio-text trees that can ask callers a series of questions and record their responses, offer tiered menus of product information, route calls to a support queue during working hours and to a mailbox after hours, immediately play legal disclaimers or “snow day” recordings to all callers before allowing them to interact with the system, and so on.

For information on call management in Unity Connection and the various elements that make up the Unity Connection conversation such as call handlers, directory handlers, interview handlers, call routing tables, schedules and holidays, and restriction tables, see the System Administration Guide for Cisco Unity Connection *Release 11.x*. Also in that guide is information on creating a call management plan, how outside callers and users interact with the Unity Connection conversation, and how administrators and users can customize the Unity Connection conversation. The guide is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

In an auto attendant configuration, Unity Connection is designed to take maximum load of eight calls per second per node or 16 calls per second for Unity Connection cluster.

In auto attendant configuration, Unity Connection recommends you to:

- Use Active-Active topology for distributing the traffic between publisher and subscriber in case of cluster. To achieve Active-Active topology, select the round robin routing on Cisco Unified CM.
- Evaluate the overall solution architecture periodically as the load on the solution grows over time.
- Implement Call Admissions Control (CAC) functionality on Cisco Unified CM to limit Unity Connection port utilization to 80% when number of calls reaches peak volume.
- Verify the system behavior under auto attendant peak call load in pilot or lab before deploying.

If auto attendant traffic volume exceeds more than eight calls per second per node or 16 calls per second for Unity Connection cluster, you should use Cisco Voice Portal (CVP) in place of Unity Connection.

Speech Connect

Unity Connection includes a speech-enabled enhancement to the automated attendant functionality, called Speech Connect. Speech Connect uses voice-enabled directory handlers that allow both employees and outside callers can say the name of an employee and instantly be connected, without having to navigate an audio-text tree, and without knowing the extension of the employee. For easy access for employees, you can configure a Speech Connect speed dial on user phones.

If multiple employees have the same name or if Speech Connect does not have a perfect match for the name spoken by the caller, it presents numerous name choices for the caller and can include additional information such as the employee location or department. If a user or a call handler does not have a recorded name, Unity Connection uses Text to Speech to play the display name of the user or call handler.

With text-to-speech feature enabled in Unity Connection, user can play the emails using phone that are accessible through the configured unified messaging account (Exchange or Office 365).

For detailed information about setting up directory handlers, see the “Directory Handlers” section of the “Call Management” chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html
.

Dial Plan Flexibility: Partitions and Search Spaces

Dial plan flexibility is supported through the use of partitions and search spaces, with which you can segment the Unity Connection directory for both dialing and addressing. For example, partitions and search spaces can be configured to allow for overlapping extensions, abbreviated dialing, or multi-tenant configurations.

If a user in a partition sends a voice message to another user in some other partition and both the users belongs to the same search space and share the same extension, then the called party partition gets replaced with the calling party partition. To resolve the overlapping of dial plan:

- Use E.164 numbers with both the calling party and called party extensions.
- Disable Identified User Messaging in System Settings of Unity Connection Administration to disable the Phone Number Resolution and users see only the phone number of the called party and not the phone number of the calling party who left the voicemail message.

For more information on using partitions and search spaces, see the “Dial Plan” section of the “Call Management” chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Video Messaging

Beginning with Unity Connection 11.5(1) and later, in addition to audio message, a user or an outside caller can also send video message to another user using video enabled end point. To record and send a video message, make sure that:

- Video messaging is enabled in Unity Connection for the user.
- End point is video enabled.

A user or an outside caller can send video message to another user only in case of Ring No Answer (RNA). Unity Connection does not support sending video messages to the outside caller.

Note Once a user is signed in to Unity Connection, even if the video messaging is enabled for a user, the user can not compose a video message. The user can only play the video messages received from the users or outside callers.

See the following references for more information video messaging:

- "Video" chapter of *System Administration Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.
- "Video Messaging" chapter of *Design Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/design/guide/b_11xcucdg.html.
- "Requirement for using Video Messaging" section of the *System Requirements for Cisco Unity Connection, Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.
- Release notes for Cisco Jabber with operating systems at http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html.

Languages

When multiple languages are installed, you can configure the language for system prompts that are played to users and callers. Separate greetings can be recorded for users and call handlers in each language that is installed on the system. Routing rules can be configured to set the language for a call based on how the call reached the system.

For a list of supported languages, see the "Available Languages for Unity Connection Components" section of System Requirements for Cisco Unity Connection *Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Synchronization of Unity Connection and Exchange Mailboxes—Single Inbox

You can configure Unity Connection to synchronize voice messages in a Unity Connection user mailbox with the user Exchange mailbox. For more information, see the "Configuring Unified Messaging" chapter of the Unified Messaging Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

You can configure Unity Connection to synchronize voice messages in a Unity Connection user mailbox with the user Exchange mailbox configured on Microsoft Business Productivity Online Suite (BPOS-Dedicated) environments as well as other third party hosted dedicated Exchange environments.

Note Third-party hosted Exchange solution provider is responsible for the qualification or testing of the third-party Exchange environment to ensure proper integration with Unity Connection.

Bandwidth and latency requirements are identical to the bandwidth and latency requirements for on-premise Microsoft Exchange environments. The following attributes of BPOS-D environments are identical to the attributes of on-premise Microsoft Exchange environments:

- Throttling Policy
- Impersonation Account

- Scalability

For more information, see the About Single Inbox, on page 45 section.

You can also configure Connection to synchronize voice messages in Unity Connection user mailbox with the user Exchange mailbox configured on Microsoft Office 365(Exchange 2010 based wave 14).

Access to Calendar, Meeting, and Contact Information

When Unity Connection is configured for a calendar integration, users can access calendar and meeting information from Cisco Unified MeetingPlace, Cisco Unified MeetingPlace Express, and Microsoft Exchange, and can import Exchange contacts for use by rules created in the Personal Call Transfer Rules web tool and for use by voice commands when placing outgoing calls.

Note MeetingPlace Express is not supported with Unity Connection 10.x and later.

For more information, see the “Configuring Unified Messaging” chapter of the Unified Messaging Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

Desktop Message Access

Unity Connection supports access to voice messages through a wide range of desktop clients, including:

- IMAP clients—Third-party IMAP clients such as email clients are supported for accessing voice messages from Unity Connection. Users can read, reply to, and forward messages from these types of clients. For more information, see the “Integrated Messaging” section of the “Messaging” chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

IMAP clients are supported when Unity Connection is configured in the following modes:

- IPv4 only mode
- Dual Mode (IPv4/IPv6)

For more information see the “Changing the IP Address or Hostname of a Unity Connection Server” of the “Maintaining Cisco Unity Connection Server” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

- Cisco Unity Connection ViewMail for Microsoft Outlook plug-in—In addition to basic IMAP access to Unity Connection voice messages, the ViewMail for Outlook form allows playing and recording messages from the Outlook client using either the phone or workstation speakers and microphones. Users can compose, read, reply to, and forward messages when using ViewMail. For more information on the ViewMail for Outlook client, see the “Configuring an Email Account to access Unity Connection Voice Messages” chapter of the User Workstation Setup Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwsx.html.

- **Web Inbox** —The Web Inbox is an application that enables users to play, compose, reply to or forward, and manage Unity Connection voice messages using a web browser. The Web Inbox replaces the Messaging Inbox web tool that was available in the Cisco Personal Communications Assistant (Cisco PCA) in earlier releases of Unity Connection.
- Cisco Unified Personal Communicator—Cisco Unified Personal Communicator is a desktop client that allows users to play voice messages. Users can read and delete messages from Cisco Unified Personal Communicator (CUPC). For more information, see the CUPC product pages at http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-personal-communicator/data_sheet_c78-647911.html.
- **Cisco Unified Messaging with IBM Lotus Sametime**—Cisco Unified Messaging with IBM Lotus Sametime integrates Unity Connection voicemail into the IBM Lotus Sametime instant messaging application, allowing users to play their voice messages within Lotus Sametime. A list of all voice messages, including the caller name or number and the date and time, are displayed in a panel on the client window. Users simply click to play their voice messages. They can also sort and delete messages directly from the Lotus Sametime application. For more information, see the Release Notes for Cisco Unified Messaging with IBM Lotus Sametime at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.
- **Visual Voicemail**—Visual Voicemail is part of the Cisco Unified Communications Widgets suite of applications. Visual Voicemail allows users to view, listen, compose, forward, delete, and respond to voice messages from their Cisco Unified IP Phone display without having to dial into their Unity Connection mailboxes. Visual Voicemail provides enhanced functionality compared with Unity Connection Phone View, an older application that provides limited access to messages from the phone display. You should use Visual Voicemail rather than the older feature. For system requirements and information on installing, configuring, and using Visual Voicemail, see the documentation at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-widgets/tsd-products-support-series-home.html.
- RSS Feeds—As an alternative to checking messages by phone or using the Web Inbox, an IMAP client users can retrieve voice messages using an RSS (Really Simple Syndication) reader. When a user marks a message as read, the message is no longer displayed in the RSS reader, but a saved copy is available in the Unity Connection mailbox of the user. For more information on configuring Unity Connection to supply RSS feeds, see the "Configuring an RSS Reader to View Voice Messages" section of the "Advanced System Settings" chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.
- Jabber - Unity Connection 11.x supports Cisco Jabber as client. For more information on Cisco Jabber for Android, see the release notes for the product at releases at http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html.

Accessing Voice Messages Using SMTP Based HTML Notifications

Unity Connection allows you to deliver embedded HTML notifications for a new voice message via SMTP to the end users. The HTML notifications on the computer support both Web email clients, such as Google Mail or Yahoo Mail) and desktop email clients (for example, Microsoft Outlook and IBM Lotus Notes). However, the HTML notifications on the mobile supports only Web email clients.

Unlike the text-based SMTP notifications, the HTML notification functionality makes listening to your voice message just a click away. Once the user clicks on the play option in the new HTML-based notification email, the Mini Web Inbox browser-based client application is loaded to play that notified voice message. The HTML notification is also an alternative to traditional Unified Messaging and IMAP messaging, which allows integration with not only Exchange and Domino, but with Gmail as well.

The content and format of the HTML notifications received via email can be customized through a notification template, custom variables, and custom graphics. Cisco Unity Connection Administration (CUCA) and the Cisco Unity Connection Provisioning Interface (CUPI) APIs can be used to work on notification templates. The administrator need to follow a checklist and must take care of few steps while working on notification templates.

To use the HTML notification templates, the HTML notification device must be enabled and a notification template must be assigned to it. For more information on checklist for the HTML notifications, see the "Setting Up SMTP Message Notification" section of the "Notifications" chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

The users are also allowed to set up an HTML notification device and configure the other settings using the Messaging Assistant web tool of Cisco Personal Communications Assistant (PCA). The user can access the notified voice message clicking the hyperlink given in the email for launching the Mini Web Inbox. With Mini Web Inbox, the user can play, reply, reply all, forward, or delete the voice messages using a phone or a computer. On mobile, Mini Web Inbox is supported via telephone record and playback (TRAP) connections on the native browser.

For more information on the Mini Web Inbox, see the Quick Start Guide for the Cisco Unity Connection Mini Web Inbox available at
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/quick_start/guide/b_11xcucqsgminiinbox.html.

The new HTML-based notifications functionality provides user with a new set of the Cisco Unity Connection Imaging Interface (CUII) APIs. In addition, there are certain set of activities that can be performed by the administrator and the user with some new introduced set of CUPI APIs.

For more information on how to manage notification templates using the Cisco Unity Connection Imaging Interface (CUII) and Cisco Unity Connection Provisioning Interface (CUPI) APIs, see the Cisco Unity Connection APIs, available at the http://docwiki.cisco.com/wiki/cisco_unity_connection_apis.

To troubleshoot any issue while creating templates or launching the Mini Web Inbox, see the "Troubleshooting Mini Web Inbox" chapter of the Troubleshooting Guide for Cisco Unity Connection, Release 11.x available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/troubleshooting/guide/b_11xcuctsg.html.

Transcriptions of Voice Messages (SpeechView)

SpeechView provides transcription of user voice messages. Users can view transcriptions of their messages using an IMAP client that is configured to access their voice messages. The transcription text can also be sent to an email address or mobile device.

In Unity Connection, based on your requirements, you can select either standard or professional SpeechView service to read the voicemail. The standard SpeechView service is a fully automated transcription service. However, professional SpeechView service involves automated transcription as well as human assistance in converting speech to text and delivering the text version of the voice message to your email inbox.

For information on configuring SpeechView, see the "SpeechView" chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Mobile Clients

Unity Connection supports access to voice messages from Windows mobile phones, RIM BlackBerry devices, and Symbian OS phones through Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator. Cisco Unity Connection also supports Cisco CIUS tablet as client. Apple iPhones with Unity Connection are supported via Cisco Mobile.

Unity Connection supports Cisco Jabber as client. For more information on Cisco Jabber for Android, see the release notes for the product at releases at http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html.

Fax Messages

Users can send a fax to a fax machine for printing (users can specify the fax number by phone), download a fax from a supported IMAP client, and forward fax messages to other Unity Connection users.

Note Cisco is not going to sell Cisco fax server after May 2011 but the support for fax server continues until May 2014.

When used in conjunction with fax detection on the Cisco IOS gateway, users can have a single number to receive both voice calls and fax calls, with voice calls forwarding to Unity Connection and fax calls forwarding to the third-party fax server. For more information, see the “Fax Server” chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Unity Connection can integrate with the following third-party fax servers to support fax messages:

- OpenText Fax Server, RightFax Edition, version 10.x and later (http://www.opentext.com/)
- Sagemcom Xmedius Fax SP version 6.5.5 (http://www.sagemcom.com/)
- Cisco Fax Server, version 10.x

Users can send a fax to a fax machine for printing (users can specify the fax number by phone), download a fax from a supported IMAP client, and forward fax messages to other users. When used in conjunction with fax detection on the Cisco IOS gateway, users can have a single number to receive both voice calls and fax calls, with voice calls forwarding to Unity Connection and fax calls forwarding to the third-party fax servers. For more information, see the Third-Party Fax Servers Integration, on page 139 chapter.

Flexible Administration and Serviceability

Administrative Tools

Unity Connection provides a set of tools for administrating, monitoring, and troubleshooting the system. These tools, some of which are also used by Cisco Unified Communications Manager, are designed to offer a consistent experience and to streamline the ongoing management and operation of the system.

- **Cisco Unified Serviceability**—A monitoring and troubleshooting tool for serviceability that is shared with Cisco Unified Communications Manager. This tool allows you generate reports, enable alarms, set trace information, activate or deactivate services that are generic to the platform, and configure simple network management protocol (SNMP) operations.

- **Cisco Unity Connection Serviceability**—A monitoring and troubleshooting tool for serviceability that is used only by Unity Connection. This tool allows you generate reports, enable alarms, set trace information, manage a Unity Connection cluster, and activate or deactivate services that are specific to Unity Connection.
- **Real-Time Monitoring Tool**—A tool that runs as a client-side application. This tool can monitor system performance, view system error messages, and collect trace log files.
- **Cisco Unified OS Administration**—A tool that you can use to change operating system settings (for example, IP address, or NTP servers), view hardware and software configuration information (for example, the amount of memory or the Cisco Unified Communications Operating System version), manage SSL certificates, upgrade Unity Connection and the operating system (they are upgraded together), and enable remote access to the Unity Connection server.
- **Cisco Unity Connection Administration**—A tool used for most administrative tasks, including specifying settings for users and implementing a call management plan. Unity Connection Administration provides access to several other tools including the Bulk Administration Tool, Custom Keypad Mapping, Task Management, and tools for importing and migrating user accounts.
- **Disaster Recovery System**—A tool that allows you to back up and, if necessary, restore data and voice messages. For more information, see the Disaster Recovery System and COBRAS, on page 131 chapter.

For more information about all of the administrative tools, see the “Tools” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Unity Connection also allows administration tasks to be segmented by administrator roles, so that administrators can be given permission to perform a range of operations, from doing individual tasks (for example, resetting passwords or unlocking accounts) to doing all Unity Connection administration functions. For more information, see the “Roles” section of the “User Attributes” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

End User Web Tools

When end users are given access to the browser-based Cisco Personal Communications Assistant (PCA), they can also be granted access to the following web tools:

- Messaging Assistant—Allows users to quickly and easily change and manage personal settings such as voicemail options, passwords, personal distribution lists, and message-delivery options.
- Cisco Unity Connection Personal Call Transfer Rules—Allows users to create call transfer rules that forward and screen incoming calls based on caller, time of day, or calendar status. (Personal Call Transfer Rules are supported only when Unity Connection is integrated with Cisco Unified Communications Manager phone systems.)
- Web Inbox —Allows users to send and access voice messages.

Note Users can directly access the Web Inbox navigating to http://<Connection host name>/inbox.

To learn more about these tools, see the applicable User Guide for Cisco Unity Connection *Release 11.x* and the Help for each tool. Unity Connection user guides are available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-user-guide-list.html.

Application Programming Interfaces (APIs)

Unity Connection includes several Representational State Transfer (REST) application programming interfaces (APIs) that provide provisioning, messaging, and telephony access to Unity Connection. These APIs provide the ability to integrate Unity Connection features into existing enterprise-wide provisioning management systems and messaging clients.

The APIs are REST interfaces that standardize operations such as add, delete, view, and modify.

Cisco Unity Connection Provisioning Interface (CUPI)

The Cisco Unity Connection Provisioning Interface (CUPI) API provides access to the most commonly provisioned data on Unity Connection systems—users, contacts, distribution lists, and call handlers.

Using CUPI for administrators, the following can be accomplished:

- Create, read, update, and delete class of service settings, schedules, user alternate names, unified messaging services, private lists, user templates, routing rules, distribution lists, call handlers, contacts, partitions and search spaces, and users and user configurations
- Reset passwords
- Import LDAP users

Using CUPI for end users, the following can be accomplished:

- Update transfer options (basic transfer rules), unified messaging account passwords, and user passwords and PINs
- Record greetings and voice names
- Create, read, update, and delete private lists and private list members, alternate names, and user-defined alternate extensions
- Read SMTP proxy addresses. basic user information (for example, alias, display name, and DTMF access ID), class of service information, and administrator-defined alternate extensions

For more information about CUPI, see the http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Provisioning_Interface_%28CUPI%29_API.

Cisco Unity Connection Messaging Interface (CUMI)

Cisco Unity Connection Messaging Interface (CUMI) API provides access to user messages.

Using CUMI, the following can be accomplished:

- Play messages
- Send, reply to, and forward messages
- Send and play broadcast messages
- Send, accept, and reject dispatch messages

- Receive notifications of new messages
- Access secure messages
- Create an archive of messages that are marked for investigative hold in order to prevent messages from being automatically deleted by message aging or message expiration.
- View mailbox quota information
- View message counts

For more information about CUMI, see the http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Messaging_Interface_%28CUMI%29_API.

Cisco Unity Connection Telephony Interface (CUTI)

Cisco Unity Connection Telephony Interface (CUTI) API provides the ability to play and record audio content over the phone.

Using CUTI, the following can be accomplished:

- Initiate dialouts to phone devices
- Play back and record greetings, messages, and other audio
- Control playback speed and volume
- Stop and resume play back and record

For more information about CUTI, see the http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Telephony_Interface_%28CUTI%29_API.

Cisco Unity Connection Notification Interface (CUNI)

Cisco Unity Connection Notification Interface (CUNI) API provides notification for one or more users. CUNI is designed for use in server-to-server applications where receiving notifications for many users over a single connection is required. CUNI is designed to handle a small number of clients that are each subscribing for notifications on a large set of subscribers. CUNI requires administrative credentials, making it inappropriate for browser applications to use directly.

For more information about CUNI, see the http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Notification_Interface_%28CUNI%29_API.

Cisco Unity Connection Imaging Interface (CUII)

Cisco Unity Connection Imaging Interface (CUII) API provides the ability to fetch mailbox information that includes message status and MWI status.

Using CUII, you can get the following information:

- Unread messages count in INBOX folder
- Urgent unread messages count in INBOX folder
- State of a particular message and the corresponding image
- MWI status and the corresponding image

For more information about CUII, see the http://docwiki.cisco.com/wiki/Cisco_Unity_Connection_Imaging_Interface_%28CUII%29_API.

Licensing

In Unity Connection, licenses are only required for users and features, which includes SpeechView, SpeechView Pro, and SpeechView Connect.The licenses are now managed by the Enterprise License Manager (ELM) server. To use the licensed features on Unity Connection, the valid licenses for the features must be installed on the Enterprise License Manager (ELM) server and Unity Connection must communicate with the ELM server to obtain the license. The ELM server provides centralized, simplified, and enterprise-wide management of user-based licensing. For more information on the ELM server and its configuration, see the Enterprise License Manager User Guide available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/elmuserguide/9_0_1/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html.

Unity Connection remains in the Demonstration (Demo) mode until it connects with the ELM server. For information on Unity Connection licenses, see the " Managing Licenses"chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

LDAP Directory Synchronization and Authentication

If you are using a supported LDAP directory for your corporate directory, Unity Connection gives you the option to synchronize a small subset of user data in the Unity Connection database with user data in the LDAP directory. In addition, if you configure directory synchronization, you can have Unity Connection authenticate user access to Unity Connection web applications against Active Directory credentials. You can also configure Unity Connection to periodically resynchronize Unity Connection user data with user data in the LDAP directory.

Unity Connection LDAP directory support does not require directory schema extensions, and access to the directory is read-only.

Unity Connection also supports standalone users and users imported from Cisco Unified Communications Manager via AXL. Both standalone users and users imported from Cisco Unified CM can be converted to LDAP users at any time.

For more information on Unity Connection support for LDAP synchronization and authentication, see the LDAP Directory Integration with Cisco Unity Connection, on page 81 chapter.

Security

Unity Connection supports security in a number of areas of the product:

- **Platform**—Unity Connection is based on the Linux-based Cisco Unified Communications Operating System. The operating system is locked down, and no root access is allowed. For more information on the Cisco Unified Communications Operating System, see the Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection, *Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/os_administration/b_11xcucosagx.html.
- **Security Enhanced Linux (SELinux)**—In previous Unity Connection releases, Cisco Security Agent was installed on the Unity Connection server to secure communication with other servers and with clients. With Unity Connection 8.6, Cisco Security Agent has been replaced with Security-Enhanced Linux (SELinux).The SELinux access-control security policies have been configured specifically for Unity

Connection. For example, the same TCP and UDP ports that must be opened in a firewall to allow inbound and outbound communication are also opened in SELinux. For a list of these ports, see the "IP Communications Required by Cisco Unity Connection" chapter of the Security Guide for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

Note You cannot change the SELinux security policies.

You can disable SELinux policy enforcement using the **utils os secure** CLI command if necessary, for example, for troubleshooting. However, by disabling SELinux, you are subjecting the Unity Connection server to unauthorized access. For more information on the **utils os secure** CLI command, see the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

- **Call signaling and media stream**—Unity Connection allows for authentication and encryption of call signaling and media with both SCCP and SIP trunk integrations with Cisco Unified Communications Manager. For more information, see the Integrating Cisco Unity Connection with Phone System chapter.

- **Unauthorized access**—In order to help prevent unauthorized access, Unity Connection allows for authentication polices (for both phone and web access) that can control the number of attempted sign-ins, account lockout policies, minimum password lengths, and password expiration. For more information, see the "Authentication Rules" section of the "System Settings" chapter of the *System Administration Guide for Cisco Unity Connection, Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html

- **Unauthorized transfers and dial outs**—Unity Connection restriction tables control which numbers are allowed for transfers and dialouts, thus locking down unauthorized use of the system by users and helping prevent toll fraud. For more information, see the "Restriction Tables" section of the "Call Management" chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html

- **Secure messages**—Unity Connection supports secure messaging. For more information, see the Secure Messages, on page 15 section .

- Communications between Cisco Unity Connection and clients—For more information on securing the communications between Unity Connection and clients, see the Securing Communications between Unity Connection and Clients, on page 15.

- **Single Sign On**—The SAML SSO feature requires Active Directory and Identity Provider to provide single sign-on access to web applications on Unified Communication products. SAML SSO allows the LDAP users to login with a username and password that authenticates on Identity Provider. The non-LDAP users with administrator rights login to Cisco Unity Connection Administration using Recovery URL. When SSO login fails (e.g. If Identity Provider or Active Directory is inactive), Recovery URL provides alternate access to the administrative and serviceability web applications via username and password. For more information on SAML SSO, see the Quick Start Guide for SAML SSO in Cisco Unity Connection Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/quick_start/guide/b_11xcucqssamlsso.html.

Note Non-LDAP users are the users that reside locally on Unity Connection server.

A user signed in to any of the supported web applications on Unified Communication products (after enabling the SAML SSO feature) also gains access to the following web applications on Unity Connection:

Unity Connection users	Web applications
LDAP users with administrator rights	• Cisco Unity Connection Administration • Cisco Unity Connection Serviceability • Cisco Unified Serviceability • Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version) • Real Time Monitoring Tool
LDAP users without administrator rights	• Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox (desktop version)

Note To allow users to access Web Inbox and Mini Web Inbox, you must have a user with mailbox. Also navigate to Unity Connection Administration> Class Of Service > Licensed Features and make sure that the Allow Users to Use the Web Inbox, Messaging Inbox and RSS Feeds check box is checked.

With Unity Connection 10.5(1) and later, VMRest APIs expand single sign-on access (SSO) support to include authentication using a SSO OAuth 2.0 token.

- Cross-Origin Resource Sharing (CORS)- The Cross-Origin Resource Sharing feature allows the client applications of a cross domain server to access content on a Unity Connection server.

With Unity Connection 11.x, the client applications are allowed to process the cross-origin requests in a more secured way. CORS uses HTTP headers to establish an agreement between the web browser and Unity Connection server to provide services to permitted domains.

For more information on CORS, see the “Cross Origin Resource Sharing” section of the “System Settings” chapter in System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

- Multi-Server Certificate Support for Tomcat- Multi-server Subject Alternate Name (SAN) is a section defined under X.509 certificate extensions. SAN contains multiple Fully Qualified Domain Names (FQDN) or hostnames or other valid names. X.509 technology allows placing a trust in the identity of an entity such as Internet websites when it is digitally signed by a Certificate Authority (CA). SAN field allows multiple FQDNs, domain names or other approved names to be included in X.509 certificate. This way a user does not need to generate a certificate for each server. Instead one certificate identifies multiple servers.

Note For telephony integration, multi-server SAN certificate is supported only with SIP integration. However, with SCCP integration, only single-server certificate is supported.

For more information on Configuring, Generating CSR and Downloading CSR using Multi-server SAN Certificate, see the “Security” chapter of the Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection- Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/os_administration/b_11xcucosagx.html.

Secure Messages

Messages that are marked secure are stored only on the Unity Connection server, thereby disallowing secure messages from leaving an organization. Users cannot make local copies of secure messages. Message aging policies allow administrators to control how long secure messages are retained before they are archived or permanently deleted.

Secure messages can be played only using the following interfaces:

- Phone
- Web Inbox
- Cisco Unity Connection ViewMail for Microsoft Outlook
- Cisco Unity Connection ViewMail for IBM Lotus Notes
- Cisco Unified Personal Communicator (CUPC)
- Cisco Unified Mobile Communicator and Cisco Mobile
- Cisco Unified Messaging with IBM Lotus Sametime Plug-in
- Cisco Jabber

Secure messages are streamed securely to these interfaces and do not leave the Unity Connection server. When Unity Connection servers are networked together in a Unity Connection site, users on one system can send secure messages to users on another. In that situation, secure messages are encrypted with SMIME while they are in transit between servers.

The following interfaces do not support playback of secure messages:

- Third-party IMAP email clients other than Cisco Unity Connection ViewMail for Microsoft Outlook
- RSS Readers

For more information on secure messages, see the “Securing User Messages” chapter of the Security Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html

Securing Communications between Unity Connection and Clients

- **Cisco Personal Communications Assistant**—For information on securing the Cisco Personal Communications Assistant (PCA) and Cisco Unity Connection web tools client access to Unity Connection, see the “Using SSL to Secure Client/Server Connections” chapter of the Security Guide for Cisco Unity

Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html

- **IMAP clients**—For information on securing IMAP email client access to Unity Connection, see the "Using SSL to Secure Client/Server Connections" chapter of the Security Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html and the "Configuring an Email Account to Access Unity Connection Voice Messages" chapter of the User Workstation Setup Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user_setup/guide/b_11xcucuwsx.html.
- **Mobile clients**—For information on securing communication between mobile clients and Cisco Unity Connection, see the Cisco Mobile, Cisco Unified Mobile Communicator, and Cisco Unified Mobility Advantage documentation, available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.
- **RSS clients**—For information on securing communication between RSS clients and Cisco Unity Connection, see the "Configuring an RSS Reader to View Voice Messages" section of the "Advanced System Settings" chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x,* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Tenant Partitioning

Tenant Partitioning is a cloud based voice mail solution where service providers provide voice mail service to multiple small medium businesses (SMB) on a single installation of Unity Connection.A tenant is a logical grouping of objects within the Unity Connection appliance that together make an independent tenant (customer) hosted on the server. Unity Connection allows you to have more than one tenant on a single installation. These tenants exist as islands within the server and would have no knowledge of each other.Tenant Partitioning is the Unity Connection feature that enables the appliance to host more than one tenant. For more information, see the "Tenant Partitioning, on page 59 "chapter.

Supported Unity Connection Platforms

For a list of servers that are qualified for use with Unity Connection, including detailed hardware specifications, the maximum number of ports, the maximum number of users, the total number of minutes of message storage, and so on, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Note that when a customer configures a Unity Connection cluster (active/active high availability), two Unity Connection servers are required:

- The publisher server, which publishes the database and message store.
- The subscriber server, which subscribes to the database and message store on the publisher server.

Note Both servers can service call traffic and client/administration traffic.

Voice Recognition is also supported on the Unity Connection servers. For capacity planning for voice recognition, see the *Cisco Unity Connection Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html .

Supported Phone Systems

Cisco Unity Connection natively integrates with Cisco Unified Communications Manager and with Cisco Unified Communications Manager Express through Skinny Client Control Protocol (SCCP) or through a SIP trunk.

If the customer integrates Unity Connection with a circuit-switched phone system, additional hardware is needed:

- Many integrations with circuit-switched phone systems use PIMG or TIMG units for analog, digital, or T1 interfaces. Serial integrations (SMDI, MCI, and MD-110) with analog interfaces also require special cables. For more information about PIMG/TIMG integrations, see the applicable integration guide at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.
- If the customer integrates Unity Connection with a QSIG-enabled phone system, an ISR voice gateway is required. For more information, see the applicable integration guide at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Unity Connection can also be integrated with multiple phone systems. For more information, see the *Multiple Phone System Integrations Guide for Cisco Unity Connection 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/multiple_integration/b_cuc11xintmultiple.html.

For the requirements of the phone system integration, see the System Requirements for Cisco Unity Connection *Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

For more information on phone system integrations, see the Integrating Cisco Unity Connection with Phone System, on page 93 chapter.

For supported deployment models, see the "Overview of Cisco Collaboration System Components and Architecture" chapter of the *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND),* available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Support for Comet Notifications over SSL

Unity Connection allows the user to send comet notifications over SSL. To send comet notifications over SSL, you need to enable comet notification over the SSL mode using the CLI command utils cuc jetty ssl enable.

For more information on CLI commands that enable or disable Connection Jetty over SSL, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 10.0 (1) http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

When Unity Connection Jetty over SSL mode is enabled, you need to restart the Unity Connection Jetty service so that Unity Connection Jetty and comet notification client use the new SSL certificates.

For more information on restarting connection Jetty, see the “Securing Connection Administration, Cisco PCA, Unity Connection SRSV, and IMAP Email Client Access to Unity Connection” section of the “Using SSL to Secure Client/ Server Connections” chapter of the Security Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

For information on number of Jabber endpoints that Unity Connection supports with single inbox users for specific OVA, see the " Jabber Scaling Platform" section of the Supported Platforms Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html

Unity Connection Clusters (Active/Active High Availability and Redundancy)

Unity Connection supports a two-server active/active cluster to provide high availability and redundancy. Both servers in the Unity Connection cluster run Unity Connection, and both accept calls, HTTP requests, and IMAP requests. If one server in the Unity Connection cluster becomes inactive, the other server continues to provide the end-user functionality including voice calls, HTTP requests, and IMAP requests. In this situation, a lower port capacity is available for taking voice calls. For more information, see the Cisco Unity Connection Clusters (Active/Active High Availability), on page 123 chapter.

Networking

Each Unity Connection server (or cluster) has a maximum number of users that it can serve. When the messaging needs of your organization require more than one Unity Connection server or cluster, or you need a way to combine multiple Unity Connection directories or to internetwork Unity Connection with Cisco Unity, you can link Unity Connection servers or clusters together to form sites, and link a Unity Connection site with another Unity Connection site or with a Cisco Unity site to form a Cisco Voicemail Organization.

Unity Connection supports three types of networking:

- Legacy Networking
    - Intersite Networking
    - Intrasite Networking

    Note SMTP Protocol is used for directory synchronization within a network.

- VPIM Networking
- HTTPS Networking

For more information on HTTPS networking, see the HTTPS Networking Guide for Cisco Unity Connection Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/https_networking/guide/b_11xcuchttpsnet.html.

For more information on Legacy and HTTPS networking design, see the Networking chapter

Third-Party Voicemail Interoperability

Unity Connection supports Voice Profile for Internet Mail (VPIM) version 2 that allows the exchange of voice and text messages with other messaging systems. You can use VPIM Networking to network Unity Connection with other voice messaging systems, including Cisco Unity, Unity Connection, Cisco Unity Express, or any third-party voice messaging system that supports the VPIM version 2 protocol.

For more information on VPIM Networking design, see the Networking chapter.

For More Information

System Requirements

The System Requirements for Cisco Unity Connection *Release 11.x* lists the requirements for installing the Cisco Unity Connection system.

The document is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Compatibility

The Compatibility Matrix includes the supported version combinations for Cisco Unity Connection and the software installed on user workstations, including browsers and versions supported for each browser when using the Cisco Personal Communications Assistant and Cisco Unity Connection web tools, supported IMAP clients, and information on the versions of Microsoft Outlook that are supported with ViewMail for Outlook and ViewMail for Notes. It includes the supported version combinations for SCCP integrations and SIP integrations with Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express.

The document is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

Supported Deployment Models for Unity Connection and Phone Systems

For supported deployment models, see the "Cisco Voice Messaging" chapter of the *Cisco Unified Communications System 11.x SRND* at .

Deploying ViewMail for Outlook

Deploying the ViewMail for Outlook (VMO) Windows Installer File (MSI) is supported through any software distribution package that supports the Windows Installer File (MSI) format. For more information, see the Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook, available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Release Notes for Cisco Unity Connection

Release Notes for Cisco Unity Connection contain information on new and changed requirements and support, new and changed functionality, limitations and restrictions, open and resolved caveats, and documentation updates.

Release notes are available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.

Documentation Guide for Cisco Unity Connection

The Documentation Guide for Cisco Unity Connection contains descriptions and links for all documentation produced for a particular Unity Connection release.

The Guide is available at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-documentation-roadmaps-list.html.

CHAPTER 2

Optional Network Resource Requirements

DHCP

Use of Dynamic Host Configuration Protocol (DHCP) is optional with Unity Connection and can be used to automatically configure network settings on the Unity Connection server. If DHCP is not used, network settings such as hostname, IP address, IP mask, and gateway address must be manually entered during install or configured after install using the command line interface.

DNS

Use of DNS name resolution is optional with Unity Connection, but if available, should be used with Unity Connection. If DNS name resolution is not enabled, IP addresses (not hostnames) should be used for all network devices.

Microsoft Exchange

For all versions of Unity Connection, when you are using Exchange 2013, Exchange 2010 or Exchange 2007 as a calendar application, you can configure Unity Connection to allow users to do several meeting-specific tasks using the phone, for example, to hear a list of the participants for a meeting, send a message to the meeting organizer, or send a message to the meeting participants. Meeting organizers can also cancel a meeting. In addition, if users are using Microsoft Outlook, they can hear a list of upcoming meetings, and accept or decline meeting invitations.

Unity Connection also enables users to import Exchange contacts using the Messaging Assistant web tool. The contact information can then be used in rules that users create in the Cisco Unity Connection Personal Call Transfer Rules web tool and when users place outgoing calls using voice commands.

Unity Connection can play Exchange email over the phone using Text to Speech.

You can also synchronize Unity Connection and Exchange mailboxes so that Unity Connection voice messages appear in the Outlook inbox. This feature is commonly known as single inbox.

For more information on supported versions of Microsoft Exchange for accessing calendar information, importing personal contacts, accessing email, and configuring mailbox synchronization, see the "Requirements for using Unified Messaging Features" section of the System Requirements Guide for Cisco Unity Connection *Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html

Also see the "Configuring Unified Messaging" chapter of the Unified Messaging Guide for Cisco Unity Connection, *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

LDAP Directory

Unity Connection can optionally use an LDAP directory (for example, Microsoft Active Directory) for LDAP directory synchronization and authentication. For more information on supported LDAP directories, see the "Requirement for an LDAP Directory Integration" section of the System Requirements for Cisco Unity Connection *Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html

See the LDAP Directory Integration with Cisco Unity Connection, on page 81 chapter for design considerations when integrating Unity Connection with an LDAP directory.

For LDAP directory to work smoothly with Unity Connection in WAN environment you need to take care of following:

- Latency should not exceed 80 ms round-trip
- Access Control lists for corresponding ports and IPs shall be provisioned on the network devices.

CHAPTER 3

Sizing and Scaling Cisco Unity Connection Servers

For a list of servers that meet Unity Connection specifications, see the Cisco Unity Connection 11.x Supported Platforms List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Audio Codecs

Audio Codec Usage for Call Connections and Recording

In Unity Connection, a call in any audio codec format supported by SCCP or SIP signaling—G.711 mu-law, G.711 a-law, G.722, G.729, and iLBC—are always transcoded to PCM linear. From PCM linear, the recording is encoded in the system-level recording audio codec—PCM linear, G.711 mu-law, G.711 a-law, G.729a, or G.726—a systemwide setting in Cisco Unity Connection Administration. G.711 mu-law is the default.

In this section, we refer to the audio codec that is negotiated between the calling device and Unity Connection as the "line codec," and the audio codec that is set as the system-level recording audio codec as the "recording codec."

Supported Line Codecs (Advertised Codecs)

- G.711 mu-law
- G.711 a-law
- G.722
- G.729
- iLBC

Supported Recording Codecs (System-Level Recording Audio Codecs)

- PCM linear
- G.711 mu-law (default)
- G.711 a-law
- G.729a
- G.726
- GSM 6.10

Because transcoding occurs in every connection, there is little difference in system impact when the line codec differs from the recording codec. For example, using G.729a as the line codec and G.711 mu-law as the recording codec does not place a significant additional load on the Unity Connection server for transcoding. However, the iLBC or G.722 codecs require more computation to transcode, and therefore places a significant additional load on the Unity Connection server. Consequently, a Unity Connection server can support only half as many G.722 or iLBC connections as it can G.711 mu-law connections.

Note Use of the G.722 or iLBC codec as line codecs or advertised codecs reduces the number of voice ports that can be provisioned on the Unity Connection server. For more information on the number of voice ports supported for each platform overlay when using G.722 or iLBC codecs, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Generally, you should not change the system recording format from the default setting except in the following situations:

- To address disk space considerations, consider using a low bit-rate codec such as G.729a or G.726. Note that a low bit-rate codec produces lower quality audio than a high bit-rate codec such as G.711 mu-law.
- To improve the audio quality of recordings for endpoints that use G.722 as the line codec, consider using PCM linear. Note that PCM linear increases the disk space that is used.

There are additional possible reasons to change the recording codec or to choose only to advertise specific line codecs. Review the following information when making decisions on the system-level recording audio codec and the advertised codecs on the SCCP or SIP integration:

- The audio codecs that are negotiated between the majority of the endpoints and Unity Connection. This information helps you decide the audio codecs that Unity Connection should advertise and the audio codecs that Unity Connection should not advertise. You can then decide when you need Cisco Unified Communications Manager to provide hardware transcoding resources rather than using Unity Connection to provide computationally significant native transcoding, such as when the configuration requires a number of clients to connect to Unity Connection using G.722 or iLBC.

- The types of graphical user interface (GUI) clients that play the recordings (for example, web browsers, email clients, or media players) and the audio codecs that these GUI clients support.
- The quality of the sound produced by the selected audio codec. Some audio codecs produce higher audio quality than other audio codecs. For example, G.711 produces a higher audio quality than G.729a and is a better choice when higher audio quality is necessary.
- The amount of disk space that the audio codec takes up per second of recording time.

PCM linear produces the highest audio quality and is the most widely supported by media players, yet it uses the most disk space and bandwidth (16 KB/sec). G.711 (both a-law and mu-law) produces moderate audio quality compared to PCM linear and is also widely supported by media players, though it uses half as much disk space and bandwidth (8 KB/sec). G.729a produces the lowest audio quality of the four supported audio codecs and is poorly supported by media players because it requires a license for use. Yet this audio codec uses the least amount of disk space (1 KB/sec). G.726 produces moderate audio quality, is moderately supported by media players, and uses less disk space than most of the other codecs (3 KB/sec). This information is summarized in below table.

Table 1: Comparison of Audio Codecs Used for Recording

Recording Audio Codec	Audio Quality	Supportability	Disk Space Used	Sampling Rate	Channels	Sample Size
PCM linear	Highest	Widely supported	16 KB/sec	8 kHz/sec	1	16 bits
G.711 mu-law/a-law	Moderate	Widely supported	8 KB/sec	8 kHz/sec	1	8 bits
G726	Moderate	Moderately supported	4 KB/sec	8 kHz/sec	1	4 bits
GSM 6.10	Moderate	Poorly supported	1.63 KB/sec	8 kHz/sec	1	N/A
G.729a	Lowest	Poorly supported	1 KB/sec	8 kHz/sec	1	N/A

For details on changing the audio codec that is advertised by Unity Connection, or the system-level recording audio codec, see the “Changing the Audio or Video Format of Recordings” section of the “User Settings” chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

When modifying the advertised audio codecs, the choices are G.711 mu-law, G.711 a-law, G.722, G.729, and iLBC. In addition, you also indicate an order of preference for the chosen codecs.

For SCCP integrations, the order of the audio codecs is not important because Cisco Unified CM negotiates the audio codec based on the location of the port and the device in the negotiated call. However, for SIP integrations the order of the audio codecs is important. If one audio codec is preferred over another audio codec, Unity Connection advertises that it supports both audio codecs but prefers to use the one specified over the other.

Note In Web Inbox, the received voice messages are always played or downloaded in PCM linear whether any codec is selected to record the messages.

Audio Codec Considerations for VPIM Networking

If VPIM networking connects Unity Connection to another Unity Connection server, to a Cisco Unity server, or to a third-party voice-messaging system, you must choose a compatible audio codec.

Note the following audio codec considerations for Unity Connection VPIM networking:

- For inbound messages, Unity Connection can do one of the following:
  - Convert voice messages to any audio format that Unity Connection supports.
  - Not convert the audio format of the voice message, keeping the voice message in its original audio format.
- For outbound voice messages, Unity Connection can do one of the following:
  - Convert voice messages to the G.726 audio format.
  - Not convert the audio format of the voice message, keeping the voice message in its original audio format. Not converting is useful when you use VPIM networking to send voice messages between Unity Connection servers, or between Unity Connection and Cisco Unity servers.

For more information on VPIM Networking, see the VPIM Networking, on page 43 .

Voice Messaging Ports

- **The existing voice messaging system** -Evaluate how well the existing voice messaging system functions, if applicable. This evaluation may give you some idea how many ports are needed for taking voice messages, for turning message waiting indicators (MWIs) on and off, and for message notification.
- **Use of the Web Inbox web client, or the Cisco Unity Connection ViewMail for Microsoft Outlook client** -When users use the Web Inbox web client, the Messaging Inbox web client, or the ViewMail for Outlook client, Unity Connection uses telephone record and playback (TRAP) to allow users to play and record voice messages by phone rather than using speakers and a microphone. This feature is especially useful when users work in cubicles, where there is a lack of privacy. However, when a user plays or records a message using TRAP, a port on the Unity Connection server is used. (No port is used when a user uses speakers and a microphone to play and record messages.) If the customer wants users to use TRAP, calculations for the total number of voice ports required need to take this into account.
- **Unity Connection cluster** -In some cases, an existing voice messaging system has more voice messaging ports than Unity Connection supports. When configured as a Unity Connection cluster (an active/active high availability Unity Connection server pair), the Unity Connection system can support double the number of voice messaging ports compared to a single-server deployment. For more information, see the Cisco Unity Connection Clusters (Active/Active High Availability), on page 123 chapter.
- **Networking** -The customer can purchase additional Unity Connection servers or Unity Connection cluster pairs and connect them using intrasite and/or intersite networking to increase the number of voice ports supported. For more information, see the Networking, on page 35 chapter.

For additional information on the number of voice messaging ports, see the " Planning the Usage of Voice Messaging Ports " section in the applicable Cisco Unity Connection integration guide at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/sip-csps/b_cuc11xintcsps.html.

Storage Capacity for Voice Messages

For Unity Connection systems that are configured to store voicemails only (no emails or faxes are stored on the server), base the server requirements on the total number of voice storage minutes required for each user. A supported Unity Connection server generally provides storage for at least 20 to 30 minutes of voice messages per user for the maximum number of users supported on that server. See the *Cisco Unity Connection 11.x Supported Platforms List* for the exact amount of voice-message storage supported for each server.

For Unity Connection systems that are configured to store faxes and email replies to voice messages in addition to voice messages, you cannot base server requirements on the total number of voice-storage minutes required for each user because the message store on the Unity Connection server also include faxes and possibly email. However, you can calculate the storage requirement for the desired number of voice-storage minutes and add that to the current mailbox limits.

For Unity Connection systems that are configured to store faxes and email replies to voice messages in addition to voice messages, start with the total number of voice-storage minutes required for each user, and add the amount of storage space that you want users to have for faxes. In general, the email stored in Unity Connection should not significantly affect storage capacity.

Note The email stored in Unity Connection is only replies to or forwards of Unity Connection voice messages, with or without the original voice message. This email is not related to email in the email inbox of the user.

If the customer is replacing an existing voice-messaging system with Unity Connection, it may be possible to obtain information from the existing system on the average number of minutes of voice messages that users currently have. You can then multiply the average number of minutes by the recording size per minute—according to the codec that Unity Connection uses to record messages—to arrive at the average amount of disk space required for voice messages per user.

Start with a one-to-one correlation between the legacy voice-messaging system and Unity Connection. If the legacy system handles a larger capacity than the largest Unity Connection server, consider splitting the legacy user population onto more than one Unity Connection server.

Users

For the maximum number of users supported for each supported server, planning, and selection of servers, take into account the possibility of adding users in the future. For more information, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For information on moving users from one Cisco Unity Connection server to another, see the “Moving or Migrating Users Between Locations in Cisco Unity Connection” section of the “Users” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Simultaneous TUI/VUI Sessions

To determine the maximum number of simultaneous TUI (touchtone conversation) and/or VUI (voice-recognition) sessions that Unity Connection can support, consider the following:

- **Unity Connection cluster**—If a Unity Connection cluster server pair is configured (active/active high availability) instead of a standalone Unity Connection server, the maximum number of TUI and/or VUI sessions supported is doubled for each platform overlay. For the maximum number of sessions that Unity Connection can support for each platform overlay when a Unity Connection cluster is configured, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

- **Desktop Clients**—When desktop clients (for example, the Web Inbox and IMAP) are deployed, the maximum number of TUI and/or VUI sessions that Unity Connection supports is reduced for Platform Overlay 1 servers. For more information, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Note that some IMAP clients (for example, Cisco Unified Personal Communicator 7.0 and earlier) do not support the IMAP IDLE command. IMAP clients that do not support IMAP IDLE consume more system resources on a Unity Connection server. As a result, each active instance of each client that does not support IMAP Idle and is accessing Unity Connection voice messages counts as four active clients. See the IMAP Clients Used to Access Unity Connection Voice Messages for additional details.

- **G.722 and iLBC Audio Codecs**—Using G.722 or iLBC audio codecs “on the line” or as advertised codecs reduces the maximum number of TUI and/or VUI sessions that Unity Connection supports for each platform overlay by 50 percent as compared to using the G.711 audio codec. For the maximum number of sessions that Unity Connection supports for each platform overlay when using the G.722 or iLBC audio codec, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html. For a discussion of supported system recording and advertised or “on the line” audio codecs with Unity Connection, see the Audio Codecs.

- **Media Encryption and Authentication using Secure Real Time Protocol (SRTP)**—Using SRTP for media encryption and authentication reduces the maximum number of TUI and/or VUI sessions that Unity Connection supports for each platform overlay upto 15 percent.

IMAP Clients Used to Access Unity Connection Voice Messages

Third-party IMAP clients such as email clients are supported for accessing voice messages from Unity Connection. Scalability of IMAP clients depends on whether they support IMAP Idle. Using clients that support IMAP Idle reduces the load on the Unity Connection server; a Unity Connection server can support four times as many IMAP Idle clients as it can non-IMAP Idle clients. (IMAP Idle, described in RFC 2177, allows a client to indicate to the server that it is ready to accept real-time notifications.)

Most third-party IMAP email clients, such as Microsoft Outlook and Lotus Notes, support IMAP Idle. Cisco Unified Personal Communicator (CUPC) version 8.0 and later supports IMAP idle. The Unity Connection Plug-in for IBM Lotus Sametime version 7.11 and later supports IMAP idle. Among the clients that do not support IMAP Idle are Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator. For information on whether a client supports IMAP Idle, see the documentation for the client. For information on the number of IMAP clients supported for each platform overlay (each grouping of comparable supported Unity Connection servers), see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

You can mix IMAP Idle and non-IMAP Idle clients if necessary. However, to simplify sizing calculations, you should isolate IMAP Idle and non-IMAP Idle clients on separate Unity Connection servers or cluster server pairs (active/active high availability). If you must mix IMAP Idle and non-IMAP Idle clients on the same server or cluster server pair, count each non-IMAP Idle client as four IMAP Idle clients for sizing calculations. In addition, you may want to put users who use IMAP Idle clients and users who use non-IMAP Idle clients into separate classes of service so that you can run a report that tells you how many of each you have accessing voice messages on a given Unity Connection server.

Note that when you isolate IMAP Idle and non-IMAP Idle clients on separate servers or cluster server pairs, you should set up networking between the servers if they are not already networked. For more information on Unity Connection networking, see the Networking, on page 35 chapter.

Note Accessing voice messages from Unity Connection through IMAP clients is supported with both the IPv4 and IPv6 addresses. However, sending voice messages to Unity Connection using SMTP is only supported with the IPv4 addresses.

Visual Voicemail Clients and Sessions

The maximum number of visual voicemail clients is equivalent to the maximum number of users supported by a Unity Connection server or a cluster (active/active high availability) server pair. For the maximum number of Visual Voicemail clients, sessions, or ports supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

The maximum number of Visual Voicemail sessions is equivalent to the maximum number of ports available on a Unity Connection server or cluster (active/active high availability) server pair.

For supported versions of Cisco Unified Communications Manager and Cisco IP Phones with the Visual Voicemail feature, see System Requirements for Cisco Unity Connection *Release 11.x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/11xcucsysreqs.html.

For system requirements, see the *Release Notes for Visual Voicemail Release 8.5* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

For installation and configuration information, see the applicable *Installation and Configuration Guide for Visual Voicemail Release* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cupa/visual_voicemail/8-5/install/guide/vv_install.html.

For end-user information, see the *Quick Start Guide: Visual Voicemail Release 8.5* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cupa/visual_voicemail/8-5/quick_start/guide/Quick_Start_Guide_for_Visual_Voicemail_Release_8-5_chapter1.html.

Simultaneous Mobile Clients

Cisco Unified Mobility Advantage (CUMA) Release 7.0 connects to the Unity Connection server using IMAP, so it is considered an IMAP client. Because the Cisco Unified Mobility Advantage IMAP connection is not an IMAP Idle connection, the maximum number of simultaneous mobile clients supported by Cisco Unified Mobility Advantage, Cisco Unified Mobile Communicator, and Unity Connection is reduced by approximately 70 percent. For the maximum number of Cisco Unified Mobility Advantage clients and Cisco Unified Mobile Communicator clients supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Messaging Assistant Clients

The maximum number of Messaging Assistant clients is equivalent to the maximum number of users supported by a Unity Connection server or a cluster (active/active high availability) server pair. For the maximum number of Messaging Assistant clients or users supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For information on using the Messaging Assistant, see the User Guide for the Cisco Unity Connection Personal Call Transfer Rules Web Tool *(Release 11.x)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user/guide/pctr/b_11xcucugpctr.html.

Web Inbox Clients

For the maximum number of Web Inbox clients supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For information on using the Web Inbox, see the Quick Start Guide for the Cisco Unity Connection Web Inbox *(Release 11.x)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/quick_start/guide/b_11xcucqsginbox.html.

Cisco Unified Personal Communicator Clients

The Cisco Unified Personal Communicator (CUPC) client does not support IMAP Idle, so the number of CUPC clients supported by a Unity Connection server or a cluster (active/active high availability) server pair is lower than the maximum number of users. For the maximum number of CUPC clients supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For information on using CUPC, see the applicable Cisco Unified Personal Communicator user guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-personal-communicator/products-user-guide-list.html.

IBM Lotus Sametime Clients

The voice messaging plug-in for the IBM Lotus Sametime client does not support IMAP Idle, so the number of IBM Lotus Sametime clients supported by a Unity Connection server or a cluster (active/active high availability) server pair is lower than the maximum number of users. For the maximum number of IBM Lotus Sametime clients supported for each platform overlay, see the *Cisco Unity Connection 11.x Supported Platforms*

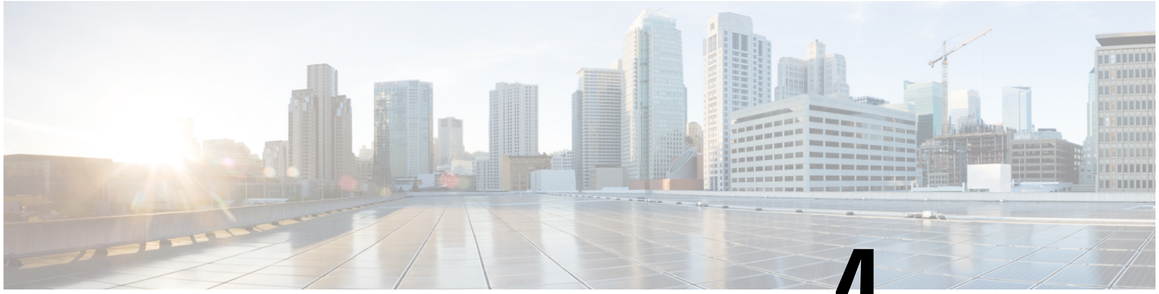
List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For information on the IBM Lotus Sametime client, see the applicable version of *Release Notes for Cisco Unified Messaging with IBM Lotus Sametime* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html.

RSS Reader Clients

The maximum number of RSS reader clients is equivalent to the maximum number of users supported by a Unity Connection server or a cluster (active/active high availability) server pair.

For more information on the RSS Feed feature and RSS reader clients, see the "Configuring an RSS Reader to View Voice Messages" section of the "Advanced System Settings" chapter of the System Administration Guide for Cisco Unity Connection *Release 11.x,* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.



CHAPTER 4

Virtualization

Virtualization Requirements

Detailed requirements for installing Unity Connection on a virtual machine are listed in the "Requirements for Installing Unity Connection on a Virtual Machine" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html

Scalability Differences between Physical and Virtual Configurations

The maximum number of ports, the maximum number of users with mailboxes, and other scalability specifications differ between comparable physical and virtual configurations. For detailed information, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Installing Unity Connection Cluster on Virtual Machines

Note the following about Unity Connection clusters and virtualization:

- You can install a Unity Connection cluster on two virtual machines, or you can install a cluster on one virtual machine and one physical machine.
- If you install a Unity Connection cluster on two virtual machines, the virtual machines must not be on the same blade. Ideally, the virtual machines are on separate chassis.
- If you install a Unity Connection cluster on one virtual machine and one physical machine, you should configure the virtual machine to match the specifications of the physical server for CPU, memory, and disk space. If disk space on the physical server and virtual machine do not match, Unity Connection uses

the smaller disk size to determine when the disk on which messages are stored has reached maximum capacity.

- For information on installing Unity Connection on physical hosts and on virtual machines, see the "Installing Cisco Unity Connection" chapter of the Install, Upgrade, and Maintenance Guide for *Cisco Unity Connection, Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Migrating Unity Connection from Physical Servers to Virtual Machines

Note the following about migrating Unity Connection from a physical server to a virtual machine:

- The physical hosts that are supported for use in a physical environment and those that are supported in a virtual environment are mutually exclusive. If you are currently running Unity Connection in a physical environment, you must replace the server. For information on physical hosts that are supported in a virtual environment, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.
- For information on migrating from physical servers to virtual machines, see the s" section of the "Maintaining Cisco Unity Connection Server" chapter of the Install, Upgrade, and Maintenance Guide for *Cisco Unity Connection, Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

CHAPTER 5

Networking

HTTPS Networking

Unity Connection supports HTTPS Networking, that allows you to connect different Unity Connection servers and clusters in a single site network. HTTP networking provides more scalable Unity Connection deployments as compared to legacy networking. The architecture of HTTPS networking is scalable both in terms of number of Unity Connection locations and the total directory size. HTTPS Protocol is used for directory synchronization within a network.

In addition to HTTPS networking, Unity Connection also supports legacy networking to connect multiple Unity Connection servers in a network. However, you should deploy a new network as per HTTPS networking. Legacy networking includes both intrasite (digital) and intersite networking.The legacy and HTTPS networking are not supported simultaneously in the same network. In legacy networking, SMTP is the method used within a site, and HTTPS is used in Intersite networking when linking two separate sites.

Designing a Unity Connection Network using HTTPS

When the messaging needs of your organization require more than one Unity Connection server or cluster, you need a way to combine multiple Unity Connection directories or to ensure that the connected servers can communicate with each other. The concept of networking, HTTPS Networking, is introduced to connect different Unity Connection servers and clusters in a network.

Note The legacy (SMTP) and new HTTPS networking are not supported simultaneously in the same network.

In hub-spoke topology, all the directory information among the spokes is shared through the hub(s) connecting the spokes. For example, in the above figure, if spoke A needs to synchronize directory information with spoke E, the directory information flows from spoke A to hub B, hub B to hub C, hub C to hub D, and then from hub D to spoke E.

Each Unity Connection server (or cluster) is represented in the network as a single Unity Connection location, which is created locally during installation and which cannot be deleted from the server itself. When you join the server (or cluster) to an existing location in a network, a Unity Connection location is automatically created for the server (or cluster).

Note In an HTTPS network the round-trip latency should not be more than 250 ms between Hub and Spoke nodes.

Note HTTPS networking supports single site networks only. You cannot connect multiple HTTPS networks or single site networks together to form a larger network. The maximum number of Unity Connection locations that you can connect in an HTTPS network is 25.

OVA Selection and HTTPS

When deciding which OVA template to deploy, it is important to determine the role of the servers in your environment relative to HTTPS networking. For example, if you are building a VPIM server to support 150,000 VPIM users, you would use the largest OVA template, and the server would only contain VPIM accounts, not subscribers.

Due to the limitations of the smaller OVA templates, you need to take careful consideration of growth as well as whether the node is a hub or spoke in the network when choosing your OVA. If your network size grows past the directory size limits of your chosen OVA, you need to rebuild or replace your servers with larger Novas to accommodate the larger directory size. It is a good idea to select a larger template than you think you need for just this reason. The smallest OVA template, in most cases, should only be used for spoke servers in the network.

For information about the maximum number of locations and other directory objects supported in a Unity Connection site, see the “Directory Object Limits” section in the System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html

Migrating from Legacy (SMTP) Networking to HTTPS Networking

Currently, the only supported method of migrating from legacy networking to HTTPS networking is a manual method. In the future, there is a migration tool available to make the process easier. The migration method is outlined in the HTTPS Networking Guide for Cisco Unity Connection , Release 11.x.

For information about the migration method, see the “Migration from Legacy network to HTTPS Network” chapter in the *HTTPS Networking Guide for Cisco Unity Connection , Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/https_networking/guide/b_11xcuchttpsnet.html.

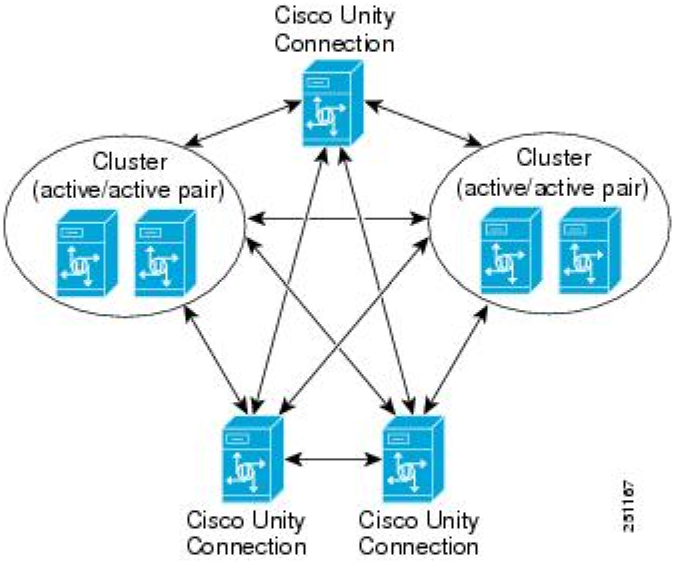
Legacy Networking

Intrasite Networking

If your organization has more users than a single Unity Connection server or cluster pair can support, you can join two or more Connection servers or clusters (up to a maximum of ten) to form a well-connected network, referred to as a Connection site. The servers that are joined to the site are referred to as locations. (When a Connection cluster is configured, the cluster counts as one location in the site.) Each location is said to be linked to every other location in the site via an intrasite link. Figure 5-2 illustrates a site of five Connection locations joined by intrasite links.

Intrasite networking is not supported for use with Cisco Business Edition 5000 and is supported only with Cisco Business Edition 6000/7000.

Figure 1: A Cisco Unity Connection Site Joined by Intrasite Links Among Locations



Within a site, Unity Connection locations automatically exchange directory information, so that a user on one location can dial out to or address messages to a user on any other system by name or extension, provided that the target user is reachable in the search scope of the originating user. The networked systems function as though they share a single directory. Users do not need to know where another user is located; they need only the name or extension number to address a message to any user or system distribution list in the directory.

Because intrasite links use SMTP transport for both directory replication and message transport, Unity Connection locations in a site can be deployed across geographic boundaries. Each server that is joined to the site must be able to access all other servers in the site directly through TCP/IP port 25, or SMTP messages must be routable among the servers through an SMTP smart host.

If your site includes a Unity Connection cluster, you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

In a site, each Unity Connection object is created and homed on a single Unity Connection location. An object can only be modified or deleted on the location where it was created. Each location has its own directory of users and other objects, and replicates a subset of these objects and their properties to other locations.

The following objects are replicated in a Unity Connection site:

- Users
- Administrator-defined contacts (including those associated with a VPIM location)
- System distribution lists (including membership)
- Locations (Unity Connection and VPIM)
- Partitions
- Search spaces
- Recorded voice names

For information about the maximum number of locations and other directory objects supported in a Unity Connection site, see the “Directory Object Limits” section in the System Requirements for Cisco Unity Connection, Release 11.x, at https://www-author.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html

You can also optionally deploy additional cross-server features between locations in a site. Cross-server sign in allows all users to dial the same number when calling from outside the organization to sign in to Unity Connection, regardless of which Unity Connection server they are homed on. Cross-server transfer enables calls from the automated attendant of one Unity Connection location to be transferred to a user on another networked Unity Connection location, according to the call transfer and screening settings of the called user. When you enable cross-server transfer, cross-server live reply is also enabled, allowing users to return calls to message senders who are users on other networked Unity Connection locations, according to the call transfer and screening settings of the called user.

The Unity Connection site concept was known as a Digital Network in release 7.x. You can join 7.x locations, 8.x locations, and 9.x locations, 10.x locations and, 11.x locations in the same Unity Connection site, as long as you do not link the site to any other site.

For more information on intrasite networking, see the “Overview of Networking Concepts” chapter of the *Networking Guide for Cisco Unity Connection, Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html.

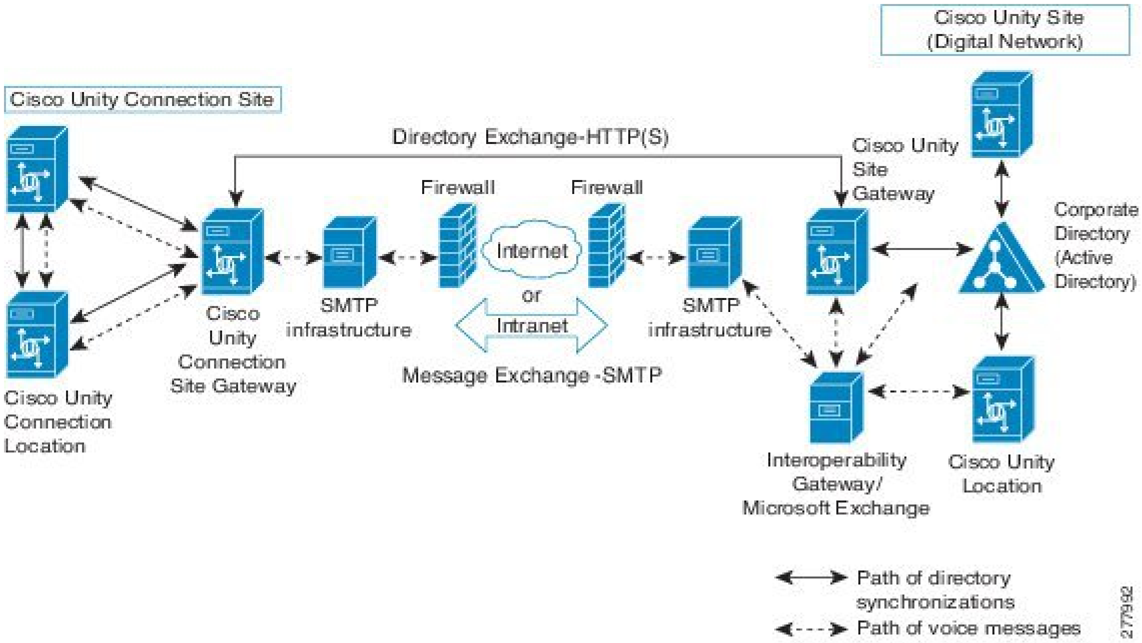
Intersite Networking between Two Unity Connection Sites

You can use an intersite link to connect one Unity Connection site to another Unity Connection site, allowing you to scale your organization from a maximum of ten locations to a maximum of twenty. The linked sites are referred to as a Cisco Voicemail Organization.

To create an intersite link, you select a single location from each site to act as a gateway to the other site. All directory synchronization communications and voice messages pass between the two site gateways, thereby limiting the connectivity requirements and bandwidth usage to the link between those two site gateway locations. The gateways use the HTTPs protocol to exchange directory synchronization updates. Intersite voice messages are transmitted and received via SMTP.

Figure 5-3 illustrates the role of the site gateways and the intersite link in connecting two Connection sites.

Figure 2: Cisco Voicemail Organization Consisting of Two Unity Connection Sites Linked via an Intersite Link


Cisco Unity Site (Digital Network)
Cisco Unity Connection Site
Directory Exchange-HTTP(S)
Cisco Unity Site Gateway
Firewall
Firewall
Internet
or
Intranet
Corporate Directory (Active Directory)
Cisco Unity Connection Site Gateway
SMTP infrastructure
SMTP infrastructure
Message Exchange -SMTP
Cisco Unity Connection Location
Interoperability Gateway/ Microsoft Exchange
Cisco Unity Location
Path of directory synchronizations
Path of voice messages
277992

Only one intersite link is supported per site. (This restriction applies to all types of intersite links, so you cannot link a Unity Connection site to another Unity Connection site and also to a Cisco Unity site.) In order to link a Unity Connection site to another site, all Unity Connection locations in the site must be running Unity Connection release 8.0 or later. Intersite Networking is not supported for use with Cisco Business Edition.

As with intrasite networking, users, system distribution lists, partitions, search spaces, and Unity Connection locations are replicated between sites. (System distribution list replication is optional.) However, contacts, system distribution list membership, and VPIM locations are not replicated between sites. Also, site gateways do not relay VPIM messages to other sites. Therefore, to deploy VPIM in the entire organization, you must independently configure each site for VPIM.

All of the optional cross-server features that are available within a Unity Connection site (cross-server sign in, cross-server transfers, and cross-server live reply) are also available between sites.

When you use a Unity Connection cluster as a site gateway, only the publisher server in the cluster participates in directory synchronization over the intersite link. However, the subscriber server can continue to provide message exchange over the intersite link if the publisher server is down. Note that in this configuration you must have a smart host available to resolve the SMTP domain of the cluster to both the publisher and subscriber servers in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down.

For more information on intersite networking, see the "Overview of Networking Concepts" chapter of the *Networking Guide for Cisco Unity Connection, Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html.

Intersite Networking between Unity Connection and Cisco Unity

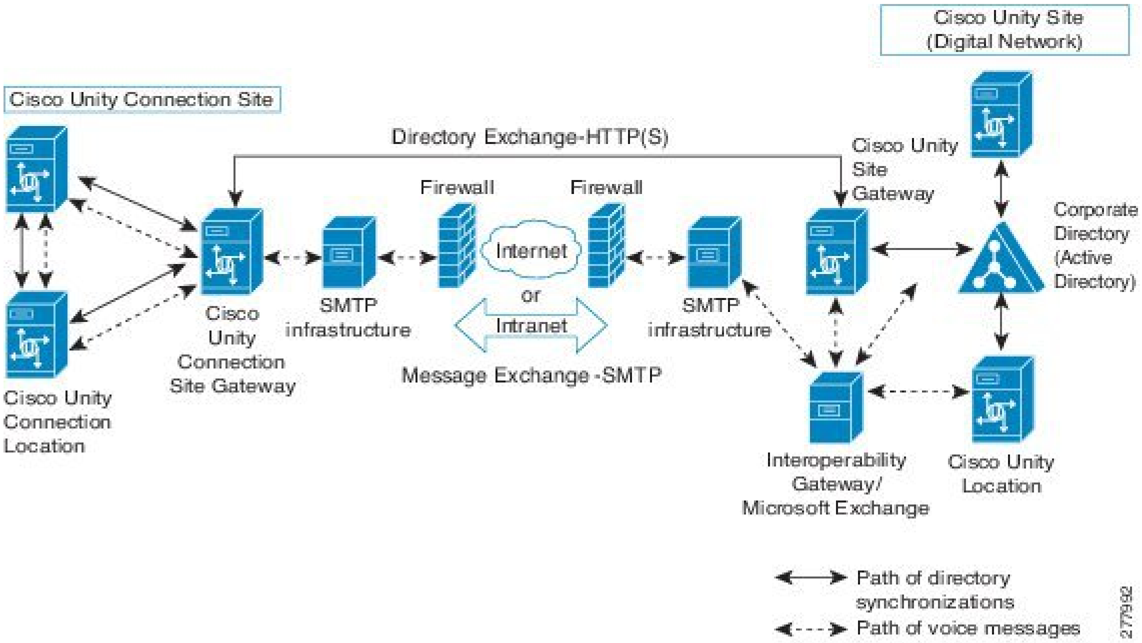
Unity Connection introduces a new option for internetworking Unity Connection and Cisco Unity servers—you can use intersite networking to connect a Unity Connection server, cluster, or site to a Cisco Unity server, failover pair, or digital network. The network of Unity Connection and Cisco Unity servers is referred to as a Cisco Voicemail Organization.

When you link a Cisco Unity site to a Unity Connection site, the gateway for each site is responsible for collecting information about all changes to the local site directory, and for polling the remote site gateway periodically to obtain information about updates to the remote site directory. The gateways use the HTTPs protocol to exchange directory synchronization updates.

For message exchange, the Interoperability Gateway for Microsoft Exchange functions as the messaging gateway for the Cisco Unity site. The Interoperability Gateway can be installed on Microsoft Exchange 2007 server configured with the Hub Transport role. (For up-to-date version support and requirements for the Interoperability Gateway, see the *Networking Options Requirements for Cisco Unity (Version 5.x and Later)* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.)

Figure 5-4 depicts—at a high level—the role of the Interoperability Gateway for Microsoft Exchange, the site gateways, and the intersite link in connecting Unity Connection and Cisco Unity sites.

Figure 3: Cisco Voicemail Organization Consisting of a Unity Connection Site Linked to a Cisco Unity Site


Cisco Unity Site
(Digital Network)
Cisco Unity Connection Site
Directory Exchange-HTTP(S)
Cisco Unity Site Gateway
Firewall
Firewall
Internet
or
Intranet
Corporate Directory (Active Directory)
Cisco Unity Connection Site Gateway
SMTP infrastructure
SMTP infrastructure
Message Exchange -SMTP
Cisco Unity Connection Location
Interoperability Gateway/ Microsoft Exchange
Cisco Unity Location
Path of directory synchronizations
Path of voice messages
277992

Note that in order to link Cisco Unity and Unity Connection sites, all servers in the Unity Connection site must be running Unity Connection 11.x. Intersite Networking is not supported for use with Cisco Business Edition.

The Cisco Unity site gateway must be running Cisco Unity 11.x. Other Cisco Unity servers in the Cisco Unity site may be running Cisco Unity 7.0 and later with Microsoft Exchange provided that the applicable engineering special is installed to add Unity Connection Networking support. For additional details and requirements for Cisco Unity, see the *Networking Options Requirements for Cisco Unity (Version 5.x and Later)* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.

When you link a Cisco Unity site and a Unity Connection site, a contact is added to the Cisco Unity directory and to Active Directory for each Unity Connection user. Likewise, a user is added to the Connection site global directory for each Cisco Unity user. Connection system contacts and VPIM contacts are not replicated to Cisco Unity, nor are Cisco Unity networking contacts (AMIS, Bridge, VPIM, Internet, or Trusted Internet subscribers) replicated to Unity Connection. Also, the site gateways do not relay messages for other types of networking (AMIS, Bridge, VPIM, and so on) across the intersite link. To deploy VPIM in the entire organization, you must independently configure each site for VPIM.

You can choose whether to replicate system distribution lists between sites, and choose which lists to replicate. Lists that contain system contacts or networking contacts cannot be configured to allow replication to other sites. For those lists that are replicated, only the list name and other information used in addressing are replicated; list membership is not replicated.

All of the optional cross-server features that are available within a Unity Connection site or Cisco Unity Digital Network (cross-server sign in, cross-server transfers, and cross-server live reply) are also available between the sites.

When you use a Unity Connection cluster as the Unity Connection site gateway, only the publisher server in the cluster participates in directory synchronization with Cisco Unity. However, the subscriber server can continue to provide message exchange over the intersite link if the publisher server is down. Likewise, when you use a Cisco Unity failover pair as the Cisco Unity site gateway, only the primary Cisco Unity server participates in directory synchronization with Unity Connection, although message exchange can continue even when the secondary Cisco Unity server is active.

For more information on intersite networking, see the "Overview of Networking Concepts" chapter of the *Networking Guide for Cisco Unity Connection, Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/11xcucnetx.html.

Designing a Unity Connection Network with Intrasite and Intersite Links

If you have a requirement to mix Unity Connection servers running releases 7.x, 8.x, 9.x, 10.x, and 11.x, or if you have more than 10 locations to network, the design is fairly straightforward—you must use only intrasite links if mixing release versions, and you must use a combination of intrasite links and an intersite link if you have more than 10 locations. However, if you have up to 10 Unity Connection locations and have the flexibility to run version 10.x on all of them, you can choose whether to link all locations in the same Connection site or to create two sites and link them together.

Table 5-1 helps you compare and contrast the benefits and drawbacks of each type of link.

Table 2: Intrasite Networking Versus Intersite Networking

	Intrasite Networking	**Intersite Networking**
Benefits	• Easider to administer: ◦ System distribution list membership is replicated throughout the site, so you do not have to decide which site should home a list. ◦ For each remote messaging server that you connect to via VPIM, you only have to configure VPIM location details once. • The message recall feature works across all locations in the site. • You can mix Unity Connection release 7.x, 8.x, 9.x, 10.x, and 11.x servers. • You have the flexibility to add an intersite link to a Cisco Unity Digital Network or to another Unity Connection site in the future.	• Supports up to 20 locations (in combination with intrasite networking). • Requires less bandwidth than intrasite networking for replication traffic over the intersite link, particularly if there are many locations on each side of the link. ◦ Data is replicated once between the gateways over the link rather than being replicated directly to all nodes in the network. ◦ System distribution list membership is not replicated across the link. ◦ Replication can be scheduled to occur only during off-hours. ◦ The intersite link uses a synchronous protocol that is more bandwidth-efficient than SMTP.
Drawbacks	• Requires higher bandwidth for replication than intersite networking. • Supports only up to 10 locations.	• Requires more administrative overhead, especially when both sites must be configured for VPIM locations. • Message recall does not work between sites. • All locations must be running Unity Connection release 11.x. • Does not allow for linking to a Cisco Unity Digital Network.

Note Dispatch messaging does not work between locations either within the same site or across sites.VPIM Networking

VPIM Networking

Cisco Unity Connection 10.x supports the Voice Profile for Internet Mail (VPIM) protocol, which is an industry standard that allows different voice messaging systems to exchange voice and text messages over the Internet or any TCP/IP network. VPIM is based on the Simple Mail Transfer Protocol (SMTP) and the Multi-Purpose Internet Mail Extension (MIME) protocols.

Unity Connection supports internetworking with voice messaging systems that support the VPIM version 2 protocol, as defined in Internet RFC 3801. For a list of messaging systems that are supported by Unity Connection for VPIM networking, see the "Requirements for VPIM Networking " section in the System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Each Unity Connection server, cluster pair, or site has a maximum number of VPIM locations and VPIM contacts that it can support. For limit information, see the " Directory Object Limits for Unity Connection " section in the System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html. When intrasite networking is configured, VPIM location and contact information is replicated to all locations in the site. If you deploy both VPIM and intrasite networking, you should designate a single Unity Connection location in the site as the bridgehead to handle the configuration of VPIM locations and contacts. Managing these objects from a single location simplifies maintenance tasks and avoids potential overlaps in contact information that could cause confusion to users when they attempt to address messages. VPIM locations and contacts are not replicated over intersite links, and site gateways do not relay VPIM messages to other sites. Therefore, if you deploy VPIM in a Cisco Voicemail Organization consisting of two Unity Connection sites or of a Unity Connection site and a Cisco Unity site, you must independently configure each site for VPIM.

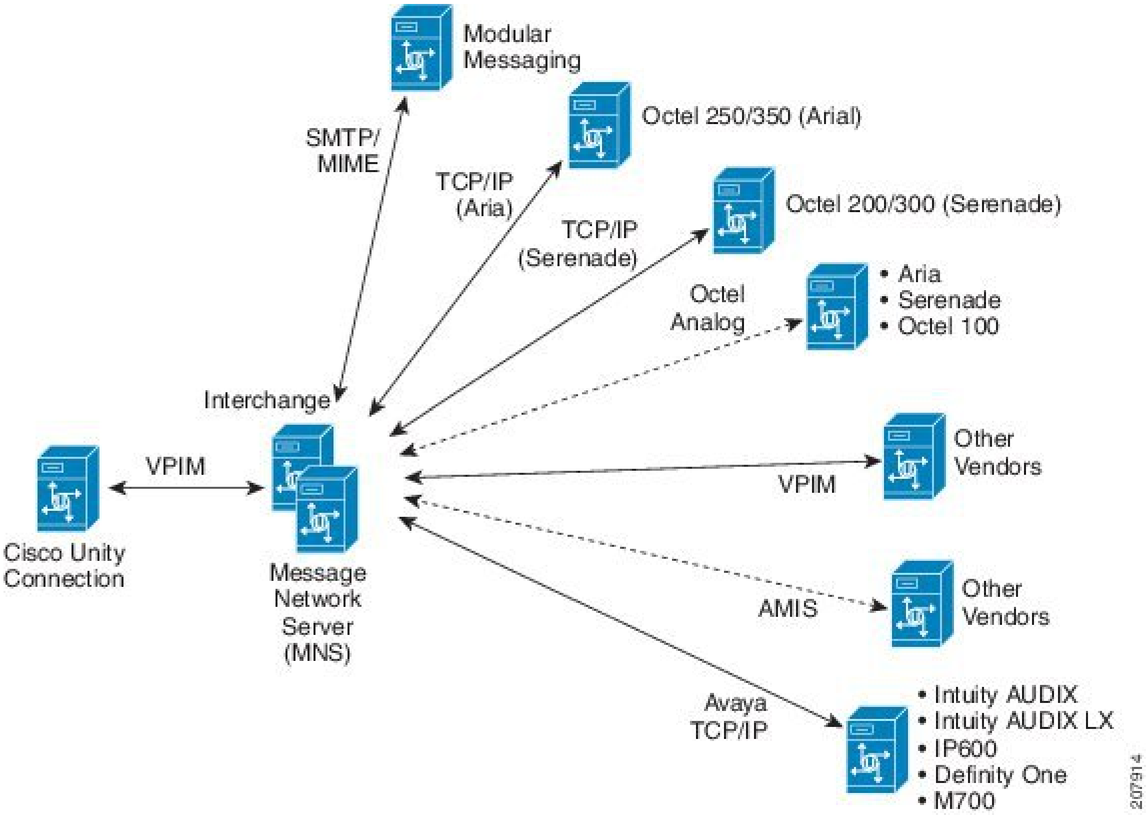
To internetwork with more VPIM locations than your server, cluster, or site can support, you can use the Cisco Unified Messaging Gateway (Cisco UMG). The Cisco UMG is configured as a single VPIM location in Unity Connection, and acts as a central hub to handle message routing and delivery to other systems (Cisco Unity, Cisco Unity Connection, Cisco Unity Express, or Avaya Message Networking solution/Interchange) that are connected to it.

For more information on VPIM Networking, design considerations, and configuration details, see the " VPIM Networking " chapter of the Networking Guide for Cisco Unity Connection Release 11.x, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html

Using VPIM between Unity Connection and Avaya Message Networking Solution or Avaya Interchange

The Avaya Message Networking solution (or the Avaya Interchange) uses a hub-and-spoke topology to allow voice messaging between systems, using a number of protocols, thus allowing a voice messaging system such as Cisco Unity Connection to send and receive network voice messages with any other system in the network. Unity Connection uses the VPIM protocol to communicate with the Interchange, and the Interchange takes care of routing the messages to and from other systems on the network using the applicable protocol. Figure 5-5 illustrates an example topology.

Figure 4: Cisco Unity Connection Communicates with the Avaya Message Network Solution



Survivable Remote Site Voicemail

Cisco Unity Connection Survivable Remote Site Voicemail (Unity Connection SRSV) is a backup voicemail solution that works in conjunction with Cisco Unified Survivable Remote Site Telephony (SRST) for providing voicemail service to a branch during WAN outages.

Unity Connection SRSV is used in the centralized Cisco Unified Communications Manager and Cisco Unity Connection environment with multiple branch offices or small sites. It provides limited voicemail and auto-attendant features that remain in synchronization with the central Unity Connection voicemail service so that when the WAN outage or failure occurs, the Unity Connection SRSV solution can provide voicemail service to the subscribers at the branch. However, as soon as the network is restored, all the voicemails received by the branch subscribers are automatically uploaded to the central Unity Connection voicemail server.

For more information on how to configure Unity Connection SRSV at branch location Unity Connection, see the guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/srsv/guide/b_11xcucsrsvx.html

CHAPTER 6

Single Inbox

About Single Inbox

Single inbox, one of the unified messaging features in Unity Connection, synchronizes voice messages in Unity Connection and Exchange mailboxes. When a user is enabled for single inbox, all Unity Connection voice messages that are sent to the user, including those sent from Cisco Unity Connection ViewMail for Microsoft Outlook, are first stored in Unity Connection and are immediately replicated to the user's Exchange mailbox. In addition, status changes (for example, from unread to read), changes to the subject line, and changes to the priority are replicated from Unity Connection to Exchange and vice versa, as applicable. For a detailed explanation and configuration of single inbox functionality, see the "Configuring Unified Messaging" chapter in the *Unified Messaging Guide for Cisco Unity Connection, Release 11.x,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

For Unity Connection system requirements for single inbox, see the "Unified Messaging Requirements: Synchronizing Unity Connection and Exchange Mailboxes" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

You can configure Connection to synchronize voice messages between Unity Connection mailboxes and the corresponding Office 365 mailboxes. When single inbox is enabled for a user, all voice messages, including those sent from Cisco ViewMail for Microsoft Outlook, are first stored in Connection and are immediately replicated to the Office 365 mailbox for the recipient. Voice messages appear in the Outlook inbox for the user alongside email and faxes, and also appear in the Connection mailbox for the user.

The synchronization of voice messages in Unity Connection and Exchange mailboxes (single inbox) supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Unity Connection platform is configured in dual (IPv4/IPv6) mode.

Note Single Inbox over IPv6 is supported only for Office 365, Exchange 2007, Exchange 2010, and Exchange 2013.

Unified Messaging Services and Unified Messaging Accounts

When you configure unified messaging, including single inbox, you add one or more unified messaging services on each Unity Connection server. Each unified messaging service specifies:

- Which Exchange servers you want to access
- Which unified messaging features you want to enable

When you add unified messaging services, consider the following:

- Settings for unified messaging services allow you either to configure Unity Connection to communicate with a specific Exchange server, or configure Unity Connection to search for Exchange servers. If you have more than a few Exchange servers, you should use the option to search for Exchange servers. If you configure Unity Connection to communicate with specific Exchange servers, you must do the following:
    - Add another unified messaging service whenever you add another Exchange server.
    - Change Unity Connection user settings whenever you move Exchange mailboxes from one Exchange server to another.
- There is no hard limit on the number of unified messaging services that you can create, but maintenance becomes time-consuming when you create more than a couple of dozen.
- To enable unified messaging features for Unity Connection users, you add one or more unified messaging accounts for each user. For each unified messaging account, you specify a unified messaging service, which determines which unified messaging features the user can use.
- If you do not want all users to have access to all unified messaging features, you can create multiple unified messaging services that enable different features or different combinations of features. For example, you might configure one unified messaging service that enables text to speech (TTS), another that enables access to Exchange calendars and contacts, and a third that enables single inbox. With this design, if you want a user to have access to all three features, you would create three unified messaging accounts for the user, one for each of the three unified messaging services.

You cannot create two unified messaging accounts that enable the same feature for the same user. For example, suppose you add two unified messaging services:

- One enables TTS and access to Exchange calendars and contacts.
- The other enables TTS and single inbox.

If you create two unified messaging accounts for the user with the goal of giving the user access to all three features, you must disable TTS in one of the unified messaging accounts.

Associating Exchange Email Addresses with Users

Unity Connection figures out who the sender and recipient are for Unity Connection voice messages that are sent using ViewMail for Outlook doing the following:

- When you install Cisco Unity Connection ViewMail for Microsoft Outlook version 8.5 or later, you specify the Unity Connection server on which the user's Unity Connection mailbox is stored. ViewMail for Outlook always sends new voice messages, forwards, and replies to that Unity Connection server.
- When you configure single inbox for a user, you specify:
    - The user's Exchange email address. This is how Unity Connection knows which Exchange mailbox to synchronize with. You can choose to have Unity Connection automatically create an SMTP proxy address for the user using the Corporate Email Address field in Unity Connection Administration.
    - An SMTP proxy address for the user, which is typically the user's Exchange email address. When the user sends a voice message using ViewMail for Outlook, the From address is the sender's Exchange email address, and the To address is the recipient's Exchange email address. Unity Connection uses the SMTP proxy address to associate the From address with the Unity Connection user who sent the message and the To address with the Unity Connection user who is the intended recipient.

Integrating Unity Connection with Active Directory can simplify populating Unity Connection user data with Exchange email addresses. For more information, see the Active Directory Considerations for Single Inbox, on page 54.

Deploying Single Inbox

How you deploy Unity Connection depends on the Unity Connection configuration. See the applicable section:

Deploying Single Inbox for One Unity Connection Server

In a deployment that includes one Unity Connection server, the server connects with one or a few Exchange servers. For example, you can configure a Unity Connection server to access mailboxes on an Exchange 2007, Exchange 2010, or Exchange 2013 server.

Deploying Single Inbox for a Unity Connection Cluster

You deploy a Unity Connection cluster much the same way you deploy a Unity Connection server. Configuration data is replicated between the two servers in the cluster, so you can change configuration settings on either server. Note that the Unity Connection Mailbox Sync service, which is required for single inbox to function, runs only on the active server and is considered a critical service. If you stop this service, the active server fails over to the secondary server, and the Unity Connection Mailbox Sync service starts running on the new acting primary server.

If there are IP restrictions on the network, such as a firewall, consider the connectivity of both Unity Connection servers to the Exchange servers.

Deploying Single Inbox for a Unity Connection Intrasite Network

Unified messaging services are not replicated among Unity Connection servers in an intrasite network, so they must be configured separately on each server in the network.

Deploying Single Inbox During Gradual Migrations from Cisco Unity

We discourage gradual migrations in general because the process is complex and time consuming. We further discourage migrating messages during a gradual migration because users who are being migrated encounter some behaviors that are confusing and atypical of Unity Connection. For more information, see the "Moving Mailboxes between Mailboxes Stores" section of the "Message Storage" chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x, available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Single Inbox Affecting Scalability

Single Inbox does not affect the number of user accounts that can be homed on a Unity Connection server.

Allowing Unity Connection or Exchange mailboxes larger than 2 GB can affect Unity Connection and Exchange performance.

Network Considerations for Single Inbox

Firewalls

If a Unity Connection server is separated by a firewall from Exchange servers, you must open the applicable ports in the firewall. If a Unity Connection cluster is configured, you must open the same ports in the firewall for both Unity Connection servers. For more information, see the "IP Communications Required by Cisco Unity Connection" chapter of the Security Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html

Bandwidth

For bandwidth requirements for single inbox, see the "Unified Messaging Requirements: Synchronizing Unity Connection and Exchange Mailboxes" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Latency

Latency is closely intertwined with the number of connections (also known as synchronization threads or threads) that Unity Connection uses to synchronize Unity Connection and Exchange mailboxes. In a low-latency environment, fewer connections are required; conversely, in a high-latency environment, more connections are required to keep up with the number of operations that need to be synchronized to Exchange.

If you do not have enough connections, users experience delays in synchronizing messages and in synchronizing message changes between Unity Connection and Exchange (for example, turning message waiting indicators off when the last voice message has been heard). However, configuring more connections is not necessarily better. In a low-latency environment, a busy Unity Connection server with a large number of connections to Exchange may significantly increase the processor load on the Exchange servers.

Note For better user experience, the round trip latency between Unity Connection and Office 365 server should not be more than 250 ms.

See the following sections for calculating the number of connections needed:

Calculating the Number of Connections for One Unity Connection Server

If you have one Unity Connection server with 2,000 or fewer users, and if round-trip latency between the Unity Connection and Exchange or Office 365 servers is 80 milliseconds or less, do not change the number of connections unless you encounter synchronization delays. The default setting of four connections are sufficient in most environments to ensure good single-inbox synchronization performance.

If you have one Unity Connection server with more than 2,000 users or more than 80 milliseconds of round-trip latency, use this formula to calculate the number of connections:

Number of connections = (Number of Unity Connection single-inbox users * (latency in milliseconds + 15)) / 50,000

If you have more than one Exchange or Office 365 CAS server, the number of Unity Connection single-inbox users is the largest number of single-inbox users who are assigned to one CAS server or CAS array. For example, suppose your Unity Connection server has 4,000 users and they are all single-inbox users. You have three Exchange or Office 365 CAS servers, with 2,000 users on one CAS server and 1,000 users on each of the other two CAS servers. For this calculation, the number of Unity Connection single-inbox users is 2,000.

Note The maximum number of connections is 64. Never reduce the number of connections to fewer than four.

For example, if your Unity Connection server has 2,000 users and 10 milliseconds of latency, and all of the mailboxes are homed on one Exchange or Office 365 server, you would not change the number of connections:

Number of connections = (2,000 * (10 + 15)) / 50,000 = 50,000 / 50,000 = 1 connection (no change to the default value of four connections)

If your Unity Connection server has 2,000 single-inbox users and 100 milliseconds of latency, and all of the mailboxes are homed on one Exchange or Office 365 server, you would increase the number of connections to 5:

Number of connections = (2,000 * (100 + 15)) / 50,000 = 230,000 / 50,000 = 4.6 connections

Note This formula is based on conservative assumptions about user activity, and about Unity Connection and Exchange or Office 365 performance, but the assumptions may not be true in all environments. For example, if you are experiencing single-inbox synchronization delays after setting the number of connections to the calculated value, and if the Exchange servers have available CPU, you may want to increase the number of connections beyond the calculated value.

Calculating the Number of Connections for a Unity Connection Cluster

If both Unity Connection servers in a cluster are in the same location, so they have the same latency when synchronizing with Exchange or Office 365, you can calculate the number of connections the same way you do for one Unity Connection server.

If one server in a cluster is collocated with the Exchange or Office 365 servers and the other is in a remote location:

- Install the publisher server in the location with the Exchange or Office 365 servers. The publisher server should always be the primary server unless the server is offline for maintenance or is unavailable for some other reason.
- Calculate the number of connections for the publisher server, meaning the Unity Connection server with lower latency. If you calculate for the server with higher latency, during peak usage, synchronization may increase the processor load on the Exchange or Office 365 CAS servers to unacceptable levels.

When the remote server becomes the active server, for example, because you are upgrading Unity Connection, you may encounter significant synchronization delays. When you calculate the number of connections for the Unity Connection server that is collocated with Exchange, you are optimizing for the server with lower latency. This number of connections may not be able to keep up with the number of operations that need to be synchronized to Exchange or Office 365. The maintenance operations that require activating the subscriber server should be performed during non-business hours and you should limit the amount of time that the subscriber server is the active server.

Calculating the Number of Connections for a Unity Connection Server Synchronizing with an Exchange CAS Array

Unity Connection is most likely to require a large number of connections with Exchange or Office 365 when connecting with a large CAS array. For example, when the Unity Connection server has 12,000 single-inbox users and the latency is 10 milliseconds, you would increase the number of connections to six:

Number of connections = (12,000 * (10 + 15)) / 50,000 = 300,000 / 50,000 = 6 connections

If your Exchange environment includes both a large CAS array and one or more Exchange or Office 365 servers that are not in the array, and if the calculated number of connections for the CAS array differs significantly from the number of connections for the individual Exchange or Office 365 servers, you may want to consider adding a Unity Connection server that is dedicated to the separate Exchange or Office 365 servers. Setting the number of connections to the lower value for the standalone Exchange or Office 365 server means synchronization delays for the CAS array, while setting the number of connections to the higher value for the CAS array means a higher processor load on the standalone Exchange or Office 365 servers.

Increasing the Number of Connections

If you have more than 2000 users on a Unity Connection server or more than 80 milliseconds of latency, you can increase the number of connections from the default value of four. Note the following:

- The maximum number of connections is 64.
- Never decrease the number of connections to fewer than four.
- After you change the number of connections, you must restart the Unity Connection Mailbox Sync service in Cisco Unity Connection Serviceability for the change to take effect.

- As Unity Connection is optimized in future versions, the optimum number of the connections for a specific environment may change.
- If you have more than one Unity Connection server synchronizing with the same Exchange server or CAS array, you may increase the processor load on the Exchange CAS servers to unacceptable levels.

To increase the number of connections that Unity Connection uses for synchronizing with each Exchange server, run the following CLI command (when a Unity Connection cluster is configured, you can run the command on either server):

run cuc dbquery unitydirdb EXECUTE PROCEDURE csp_ConfigurationModifyLong (pFullName='System.Messaging.MbxSynch.MbxSynchThreadCountPerUMServer', pValue=<value>)

where <*value*> is the number of connections that you want Unity Connection to use.

To determine the current number of connections that Unity Connection is configured to use, run the following CLI command:

run cuc dbquery unitydirdb select fullname, value from vw_configuration where fullname = 'System.Messaging.MbxSynch.MbxSynchThreadCountPerUMServer'

Load Balancing

By default, the Unity Connection Mailbox Sync service uses four threads (four HTTP or HTTPS connections) for each CAS server or CAS array that Unity Connection is configured to synchronize with. Note the following:

- The threads are torn down and recreated every 60 seconds.
- All of the requests come from the same IP address. Configure the load balancer to distribute load from the same IP address to multiple servers in the CAS array.
- Unity Connection does not maintain session cookies between requests.
- If the load balancer for the existing CAS array does not produce the desired result with the load profile that the Unity Connection Mailbox Sync service puts on it, you can set up a dedicated CAS server or CAS array to handle the Unity Connection load.

Note Cisco Unity Connection is not responsible for troubleshooting the load balancer issues as it is an external third party software. For further assistance, please contact the Load Balancer support team.

Microsoft Exchange Considerations for Single Inbox

Unified Messaging Services Account Accessing Exchange Mailboxes

Single inbox and the other unified messaging features require that you create an Active Directory account (called the unified messaging services account throughout the Unity Connection documentation) and grant the account the rights necessary for Unity Connection to perform operations on behalf of users. No user credentials are stored in the Unity Connection database; this is a change from Unity Connection 8.0, for which

TTS access to Exchange email and access to Exchange calendars and contacts required that you enter each user’s Active Directory alias and password.

Using the unified messaging services account to access Exchange mailboxes simplifies administration. However, you must secure the account to prevent unauthorized access to Exchange mailboxes.

The operations that the account performs and the permissions that the account requires are documented in the “Configuring Unified Messaging” chapter in the *Unified Messaging Guide for Cisco Unity Connection, Release 11.x,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

Deploying Exchange Servers

We tested single-inbox with Exchange using standard Exchange deployment practices, which are thoroughly documented on the Microsoft website. If you are not following Microsoft deployment guidelines for Active Directory and Exchange, you should enable single inbox gradually, for small groups of users, and closely monitor Active Directory and Exchange performance as you add more single-inbox users.

Mailbox-Size Quotas and Message Aging

By default, when a user deletes a voice message in Unity Connection, the message is sent to the Unity Connection deleted items folder and synchronized with the Outlook Deleted Items folder. When the message is deleted from the Unity Connection deleted items folder (the user can do this manually, or you can configure message aging to do it automatically), it is also deleted from the Outlook Deleted Items folder.

If you are adding the single-inbox feature to an existing system, and if you have configured Unity Connection to permanently delete messages without saving them in the deleted items folder, messages that users delete using the Web Inbox or using the Unity Connection phone interface are still permanently deleted. However, messages that users delete using Outlook are only moved to the deleted items folder in Unity Connection, not permanently deleted. This is true regardless of which Outlook folder the message is in when the user deletes it. (Even when a user deletes a voice message from the Outlook Deleted Items folder, the message is only moved to the deleted items folder in Unity Connection.)

You should do one or both of the following to prevent the hard disk on the Unity Connection server from filling up with deleted messages:

- Configure mailbox-size quotas, so that Unity Connection prompts users to delete messages when their mailboxes approach a specified size.
- Configure message aging to permanently delete messages in the Unity Connection deleted items folder.

Note Beginning with Cisco Unity Connection 10.0(1) and later releases, when the mailbox size of a user starts reaching its specified threshold limit on Unity Connection, the user receives a quota notification message. For more information on mailbox quota alert text, see the “Controlling the Size of Mailboxes” section of the “Message Storage” chapter of the System Administration Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Coordinating Mailbox-Size Quotas and Message Aging Settings in Unity Connection and Exchange

You can configure mailbox-size quotas and message aging in Exchange just as you can in Unity Connection. When you are configuring single inbox, confirm that the mailbox-size quotas and message aging in the two applications do not conflict. For example, suppose that you configure Unity Connection to delete voice messages that are more than 14 days old, and you configure Exchange to delete messages that are more than 30 days old. A user who returns from a three-week vacation finds emails in the Outlook Inbox for the entire period but finds voice messages only for the last two weeks.

When you configure Unity Connection single inbox, you need to increase the mailbox-size quotas for the corresponding Exchange mailboxes. You should increase the quota for Exchange mailboxes by the size of the quota for Unity Connection mailboxes.

Note By default, Unity Connection allows outside callers to leave voice messages regardless of the mailbox-size quota for recipient mailboxes. You can change this setting when you configure system-wide quota settings.

Exchange can be configured to tombstone or retain messages that have been permanently deleted; when single inbox is configured, this includes Unity Connection voice messages in Exchange mailboxes. Ensure that this is the desired outcome for voice messages based on your enterprise policies.

Moving Exchange Mailboxes

If you configure unified messaging services to access specific Exchange servers, Unity Connection can only detect mailbox moves between Exchange servers for some versions of Exchange. In configurations in which Unity Connection cannot detect mailbox moves, when you move Exchange mailboxes between Exchange servers, you need to add new unified messaging accounts for the affected users and delete the old unified messaging accounts.

For the affected versions of Exchange, if you frequently move mailboxes between Exchange servers for load balancing, You should configure unified messaging services to search for Exchange servers. This allows Unity Connection to automatically detect the new location of mailboxes that have been moved.

For information on which versions of Exchange are affected, see the "Moving and Restoring Exchange Mailboxes" chapter of the Unified Messaging Guide for Cisco Unity Connection*, Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

Exchange Clustering

Unity Connection supports using single inbox with Exchange 2010 or Exchange 2013 Database Availability Groups (DAG) for high availability if the DAGs are deployed according to Microsoft recommendations. Unity Connection also supports connecting to a CAS array for high availability.

Exchange 2007 clustering has not yet been tested. When testing is complete and clustering support has been determined, the "Unified Messaging Requirements: Synchronizing Unity Connection and Exchange Mailboxes" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Single Inbox Affecting Exchange Performance

Single inbox has a minor effect on Exchange performance in direct relationship to the number of users. For more information, see the white paper at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps6509/solution_overview_c22-713352.html.

Exchange Autodiscover Service

If you configure unified messaging services to search for Exchange servers, do not disable the Exchange autodiscover service, or Unity Connection cannot find Exchange servers, and unified messaging features do not work. (The autodiscover service is enabled by default.)

Exchange Server 2010 and Exchange Server 2013

For information on Exchange Server 2010 and 2013 requirements when single inbox is configured, see the "Unified Messaging Requirements: Synchronizing Unity Connection and Exchange Mailboxes" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

When you are using Exchange 2010 or Exchange 2013, you need to:

- Assign the application impersonation management role to the unified messaging services accounts.
- Configure EWS limits for the unified messaging users (Exchange 2013 and Later).
- Configure EWS limits for the unified messaging users (Exchange 2010 SP2 RU4 and Later).
- Configure EWS limits for the unified messaging services accounts (Exchange 2010 SP2 RU3 and Earlier Releases).

Exchange Server 2007

When Exchange 2007 is supported:

- The "Unified Messaging Requirements: Synchronizing Unity Connection and Exchange Mailboxes" section of System Requirements for Cisco Unity Connection, Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.
- Unity Connection supports the single-inbox feature when Exchange mailboxes are homed on any combination of Exchange 2013, Exchange 2010, and Exchange 2007 servers.

When you are using Exchange 2007, you need to:

- Grant impersonation, may impersonate, and receive-as rights to the unified messaging services accounts.
- Grant unified messaging services accounts the permission to sign in locally.

Active Directory Considerations for Single Inbox

Note the following Active Directory considerations:

- Unity Connection does not require that you extend the Active Directory schema for single inbox.
- If the Active Directory forest includes more than ten domain controllers, and if you have configured Unity Connection to search for Exchange servers, you should deploy sites in Microsoft Sites and Services and that you follow Microsoft guidelines for geospatially separating domain controllers and global catalog servers.
- A Unity Connection server can access Exchange servers in more than one forest. You must create one or more unified messaging services for each forest.
- You can configure an LDAP integration with Active Directory for data synchronization and for authentication, although it is not required for single inbox or for any of the other unified messaging features.

If you have already configured an LDAP integration, you are not required to change the LDAP integration to use single inbox. However, if you synchronized the Cisco Unified Communications Manager Mail ID field with the LDAP sAMAccountName instead of with the LDAP mail field, you may want to change the LDAP integration. During the integration process, this causes values in the LDAP mail field to appear in the Corporate Email Address field in Unity Connection.

Unified messaging requires that you enter the Exchange email address for each Unity Connection user. On the Unified Messaging Account page, each user can be configured to use either of the following values:

- The Corporate Email Address specified on the User Basics page
- The email address specified on the Unified Messaging Account page

Automatically populating the Corporate Email Address field with the value of the LDAP mail field is easier than populating the email address field on the Unified Messaging Account page using Unity Connection Administration or the Bulk Administration Tool. With a value in the Corporate Email Address field, you can also easily add an SMTP proxy address, which is required for single inbox; see the Associating Exchange Email Addresses with Users section.

For more design guidance on integrating Unity Connection with Active Directory, see the LDAP Directory Integration with Cisco Unity Connection, on page 81 chapter.

For information on how to change LDAP directory configurations, see the “LDAP” chapter of the System Administration Guide for Cisco Unity Connection*, Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Using Secure Messaging with Single Inbox

If you do not want Unity Connection voice messages stored in Exchange or archived for discoverability or compliance reasons but you still want single-inbox functionality, you can configure secure messaging. Enabling secure messaging for selected users or for all users on a Unity Connection server prevents the recorded part of voice messages from being synchronized into the Exchange mailboxes for those users. Instead, Unity Connection sends a decoy message that tells users they have a voice message. If Cisco Unity Connection ViewMail for Microsoft Outlook version 8.5 is installed, the message is streamed directly from Unity Connection. If ViewMail for Outlook is not installed, the decoy message contains only an explanation of secure messages.

Client Access to Voice Messages in Exchange Mailboxes

You can use the following client applications to access Unity Connection voice messages in Exchange mailboxes:

Cisco Unity Connection ViewMail for Microsoft Outlook

When single inbox is configured, users have the best experience when they are using Microsoft Outlook for their email application and when Cisco Unity Connection ViewMail for Microsoft Outlook version 8.5 or later is installed. ViewMail for Outlook is an add-in that allows voice messages to be heard and composed from within Microsoft Outlook 2010 or 2007.

Versions of ViewMail for Outlook prior to 8.5 are not able to access voice messages that are synchronized into Exchange by the single inbox feature.

You can simplify the deployment of ViewMail for Outlook using mass-deployment technologies that use MSI packages. For information on customizing ViewMail for Outlook–specific settings, see the "Customizing ViewMail for Outlook Setup" section in the Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook *Release 8.5(3)* or later at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/vmo/release/notes/853cucvmorn.html.

When you enable single inbox (SIB) using unified messaging service, a new Voice Outbox folder appears under the Outbox folder in Outlook. Unity Connection creates this folder in Exchange and uses it to deliver voice messages to Unity Connection; this allows Unity Connection and ViewMail for Outlook to monitor a separate folder for delivery of voice messages.

Note When you move an email message from any Outlook folder to the Voicemail Outbox folder, the email message is moved to the Deleted Items folder. The user may retrieve that deleted email message from the Deleted Items folder.

For more information about ViewMail for Outlook, see:

- *Quick Start Guide for Cisco ViewMail for Microsoft Outlook (Release 8.5 and Later)* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/vmo/quick_start/guide/85xcucqsgvmo.html.
- Release Notes for Cisco Unity Connection ViewMail for Microsoft Outlook *Release 8.5(3)* or later at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/vmo/release/notes/853cucvmorn.html.

Web Inbox

The Unity Connection Web Inbox is a web application that allows users to hear and compose Unity Connection voice messages from any computer or device that has internet access to Unity Connection. Note the following:

- Web Inbox can be embedded into other applications as a gadget.
- For playback, Web Inbox uses HTML 5 for audio playback when .wav playback is available. Otherwise, it uses QuickTime.
- Cisco Unity Connection uses Flash Player for recording voice messages through Web Inbox. However, support of Flash Player will end soon. Hence Cisco Unity Connection 11.5(1) Service Update 8 and later,

replaces Flash Player with **Web Real-Time Communication(Web RTC)** to record voice messages using **HTML5** in Web Inbox. Web RTC provides web browsers and mobile applications with real-time communication (RTC) via simple application programming interfaces (APIs).

For more information on updates of the Flash Player refer https://www.adobe.com/products/flashplayer/end-of-life.html

- *(Applicable for 11.5(1) SU7 and earlier releases),* For recording on a computer Web Inbox uses a small Flash component. Users can also upload messages that were previously recorded.
- TRaP, or playback from a telephone integrated with a telephony integration can be used for playback or recording.
- New message notifications or events come through via Unity Connection.
- When the Web Inbox session is idle for longer than the 30 minutes, Connection disconnects the session. The session timeout settings are not reconfigurable.
- Web Inbox is hosted in the Tomcat application on Unity Connection.

Note Web Inbox supports both the IPv4 and IPv6 addresses. However, the IPv6 address works only when Connection platform is configured in Dual (IPv4/IPv6) mode.

For more information on Web Inbox, see *Quick Start Guide for Cisco Unity Connection Web Inbox* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/quick_start/guide/b_11xcucqsginbox.html

Blackberry and Other Mobile Applications

Note the following about using mobile clients to access Unity Connection voice messages:

- Mobile clients such as Blackberry devices are supported with single inbox.
- Clients that use Active Sync technology and can playback encoded .wav files are supported with single inbox. The encoding need to be known, because some codecs are not supported across all mobile devices.
- Cisco Mobility applications can be used to check voice mail directly in Unity Connection as in previous releases. However, these applications currently are not supported with single inbox.
- Mobile users can only compose voice messages if they have a Cisco Mobility application or if they call into the Unity Connection server.

IMAP Email Clients and Other Email Clients

If users use IMAP email clients or other email clients to access Unity Connection voice messages that have been synchronize to Exchange by the single-inbox feature, note the following:

- Unity Connection voice messages appear in the inbox as emails with .wav file attachments.
- To compose voice messages, users must either call into Unity Connection or use a recording device and an application that can produce .wav files.

- Replies to voice messages are not synchronized into the recipient’s Exchange mailbox.

Restoring Exchange Mailboxes with Single Inbox

If you need to restore one or more Exchange mailboxes, you must disable single inbox for the Unity Connection users whose mailboxes are being restored.

⚠

Caution If you do not disable single inbox for Unity Connection users whose Exchange mailboxes are being restored, Unity Connection do not resynchronize voice messages that were received between the time that the backup from which you are restoring was created and the time that the restore is complete.

For more information, see the “Moving and Restoring Exchange Mailboxes” chapter of the Unified Messaging Guide for Cisco Unity Connection*, Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/unified_messaging/b_11xcucumgx.html.

CHAPTER 7

Tenant Partitioning

If Unity Connection server is being shared by N (N=2, 3, 4….) tenants for voicemail service, each tenant can be setup as a separate "tenant" that is effectively isolated from other tenant hosted on the same server. Hence, a tenant entity refers to logical group of resources in Unity Connection assigned to a single company, where each tenant is assigned with only one partition, search space, and phone system.

Tenant partitioning also introduces the concept of using the corporate email addresses as their alias, which enables alias uniqueness across tenants. In addition, separate Unity Connection SMTP domain is provided for each tenant.

Tenant Partitioning

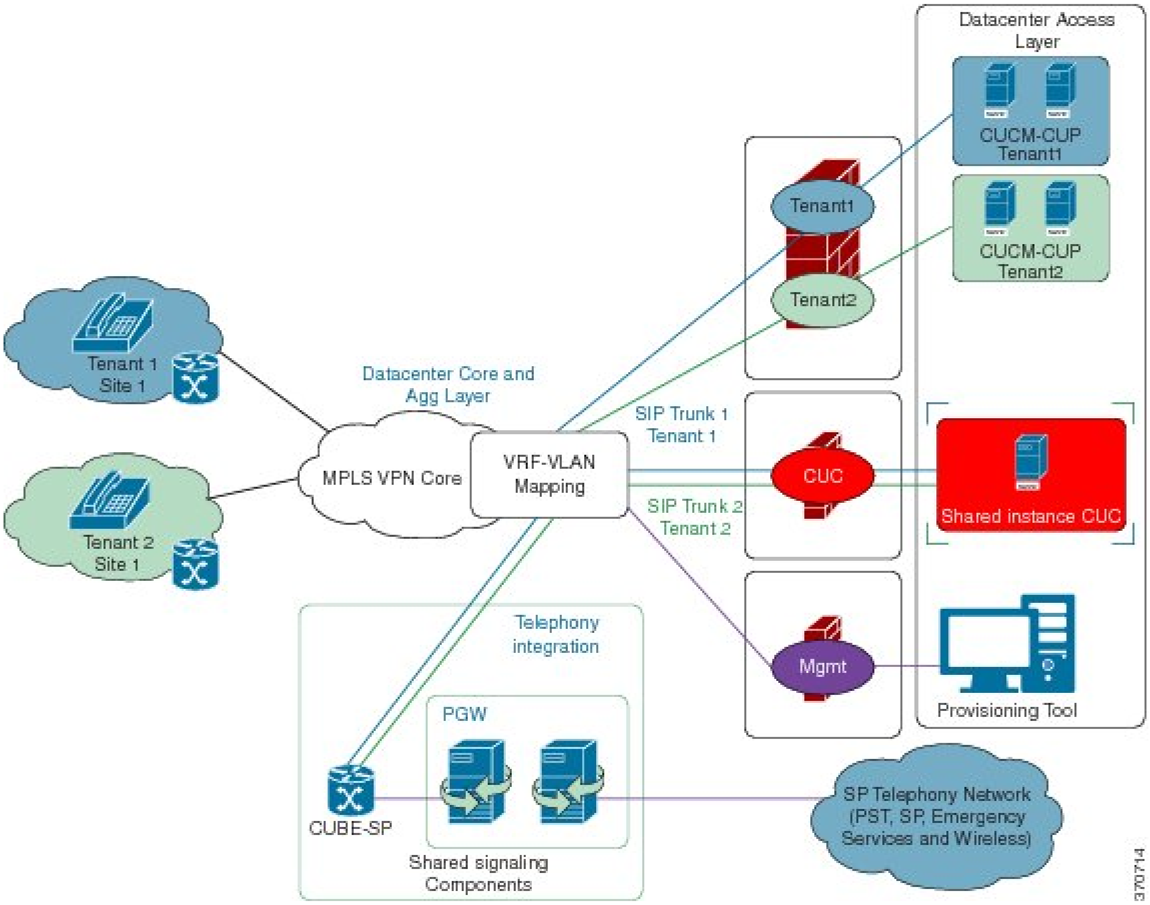
If Unity Connection server is being shared by N (N=2, 3, 4….) tenants for voicemail service, each tenant can be setup as a separate "tenant" that is effectively isolated from other tenant hosted on the same server. Hence, a tenant entity refers to logical group of resources in Unity Connection assigned to a single company, where each tenant is assigned with only one partition, search space, and phone system.

Tenant partitioning also introduces the concept of using the corporate email addresses as their alias, which enables alias uniqueness across tenants. In addition, separate Unity Connection SMTP domain is provided for each tenant.

Supported Tenant Partitioning Topology

Figure 7-1Sample Deployment scenario depicts the high level topology or deployment scenario that is being followed for tenant partitioning. Here, tenant 1 and tenant 2 have unique phone systems to identify inbound and outbound voicemail traffic. Each tenant has its own dedicated Cisco Unified Communication Manager.

Figure 5: Sample Deployment



Here each tenant has its own partition, schedule set, schedule, schedule detail, search space, search space member, phone system, class of service, user template, distribution list, distribution list membership, user operator, call handler template, directory handler, interview handler, call handlers (operator, opening greeting, Good Bye), and routing rules.

Note If you are upgrading Unity Connection 10.0(1) with Tenant Partitioning configured to a higher release then the Tenant Partitioning feature remains enabled on the upgraded system also.

Licensing

The tenant partitioning implementation does not require any additional licenses.

Scalability

Tenant Partitioning is a feature that offers a voice messaging solution for up to 60 tenants where each tenant can have maximum of 100 users on the Cisco Unity Connection 7vCPU OVA. For more information, see the "Specifications for Virtual Platform Overlays for Currently Shipping Unity Connection Servers" section of the Cisco Unity Connection 11.x Supported Platforms List at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Limitations of Tenant Partitioning

The following is the list of limitations of Tenant Partitioning:

- Each tenant is associated with only one phone system and Cisco Unified Communications Manager.
- Any other kind of networking like Diginet or VPIM is not supported.
- There is no way to share ports between multiple tenants. Each tenant has dedicated pool of ports.
- Overlapping extensions within a tenant is not supported.
- Any configurations done at the system level is not supported.
- At least one user in each tenant has to assign role of Greeting administrator so that tenant can customize their greetings.
- Tenants have to provide users alias as corporate email address to maintain uniqueness of alias across tenants.
- SAML SSO (Security Assertion Markup Language Single Sign-On) access feature in Unity Connection 10.0(1) and later releases are not supported with tenant partitioning.
- Multi-tenancy mode is not turned ON if there is any non-tenant user.
- Each object of tenant (like call handlers, directory handlers) should be mapped to object related to that tenant only.
- Custom keypad mappings are shared among all tenants.

CHAPTER 8

Migrating to Cisco Unity Connection from Another Voice-Messaging System

When the customer is replacing another voice messaging system with Unity Connection, consider the following issues:

- How do users interact with each system? For example, the options offered by the Unity Connection standard conversation (the telephone user interface, or TUI) and the key presses used to accomplish tasks may be different from what users are accustomed to using. As an alternative to the standard conversation, some customers may want to activate Optional Conversation 1 (the ARIA-like conversation available in Unity Connection) so that users hear message-retrieval menus that more closely resemble the choices they are familiar with. However, other menus—those that outside callers and Unity Connection users use to send and manage messages, as well as the menus that users use to change their Unity Connection settings—are the same as those in the standard conversation.
- Ensure that the customer understands the Unity Connection behaviors that are different from those of the voice messaging system it is replacing. For example, if the customer does not currently use an automated attendant feature and wants Unity Connection to be configured the same way, this should be noted so that the installer configures Unity Connection correctly. If it is necessary to make changes, for example to change the behavior of the opening greeting, or to zero out to an operator option during a personal greeting, these changes should be made and tested prior to the day of the cutover.
- Plan a method for creating Unity Connection users. If they be imported from an LDAP directory, imported from Cisco Unified Communications Manager, imported from a CSV file, or added using Cisco Unity Connection Administration? If they are imported from a CSV file or added using Unity Connection Administration, where does the information come from? Creating user accounts requires planning and testing prior to the cutover.
- The larger the installation or number of servers, the greater the need to perform user enrollment tasks prior to the day of the cutover. If too many users try to enroll simultaneously, some users (up to the number of voice ports available) succeed in accessing the Unity Connection server and enrolling, but the rest get a busy signal.

To prevent this negative user experience, smaller groups of users should be told a few days in advance how to call the pilot number and enroll in Unity Connection before the system goes live.

- If the customer has special audio-text applications set up in the existing voice messaging system, Unity Connection equivalents should be planned and set up before cutover. Unity Connection supports audio-text applications and provides tools for designing and configuring them.

- Unity Connection does not support group mailboxes, but the same functionality can be made available by setting up a call handler whose greeting prompts the caller to “press 1 for Pat, press 2 for Chris,” and so on. Dispatch messages may also provide the necessary functionality needed to support group mailboxes. (For more information about dispatch messaging, see the “Dispatch Messages” section of the “Messaging” chapter in the System Administration Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.
- When the Unity Connection design is finalized and verified through lab qualification, Unity Connection functionality should also be tested before cutover running a simulated load test and by running application test plans.

CHAPTER 9

Migrating from Cisco Unity to Cisco Unity Connection

When migrating from Cisco Unity to Cisco Unity Connection there are two distinct strategies to choose from: flash cut or gradual.

A gradual migration allows the Unity Connection environment to be built up over time. Directory synchronization is established between the Cisco Unity and Unity Connection sites, allowing the two sites to function as a single Cisco Voicemail Organization. Users can then be migrated over in small batches. A gradual migration might be required for multi-node sites needing to reuse Cisco Unity hardware or for sites that need an extended timeline for building out the Unity Connection infrastructure.

A flash-cut strategy eliminates the implementation and management complexity that the internetworking requirement imposes on a gradual migration, which can greatly reduce the overhead of a migration. A flash-cut approach is particularly attractive to sites using only Cisco Unity release 7.0 or earlier, as there is no need to upgrade to Cisco Unity before the migration.

Flash-Cut Migration

At a high level, a flash-cut migration process would look like this:

1. Build the Cisco Unity Connection site as a parallel infrastructure.
2. Copy all user data and selected system distribution lists using the COBRAS briefcase mode. For more information, see Help for the COBRAS tool at http://www.ciscounitytools.com/Applications/General/COBRAS/Help/COBRAS.htm.
3. Redirect all voicemail pilot numbers and related phone system routing from Cisco Unity to Unity Connection.
4. Unity Connection becomes the production voicemail server.

The cut itself (steps 2 and 3 in the list above) should occur after hours or over a weekend, depending on the scale. For more information on implementing a flash cut, see the “Migrating from Cisco Unity 4.x and Later to Unity Connection 7.x and Later” section of the “Maintaining Cisco Unity Connection Server” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

See the following sections for additional details:

Using COBRAS to Migrate Messages in a Flash-Cut Migration

COBRAS can be leveraged to copy messages from Cisco Unity to Unity Connection. If this is done, then the Cisco Unity servers can be decommissioned immediately after the flash. However, there are several limitations that should be considered before deciding to migrate messages. These are detailed in the COBRAS Help, at http://www.ciscounitytools.com/Applications/General/COBRAS/Help/COBRAS.htm.

An alternate approach is to maintain the Cisco Unity servers for a short period strictly to provide users with access to old messages. For example, a typical message retention policy might allow 30 days of access before the servers are decommissioned. Note that Cisco Unity allows users to reply to messages in this environment. This may be acceptable if Cisco Unity is in a unified messaging configuration, as users can continue to see new messages in their email client. Otherwise, for example in a voicemail-only environment, the Custom Key Map utility can be used to disable all options for “Send a message,” “Reply,” “Forward message,” and “Reply to all.”

MWI functionality on Cisco Unity should be disabled in any post-cut dual environment. This prevents conflicts that occur when two messaging systems attempt to control the same lamps. The Cisco Unity Bulk Edit utility can be used to disable MWIs for all subscribers.

Mitigating Day One Shock After a Flash-Cut Migration

A major concern with flash-cut migrations in general is that all users are exposed to a new system at once. Because almost all user settings are preserved during a COBRAS briefcase move, the flash cut from Cisco Unity to Unity Connection eliminates the potential flood of first-time enrollment activity that can easily overwhelm other voicemail migrations.

You can further mitigate the impact of the flash cut by building the full Unity Connection environment well in advance of the cut. Users can then be given access and training on the production Unity Connection servers while Cisco Unity still acts as the production messaging solution. This helps reduce day 1 loads and support cases as users have the opportunity to customize personal settings over a period of time.

The duration of a pre-cut parallel environment needs to be a balance between minimizing costs of maintaining both environments and providing sufficient time for users to familiarize themselves with Unity Connection.

MWI functionality should be disabled on the Unity Connection servers during any pre-cut time. MWI functionality needs to be enabled on Unity Connection when the flash cut is performed.

Gradual Migration Using Intersite Networking

At a high level, the process of using a Cisco Voicemail Organization to link Cisco Unity and Cisco Unity Connection would look like this:

1. Build a networked mixed environment:
    a. Upgrade Cisco Unity as needed to meet minimum requirements for Intersite networking.
    b. Install and configure at least one Cisco Unity Connection 11.x server.

   c. Begin initial preparation of search spaces and partitions on Unity Connection. (For design considerations, see the Partition Considerations, on page 68 section.)
   d. Join the Cisco Unity and Unity Connection sites with an intersite link.
   e. Complete the configuration of search spaces and partitions on Unity Connection.
   f. Complete the initial configuration of distribution lists. (For design considerations, see the Distribution List Management, on page 74 section.)
   g. Set up intersite cross-server features.

2. Migrate groups of users over an extended time period:

   a. Use COBRAS hot mode to move user accounts to Unity Connection.
   b. Reconfigure user phones to use Unity Connection pilot numbers.
   c. Optionally, configure access for migrated users to their old voice messages on the Cisco Unity server, and instruct users on how to access archived mailboxes.

3. Decommission (uninstall) each Cisco Unity server when all users on the server are migrated and archived mailboxes have expired.

For a high level overview of a Cisco Voicemail Organization that links Cisco Unity and Cisco Unity Connection sites, see the "Overview of Networking Concepts" chapter of the Networking Guide for Cisco Unity Connection *Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html.

It is critical that the migration be viewed as a one-way flow. All associated tools, such as COBRAS and PDL Builder, are intended to assist in moving objects from the Cisco Unity site to Unity Connection. There is no automated process to move users or distribution lists in the reverse direction, from Unity Connection to Cisco Unity.

In most cases a gradual migration should focus on moving subscribers from one Cisco Unity location at a time. This helps to reduce the cost and complexity of the overall Cisco Voicemail Organization. When all subscribers for a given location are migrated, the Cisco Unity server can be decommissioned and repurposed. A decommissioned server may even be repurposed as a Unity Connection server if it meets the platform requirements for Unity Connection (see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html).

Pre-Existing Dual Environments Using VPIM

With earlier releases of Cisco Unity and Unity Connection it was possible to maintain a mixed environment using VPIM networking. These mixed environments can be greatly enhanced by utilizing the intersite networking features available in Unity Connection Release 11.x. When the VPIM link has been replaced by an intersite link, the general migration process can follow a gradual migration as detailed in the Gradual Migration Using Intersite Networking, on page 66 section.

Note that it is not necessary to entirely remove the VPIM link between the two sites. Leaving the VPIM link in place preserves routing for users who reply to messages that were sent previously. However, pre-existing VPIM contacts on both sides of the network may cause addressing conflicts. These contacts should be hidden or deleted. Also, VPIM on both sides must be configured not to automatically create VPIM contacts.

For example, consider an installation where John Smith is a Unity Connection user with extension 1234. In the pre-existing VPIM environment a VPIM contact account was created for John Smith and assigned extension 1234 within Cisco Unity. When intersite networking is established, Cisco Unity attempts to create a new Unity Connection contact for John Smith. In some cases this creation fails entirely due to conflicts with the existing VPIM account. In other cases, the Unity Connection contact is created, but the primary extension for John Smith (1234) is not associated with the new account.

On Unity Connection, existing VPIM contacts can be hidden from users by reassigning them to a partition that is not addressable from any search space. Note that VPIM accounts at the Cisco Unity site cannot as easily be hidden. Also, existing VPIM accounts on Cisco Unity may prevent the proper intersite replication of corresponding Unity Connection users. To avoid addressing and synchronization conflicts, in Cisco Unity, delete all VPIM contacts that are associated with the Unity Connection location. This of course means that existing messages addressed from the VPIM contacts are no longer associated with the contact.

Any distribution lists—either system or private—that contain VPIM contacts should be updated to use the replicated Unity Connection Networking subscribers instead. Note that such updates must be performed manually. Cisco Unity distribution lists that contain VPIM contacts lose those members when the VPIM contacts are deleted. In the reverse direction it is possible for Unity Connection distribution lists to continue delivering messages via VPIM. However, even this becomes problematic as users are migrated to Unity Connection. The VPIM contacts on Unity Connection are not automatically updated during a COBRAS hot-mode migration. If a Unity Connection distribution list contains a VPIM contact for a migrated Cisco Unity subscriber, messages to that list is delivered to the archived mailbox of the subscriber on Cisco Unity.

Selecting Site Gateways

When establishing an intersite link between Cisco Unity and Unity Connection for a gradual migration, a server at each site must be designated as the site gateway. When networking has been established between the two sites, reassigning the role of site gateway to another server is not a simple task. Therefore, careful selection of the site gateways is critical. For basic prerequisites and considerations, see the "Setting Up Networking between Cisco Unity and Cisco Unity Connection Servers" chapter of the Networking Guide for Cisco Unity Connection *Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html.

At the Cisco Unity site, care should be taken to select a server that can maintain the role of site gateway for the duration of the migration. For example, any server that is to be repurposed as a Unity Connection server during the migration should not be selected. Also, if multiple dialing domains exist on the Cisco Unity site, selection of the site gateway affects the resulting dial plan (see the Fitting Unity Connection Partitions into Dialing Domains for additional details).

The role of site gateway does place nontrivial additional load on the server. Therefore, servers with the most available resources should be selected whenever possible. System load testing exposed performance impacts on the Cisco Unity site gateway related to the processing of directory information to and from the remote site. These impacts can be minimized using a Platform Overlay 2 or 3 server as the site gateway. Impact can also be reduced by minimizing the number of regular subscribers or users homed on site gateways.

While there are no minimum bandwidth requirements between the two site gateways, HTTP or HTTPS connectivity is required. A DNS environment allows FQDN resolution between the two site gateways. As long as this minimal connectivity can be met, priority should be given to other criteria discussed above.

Partition Considerations

Within the Cisco Unity site, dialing domains offer a very basic form of partitioning. When multiple dialing domains exist, extra planning is needed in deciding how the dialing domain topology is integrated with Unity Connection search spaces and partitions.

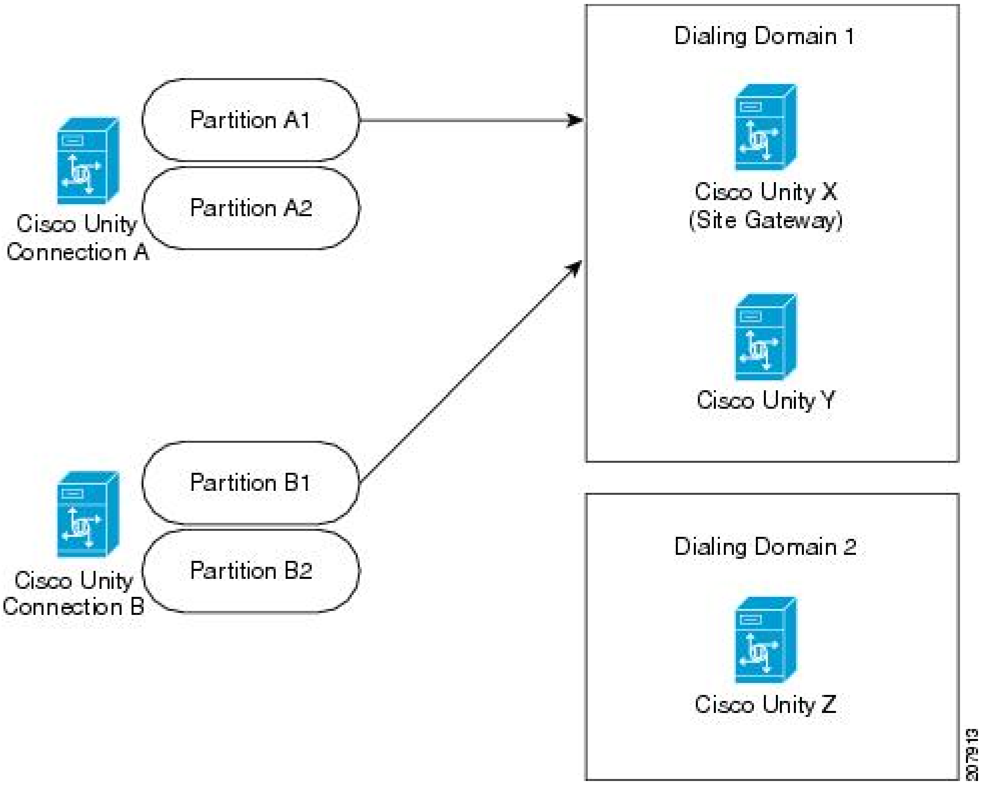
See the following sub-sections for additional details:

Fitting Unity Connection Partitions into Dialing Domains

When networked with a Cisco Unity site, each Unity Connection location has just a single partition that is made available in Cisco Unity. At the Cisco Unity site, all Unity Connection locations are assigned to the dialing domain of the site gateway. Cisco Unity attempts to add all incoming extensions from Unity Connection into this single dialing domain. Because extensions within a dialing domain must be unique, the collection of all partitions chosen across the Unity Connection site should not contain duplicates of any extension. When the collection includes duplicate extensions, or extensions that already exist in the Cisco Unity site gateway dialing domain, one or more extensions are omitted from the Cisco Unity directory.

Figure 9-1 depicts a Cisco Voicemail Organization consisting of two Unity Connection locations with two partitions each, and three Cisco Unity locations in two dialing domains. In this case, Partition A1 is selected as the partition from which user extensions map to the dialing domain for Unity Connection A (in Cisco Unity Connection Administration this is known as the Local Partition That Cisco Unity Users Can Address to By Extension), and Partition B1 is selected to map to the dialing domain for Unity Connection B. All extensions from these partitions map to Dialing Domain 1 because the Cisco Unity site gateway, Cisco Unity X, is a member of Dialing Domain 1. These partitions should be chosen such that the extensions are unique across Partition A1, Partition B1, and Dialing Domain 1. Other partitions, such as Partition A2 and Partition B2, are not used by Cisco Unity. Any extensions in those partitions are not available to users on Cisco Unity.

Figure 6: Extensions from the Partition You Select for Each Cisco Unity Connection Server Are Placed in the Dialing Domain of the Cisco Unity Site Gateway



For additional information on the local partition that Cisco Unity users can address to by extension, see the “About Linking Cisco Unity Connection and Cisco Unity Sites” section and the “Cisco Unity Dialing Domains and Cisco Unity Connection Users” section in the “Overview of Networking Concepts in Cisco Unity Connection 11.x” chapter of the Networking Guide for Cisco Unity Connection *Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx/b_11xcucnetx_chapter_01.html.

Cisco Unity automated attendant searches always treat imported. Unity Connection users as remote users. Therefore, the automated attendant search scope should be set to dialing domain on every Cisco Unity server. Callers within alternate dialing domains at the Cisco Unity site are not able to contact Unity Connection users through automated attendant searches.

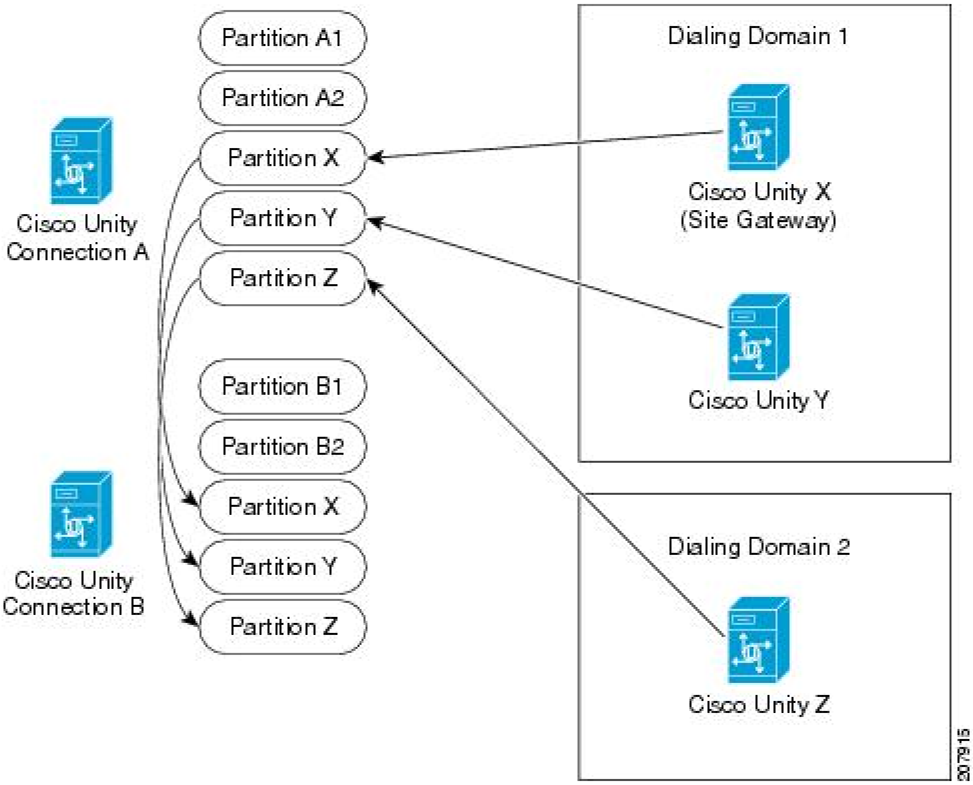
Cisco Unity subscriber-addressing searches and directory handler searches treat imported Unity Connection users as if they are homed on the Cisco Unity site gateway. On the site gateway, Unity Connection users are found even if the scope is restricted to local server. For all other servers, a local server scope does not return any Unity Connection users. Dialing domain or global directory should be selected as the scope for these types of searches in order to provide consistent behavior between the site gateway and non site gateway servers.

Fitting Dialing Domains into Cisco Unity Connection Partitions

Cisco Unity Connection does not carry over dialing domain information from Cisco Unity. For each Cisco Unity location, Unity Connection creates a dedicated partition, as shown in Figure 9-2. You might have several Cisco Unity locations in a dialing domain, with a global, non-overlapping dial plan. Unity Connection does not see this. It only sees the individual locations and creates distinct partitions for you to manage.

Figure 9-2 depicts the same Cisco Voicemail Organization shown in Figure 9-1. In this case, looking from the perspective of mapping Cisco Unity objects into Unity Connection partitions, we see that three new partitions are created on the Unity Connection A, the site gateway, when the sites are linked. Each partition corresponds to a Cisco Unity location. The new partitions are then replicated via intrasite networking to Unity Connection B.

Figure 7: A Single Cisco Unity Connection Partition is Automatically Generated for Each Cisco Unity Server And Replicated in the Unity Connection Site



When intersite networking is initially configured between Cisco Unity and Unity Connection, users who are homed on Unity Connection are not able to dial or address messages to users on Cisco Unity. This is because the Unity Connection search spaces do not contain the partitions that were auto-generated for Cisco Unity locations. After initial replication completes, Unity Connection search spaces must be modified to include the new partitions. This needs to be done at each Unity Connection location in the network. In most basic topologies, this might mean simply adding the new partitions to the default search space on each server. In complex environments consideration must also be given to all search spaces used by call handlers, directory handlers, call routing rules, and users. For example, the search space of a Unity Connection user must include the Cisco Unity partitions in order for that user to add remote site users to a private distribution list.

When users are migrated from Cisco Unity to Unity Connection they can be assigned to any local partition on the Unity Connection server. After a Cisco Unity server is fully migrated it is possible to remove the location from the network. If this is done, the auto-generated partition for that location then disappears. Therefore, focusing the user migration to one Cisco Unity server at a time can help reduce complexity at the Unity Connection site.

Migrating Away from Dialing Domains

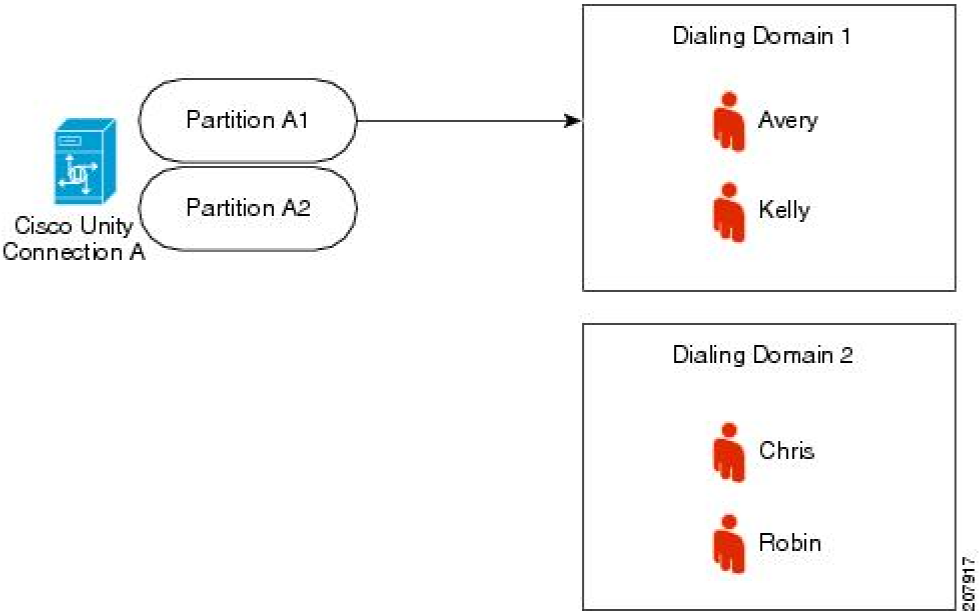
An intermediate goal of the migration might be to eliminate the need for multiple dialing domains. Doing so reduces the complexity of an organization and typically allows for more flexible dial plans. This is most effective when all servers in a dialing domain can be migrated simultaneously. If a subset of the dialing domain is migrated, connectivity between those users and the remaining dialing domain members may be disrupted. The users migrated can be provided with search spaces that allow access to any Cisco Unity Connection user as well as access to Cisco Unity subscribers in any dialing domain. However, any Unity Connection partition that is associated with those migrated users can only be mapped to the dialing domain of the Cisco Unity site gateway.

In some cases dialing domains are used to intentionally segregate users, for example to provide limited tenant services. In this case, the dialing domain of the Cisco Unity site gateway should be migrated first. If users from another dialing domain are migrated, Cisco Unity is not able to provide the same level of segregation.

Example

Before beginning the user migration from Cisco Unity to Cisco Unity Connection, Kelly and Avery are homed on Cisco Unity X, the site gateway, in Dialing Domain 1. Chris and Robin are homed on Cisco Unity Z in Dialing Domain 2. As shown in Figure 9-3, Kelly and Avery can find Unity Connection users in directory handler searches and address to them using their extensions in Partition A1, but they cannot reach Chris and Robin by the same means. Chris and Robin can address to each other but cannot address to Kelly or Avery or to users on Unity Connection A.

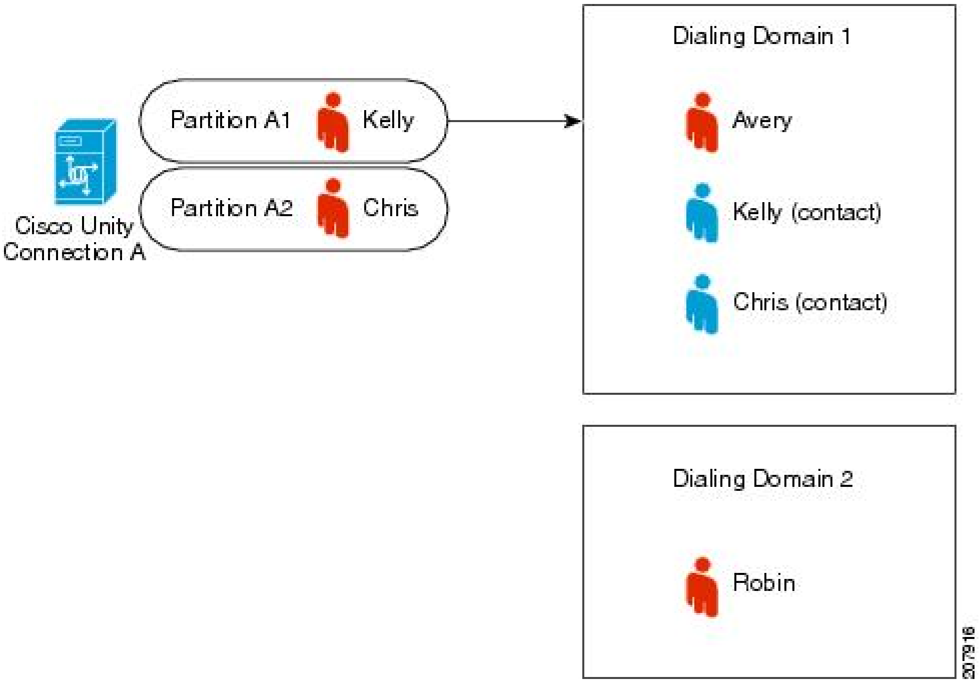
Figure 8: Example: Before Migrating Users from a Cisco Unity Site Segmented Into Two Dialing Domains to a Cisco Unity Connection Site with Two Partitions



When Kelly is migrated to Cisco Unity Connection A using COBRAS hot mode, during the migration process, Partition A1 is selected for the target partition. This means that all existing extensions and alternate extensions for Kelly is also assigned to Partition A1. Because Partition A1 is replicated into Dialing Domain 1 of Cisco Unity, all dialing and addressing scopes within the Cisco Unity site that previously controlled access to Kelly are still effective, so Avery can still reach Kelly as usual, as shown in Figure 9-4. Similarly, Kelly can be assigned to a search space that maintains the same level of access that she had before the move. Of course the search space can also be made more granular or even provide additional access.

Now suppose Chris is also migrated to Unity Connection. Even if none of Chris's extensions are placed into Partition A1 (the partition that replicates to Cisco Unity), Chris still have a contact account created by Cisco Unity within Dialing Domain 1, as shown in Figure 9-4. This means that Avery can now locate Chris when using dial by name with a directory handler or during subscriber message addressing. Robin is still unable to reach Kelly or Avery through directory handlers and subscriber message addressing, and can no longer reach Chris through these means.

Figure 9: Example: After Migrating Users from a Cisco Unity Site Segmented Into Two Dialing Domains to a Cisco Unity Connection Site with Two Partitions



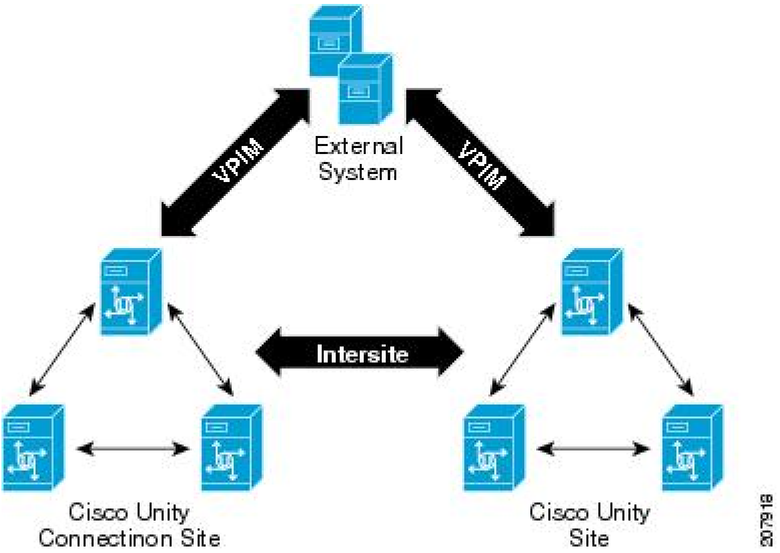
Interworking with Other Voice Messaging Networks

A Cisco Unity environment can use other voice messaging network types (Bridge, AMIS, VPIM, or Trusted Internet). However, messages from Cisco Unity Connection users cannot be relayed to remote subscribers who are associated with these other Cisco Unity delivery locations. Instead, direct networking to these other locations must be established independently from the Unity Connection site.

VPIM

A direct VPIM link can be established between the Cisco Unity Connection site and any other remote messaging network, although the VPIM link between Cisco Unity and the external system must also be maintained, as shown in Figure 9-5. Relaying messages across the intersite link to VPIM contacts is not possible in either direction. The servers acting as the VPIM bridgehead at each site can also act as the site gateway, though they do not need to.

Figure 10: Both Sites in a Cisco Voicemail Organization Must Be Independently Configured for VPIM



As users are migrated from Cisco Unity to Unity Connection, the external VPIM system needs to be updated. The exact steps required depend on the specific system. Typically, contacts or message routing are managed according to the extension of each user. Therefore, migrating users in groups within continuous extension ranges is desirable. The administrative work required at the external system may become onerous if migrated users span multiple disjointed extension ranges.

Non-VPIM

System contacts can be manually created in Cisco Unity Connection that correspond to the Trusted Internet Subscribers on Cisco Unity.

Unity Connection does not support Bridge or AMIS networking. If a remote messaging system supports only Bridge or AMIS networking, Unity Connection users are not able to address to users on those systems.

Distribution List Management

In a mixed Cisco Unity and Cisco Unity Connection network, directory synchronization can be configured to include system distribution lists. When this is done only addressing and routing information for the distribution lists is shared. Membership information for each list is stored and managed at the site where the list was created. However, with some careful advanced planning, it is possible to limit most list management activity to one site. This reduces the need to jump between Cisco Unity and Unity Connection administration for list maintenance.

System Distribution List Management on Unity Connection

Because the long term goal of a migration is to have everything on Cisco Unity Connection, it may be beneficial to move most, if not all, voicemail distribution lists, including membership, to Unity Connection right away. This can be done using Public Distribution List Builder (see Public Distribution List Builder Help for details, at http://ciscounitytools.com/Applications/Unity/PublicDistributionListBuilder/Help/PublicDLBuilder.htm). When a distribution list is created in Unity Connection, intersite networking can allow both Cisco Unity and Unity Connection users access to the list. The original list on Cisco Unity should then be removed.

Note that distribution lists that use subscriber templates for membership cannot be managed fully on Unity Connection. This is because Unity Connection does not use templates when creating contacts for replicated Cisco Unity subscribers. However, distribution list nesting can be used to manage template-based distribution lists that span both sites.

Example

A “Sales Staff” distribution list on Cisco Unity is populated using a corresponding subscriber template. When intersite networking is introduced, the Cisco Unity Sales Staff list cannot be migrated over to Unity Connection because new sales staff may still be added to the Cisco Unity site during the gradual migration. Instead, a corresponding “Sales Staff” template and distribution list are created on Unity Connection. The distribution list on Unity Connection is configured to replicate to remote sites over intersite links.

On Cisco Unity, the “Sales Staff” distribution list is renamed to “Sales Staff – Unity only.” If previously enabled, the “Show Distribution List in Email Server Address Book” attribute is removed. Using Public Distribution List Builder, the “Sales Staff – Unity only” distribution list is marked for replication to Unity Connection.

When the “Sales Staff – Unity only” distribution list has replicated from Cisco Unity to Unity Connection, it can then be added as a nested member of the “Sales Staff” distribution list on Unity Connection. The list on Unity Connection is now the master “Sales Staff” distribution list. Users on Unity Connection address to it directly while those on Cisco Unity address to it via its replicated object, which by default shows up on Cisco Unity as “Sales Staff – Voicemail.” When a new mailbox is created using the sales staff template at either site, that mailbox is immediately a recipient of the master “Sales Staff” distribution list.

Note that managing voicemail distribution lists on Unity Connection becomes problematic when Cisco Unity is a unified messaging deployment and Unity Connection users are using ViewMail for Outlook within the same Active Directory. The groups that Cisco Unity creates in Active Directory for replicated Unity Connection system distribution lists can complicate matters for Unity Connection users when they address messages via ViewMail for Outlook or other email clients. Unity Connection users who try to address messages to such lists receive a non-delivery receipt in response. Currently, Unity Connection does not provide a way to mitigate the issue for synchronized distribution lists using SMTP proxy addresses like you can for Unity Connection users.

Public Distribution List Management on Cisco Unity

When Cisco Unity and Unity Connection are both integrated (or unified in the case of Cisco Unity) it may be desirable to manage system distribution lists at the Cisco Unity site. This allows them to be fully synchronized with Active Directory. Distribution lists can be selectively enabled for directory replication to Unity Connection.

Distribution lists populated via subscriber templates can be handled in a way similar to that discussed in the System Distribution List Management on Unity Connection. Template-based lists from Unity Connection can be nested into corresponding lists on Cisco Unity. In this case the Cisco Unity lists become the master lists. Partitions and search spaces can be used to hide the sub-lists on Unity Connection from users.

Example

A “Sales Staff” distribution list on Cisco Unity is populated using a corresponding subscriber template. When Unity Connection Networking is introduced, the Cisco Unity Sales Staff distribution list cannot be migrated over to Unity Connection because new sales staff may still be added to the Cisco Unity site during the gradual migration. Instead, a corresponding “Sales Staff – Unity Connection Only” template and distribution list are created on Unity Connection. This list on Unity Connection is configured to replicate to remote sites over intersite links. The list is assigned to a partition which is not addressable by users.

When the Unity Connection distribution list is replicated to Cisco Unity, its display name appears as “Sales Staff – Unity Connection Only – voicemail.” The “Show Distribution List in Email Server Address Book” attribute should be removed for this list. It can then be added as a nested member of the Cisco Unity “Sales Staff” distribution list. The Cisco Unity “Sales Staff” distribution list is marked for replication to Unity Connection using the Public Distribution List Builder tool.

The distribution list on Cisco Unity is now the master “Sales Staff” distribution list. Users on Cisco Unity address to it directly while those on Unity Connection address to it via its replicated object, which by default shows up on Unity Connection as “Sales Staff.” When a new mailbox is created using the sales staff template at either site, that mailbox is immediately a recipient of the master “Sales Staff” distribution list.

Note that this method for managing voicemail distribution lists limits dial plan flexibility. All distribution lists that are replicated from Cisco Unity to Unity Connection are assigned to the same auto-generated partition as all other objects from the Cisco Unity location. If greater granularity for search scope partitioning is needed, distribution lists need to be managed at the Unity Connection site.

Another caveat of managing distribution lists within Unity Connection occurs as users are migrated to Unity Connection. Distribution list membership within Cisco Unity is not adjusted when COBRAS hot mode is used to migrate users. Messages to the distribution list continue to be delivered to the Exchange mailboxes of the migrated users. While these messages are accessible via the archived subscriber account, the situation may cause confusion for users. (See the Archived Mailboxes for additional details.)

Hybrid Distribution List Management

Managing distribution lists entirely on one site or the other is often not possible. In addition to the caveats mentioned in the System Distribution List Management on Unity Connection and the Public Distribution List Management on Cisco Unity, distribution lists that contain contacts cannot be replicated. This is because messages that are sent across an intersite link cannot be further relayed to remote mailboxes that are not part of the Cisco Voicemail Organization. If a user at the remote site were to attempt addressing to such a list, a non-delivery receipt (NDR) would be generated for each undeliverable contact within the list.

Example

Suppose the Cisco Unity “Sales Staff” distribution list from the previous examples also contains VPIM contacts in addition to mailbox users. In order to use templates at both sites for populating a master “Sales Staff” list, two separate distribution lists are maintained at each site. Each site has a “Sales Staff – <site>” list that contains only users from the local site, and each list is assigned to the corresponding template at each site. (The list can be hidden from users but must be configured to replicate across the intersite link.) Next, each site also has a “Sales Staff” master distribution list. The master lists contain both “Sales Staff – <site>” lists plus any remote contacts such as VPIM users. The two master lists are not replicated between the sites. Users at each site must address to the corresponding local master list.

Nesting Distribution Lists

Nesting of distribution lists can be extremely useful. However, it is important to be aware of list membership when nesting. In each of the distribution list examples in the System Distribution List Management on Unity Connection, the Public Distribution List Management on Cisco Unity, and the Hybrid Distribution List Management, two categories of lists are used at each site. The first category is local lists that are created with the intent of having list membership limited to the local site. The display names for the local lists should follow a naming convention that helps identify their role. The second category of lists is the master lists. The membership for the master lists includes objects from both sites. When nesting lists, a master list should never be nested inside another list. Following a well-defined naming convention can help ensure nesting loops are not created.

Additionally, any list that contains external contacts, such as VPIM subscribers, should not be nested within any list that is replicated. A naming convention for list display names could be extended to flag these lists. This would serve as a reminder to avoid placing such lists within a list that is intended for replication.

Private Distribution Lists

When users are migrated from Cisco Unity to Cisco Unity Connection, some private distribution list membership information may be lost. Backups only include membership information about full subscribers (users with mailboxes) and public distribution lists. Members of the private distribution list that are remote contacts (including Unity Connection users) or other private lists are not included in the private list membership backup.

Also, if a migrated user was included as a member of a private distribution list owned by a Cisco Unity subscriber who has not been migrated, that private distribution list is not automatically updated during the migration. Unless the distribution list is manually edited, messages sent to it continues to be delivered to the archived mailbox of the migrated user on Cisco Unity.

Messaging Options

For an overview of message routing between Cisco Unity and Unity Connection sites, see the "Configuring Partitions and Search Spaces for Cisco Unity and Cisco Unity Connection Interoperability" section in the "Setting Up Networking Between Cisco Unity and Cisco Unity Connection" chapter of the Networking Guide for Cisco Unity Connection, *Release 11.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/networking/guide/b_11xcucnetx.html.

Secure Messages

Cisco Unity and Unity Connection use different methods for securing messages. In particular, Unity Connection is not able to decrypt secure messages that are sent from Cisco Unity. Therefore, by default, messages marked as secure is not sent between the systems.

Optionally, you can configure both systems to enable delivery of secure messages between sites. However, in order for this to occur, all secure messages must be unencrypted as they traverse the network. An x-header is placed on the messages indicating whether they are intended to be secure. This allows the receiving site to apply secure handling of the messages when they arrive. For example, Cisco Unity can be configured to encrypt inbound messages that are flagged as secure as soon as they arrive.

Transcoding

Both Cisco Unity and Unity Connection can be configured to transcode all messages sent to the remote site. This may be required, for example, if the messages are stored locally in a format not supported at the remote site. However, use of the transcoding feature is likely to reduce audio quality of the messages. This is particularly noticeable if a message traverses between sites multiple times, for example, by being forwarded between sites, or when a distribution list contains remote users.

Example

Consider the master "Sales Staff" distribution list on Unity Connection from the System Distribution List Management on Unity Connection. A Cisco Unity user is able to send messages to this list using the replicated "Sales Staff – voicemail" list found on Cisco Unity. The message is first routed across to the Unity Connection site, introducing possible transcoding degradation. Unity Connection members of the list receive the message in this state. But then the message is further routed back across to Cisco Unity so that it can be delivered to members of the "Sales Staff – Unity only" distribution list. This introduces a second generation of transcoding degradation. We now have up to two generations of degradation for a message that, in the end, was sent between two users on the same messaging system.

Archived Mailboxes

When COBRAS hot mode is used to migrate batches of users from Cisco Unity to Unity Connection, the user mailboxes on Cisco Unity are preserved but set to an archived state. These mailboxes are hidden in the directories and cannot be directly addressed to by other users. Because messages are not moved as part of the migration process, the archived mailboxes allow users to access their messages for a period of time on the Cisco Unity server.

Because distribution list membership is not automatically updated when users are migrated, archived mailboxes can still receive new messages. The archived mailboxes should be manually purged from all Cisco Unity distribution lists, both public and private. For public distribution lists an alternate solution is to use the Public Distribution List Builder tool to move lists from Cisco Unity to Unity Connection. Even if the list already has archived mailboxes as members, Public Distribution List Builder maps and replaces those members with the correct corresponding user on Unity Connection.

The archived mailboxes are hidden in the Cisco Unity Administrator. The only administrative tasks available for these mailboxes are password resets and deletes. These tasks can be done using the Bulk Password Reset and Bulk Subscriber Delete tools. For additional information about the tools, see the respective tool Help at http://www.ciscounitytools.com/Applications/Unity/BulkPWReset/Help/BulkPWReset.htm and at http://www.ciscounitytools.com/Applications/Unity/BulkSubscriberDelete403/Help/BulkSubDelete.htm.

Voice Name Replication

Replication of recorded voice names between Cisco Unity and Unity Connection is optional. It can be enabled in one direction, both directions, or not at all. Additionally, the voice names can be converted to a different codec when they are replicated between sites. For example, if disk space is a concern at one site the names can be converted to a more compressed format.

At the Unity Connection site, Text to Speech is automatically used for users who do not have recorded names. This applies to remote Cisco Unity users also. This feature may provide a reasonable alternative to transcoding if disk space required for remote Cisco Unity users is a concern on Unity Connection.

Often, new users on Unity Connection choose not to record their own voice names because of the Unity Connection Text to Speech feature. However, Cisco Unity does not have this Text to Speech feature, so users without recorded voice names are not accessible through directory handlers. Recorded voice names are also valuable during message addressing. Therefore, it generally is a good idea to encourage Unity Connection users to record their voice names and to enable voice name replication to Cisco Unity.

Common Elements in Flash-Cut and Gradual Migration Strategies

Certain considerations apply regardless of the type of migration strategy you choose. See the following sub-sections for additional details:

Key Mapping

One thing COBRAS does not migrate is custom key map configurations. COBRAS tracks the name of the conversation that subscribers are associated with and tries to restore that on the import. However, if a key map conversation on Cisco Unity does not match the mapping of the corresponding key map on Cisco Unity

Connection, users end up with a different sounding conversation. It is up to the administrator to verify that key mapping data is configured on the target system as needed.

Speech Connect for Cisco Unity

Cisco Unity typically synchronizes data to an external Speech Connect for Cisco Unity server via Active Directory. This synchronization ends when users are migrated because Cisco Unity Connection does not push any data to Active Directory. Therefore, maintaining the external Speech Connect for Cisco Unity servers may require importing manually-generated employee data files.

Some limited synchronization is available during a gradual migration. When users are created or migrated to Unity Connection, they are replicated across the intersite link to Cisco Unity, which in turn pushes them into Active Directory as Contacts. The Speech Connect for Cisco Unity server can then import them automatically if it is configured to pull both Users and Contacts. One caveat of this configuration is that the transfer extension used by Speech Connect for Cisco Unity originates from the Cross-Server Transfer Extension on Unity Connection. This field can only be managed by system administrators. The Speech Connect for Cisco Unity server cannot be synchronized with any basic or personal transfer rules configured by or for Unity Connection users.

A better approach may be to replace the external Speech Connect for Cisco Unity servers entirely with the Speech Connect for Unity Connection solution, which utilizes the standard Unity Connection voice-enabled directory handlers and does not require a separate server. The Speech Connect for Cisco Unity servers can then be decommissioned, reducing maintenance and administrative costs associated with the additional servers. The Unity Connection solution even provides additional features not available in Speech Connect for Cisco Unity, such as disambiguation by city and/or department name. Unlike Speech Connect for Cisco Unity, the Unity Connection solution also uses partitions and personal transfer rules for users. In a gradual migration, the search scope of directory handlers can be set to include both Cisco Unity and Unity Connection users. Enabling cross-server transfer routing for the remote locations also allows the speech-enabled automated attendant to use the current transfer rules for Cisco Unity subscribers.

Note that there is no name tuning service available for Unity Connection. Also, the telephony port capacity of the Unity Connection server must be sufficiently provisioned to accommodate call loads that previously were distributed between Cisco Unity and the external Speech Connect servers.

Migrating from Cisco Unity for Domino to Unity Connection

A gradual migration using intersite networking is not possible with Cisco Unity for IBM Lotus Domino. This is because intersite networking requires at least one server at the Cisco Unity site. Release 8.x of Cisco Unity is not supported with a Domino message store.

It is possible to establish VPIM networking between a Cisco Unity for Domino site and Unity Connection. This would allow some interworking between sites should a full flash-cut migration not be possible. COBRAS can then be used for migrating users to the Unity Connection site. However, only COBRAS briefcase mode is available in this case. For more detail on COBRAS, see COBRAS Help at http://www.ciscounitytools.com/Applications/General/COBRAS/Help/COBRAS.htm. In addition, considerations from the Pre-Existing Dual Environments Using VPIM apply in this scenario.

CHAPTER 10

LDAP Directory Integration with Cisco Unity Connection

The Lightweight Directory Access Protocol (LDAP) provides applications like Cisco Unity Connection with a standard method for accessing user information that is stored in the corporate directory. Companies that centralize all user information in a single repository that is available to multiple applications can reduce maintenance costs by eliminating redundant adds, moves, and changes.

- **User creation**—Unity Connection users can be created by importing data from the LDAP directory.
- **Data synchronization**—Unity Connection can be configured to automatically synchronize user data in the Unity Connection database with data in the LDAP directory.
- **Single sign-on**—Optionally, you can configure Unity Connection to authenticate user names and passwords for Unity Connection web applications against the LDAP directory, so that users do not have to maintain multiple application passwords. (Phone passwords are still maintained in the Unity Connection database.)

Unity Connection uses standard LDAPv3 for accessing data in an LDAP directory. For a list of the LDAP directories that are supported by Unity Connection for synchronization, see the “Requirements for an LDAP Directory Integration” section in the System Requirements for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.htmll.

LDAP Synchronization

LDAP synchronization uses an internal tool called Cisco Directory Synchronization (DirSync) to synchronize a small subset of Cisco Unity Connection user data (first name, last name, alias, phone number, and so on) with the corresponding data in the corporate LDAP directory. To synchronize user data in the Unity Connection database with user data in the corporate LDAP directory, do the following tasks:

1. Configure LDAP synchronization, which defines the relationship between data in Unity Connection and data in the LDAP directory. See the Configuring LDAP Synchronization, on page 82section.
2. Create new Unity Connection users by importing data from the LDAP directory and/or linking data on existing Unity Connection users with data in the LDAP directory. See the Creating Unity Connection Users, on page 85 section.

For additional control over which LDAP users are imported into Unity Connection, you can create one or more LDAP filters before you create Unity Connection users. See the Filtering LDAP Users.

Configuring LDAP Synchronization

When you configure LDAP directory synchronization, you can create up to 20 LDAP directory configurations for each Cisco Unity Connection server or cluster. Each LDAP directory configuration can support only one domain or one organizational unit (OU); if you want to import users from five domains or OUs, you must create five LDAP directory configurations.

A Unity Connection networking site also supports up to 20 LDAP directory configurations for each Unity Connection server or cluster joined to the site. For example, if you have a site with ten servers, you can import users from up to 200 domains.

In each LDAP directory configuration, you specify:

- **The user search base that the configuration accesses:** A user search base is the position in the LDAP directory tree where Unity Connection begins its search for user accounts. Unity Connection imports all users in the tree or subtree (domain or OU) specified by the search base. A Unity Connection server or cluster can only import LDAP data from subtrees with the same directory root, for example, from the same Active Directory forest.

  Note The user search bases that are specified in the LDAP directory configurations on a Unity Connection server must include no more than a total of 120,000 LDAP users. Importing large numbers of LDAP users who do not become Unity Connection users reduces the amount of disk space available for messages, slows database performance, and causes upgrades to take longer.

  If you are using an LDAP directory other than Microsoft Active Directory, and if you create a Unity Connection LDAP directory configuration that specifies the root of the directory as the user search base, Unity Connection imports data for every user in the directory. If the root of the directory contains subtrees that you do not want Unity Connection to access (for example, a subtree for service accounts), you should do one of the following:

  - Create two or more Unity Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Unity Connection to access.
  - Create one or more LDAP search filters. For more information, see the " Filtering LDAP Users " section in the "LDAP" chapter of the System Administration Guide for Cisco Unity Connection Release 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

  For directories other than Active Directory, you should specify user search bases that include the smallest possible number of users to speed synchronization, even when that means creating multiple configurations.

  If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; Unity Connection does not follow Active Directory referrals during synchronization. The same is true for an Active Directory forest that contains multiple trees-you must create at least one configuration to access each tree. In this configuration, you must map the UserPrincipalName (UPN) attribute to the Unity Connection Alias field; the UPN is guaranteed by Active Directory to be unique across the forest. For additional considerations on the use of the UPN attribute in a multi-tree AD scenario, see the Additional Considerations for Authentication and Microsoft Active Directory, on page 89 section.

If you are using intrasite or intersite networking to network two or more Unity Connection servers that are each integrated with an LDAP directory, do not specify a user search base on one Unity Connection server that overlaps a user search base on another Unity Connection server, or you have user accounts and mailboxes for the same Unity Connection user on more than one Unity Connection server.

Note You can eliminate the potential for duplicate users by creating LDAP filters on one or more Unity Connection servers. See the " Filtering LDAP Users " section in the "LDAP" chapter of the System Administration Guide for Cisco Unity ConnectionRelease 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html .

- **The administrator account in the LDAP directory that Unity Connection uses to access the subtree specified in the user search base.**

  Connection performs a bind to the directory and authenticates using this account. You should use an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set never to expire. (If the password for the administrator account changes, Unity Connection must be reconfigured with the new password.)

  If you create more than one configuration, you should create one administrator account for each configuration and give that account permission to read all user objects only within the corresponding subtree. When creating the configuration, you enter the full distinguished name for the administrator account; therefore the account can reside anywhere in the LDAP directory tree.

- **The frequency with which Unity Connection automatically resynchronizes the Unity Connection database with the LDAP directory, if at all.**

  You can specify the date and time of the next resynchronization, whether the resynchronization occurs just once or on a schedule and, if on a schedule, what you want the frequency to be in hours, days, weeks, or months (with a minimum value of six hours). You should stagger synchronization schedules so that multiple agreements are not querying the same LDAP servers simultaneously. Schedule synchronization to occur during nonbusiness hours.

- **The port on the LDAP server that Unity Connection uses to access LDAP data.**
- **Optionally, whether to use SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server.**
- **One or more LDAP servers.**

  For some LDAP directories, you can specify up to three LDAP directory servers that Unity Connection uses when attempting to synchronize. Unity Connection tries to contact the servers in the order that you specify. If none of the directory servers responds, synchronization fails; Unity Connection tries again at the next scheduled synchronization time. You can use IP addresses rather than host names to eliminate dependencies on Domain Name System (DNS) availability.

Note Not all LDAP directories support specifying additional LDAP directory servers to act as backup in case the LDAP directory server that Unity Connection accesses for synchronization becomes unavailable. For information on whether your LDAP directory supports specifying multiple directory servers, see the " Requirements for an LDAP Directory Configuration " section in the System Requirements for Cisco Unity ConnectionRelease 11.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html .

- **The mapping of LDAP directory attributes to Unity Connection fields, as listed in below Table.**

  Note that the mapping to the Unity Connection Alias field must be the same for all configurations. As you choose an LDAP attribute to map to the Unity Connection Alias field:

  - Confirm that every user that you want to import from the LDAP directory into Unity Connection has a unique value for that attribute.
  - If there are already users in the Unity Connection database, confirm that none of the users that you want to import from the directory has a value in that attribute that matches the value in the Alias field for an existing Unity Connection user.

  Note that for every user that you want to import from the LDAP directory into Unity Connection, the LDAP sn attribute must have a value. Any LDAP user for whom the value of the sn attribute is blank is not imported into the Unity Connection database.

  To protect the integrity of data in the LDAP directory, you cannot use Unity Connection tools to change any of the values that you import. Unity Connection-specific user data (for example, greetings, notification devices, conversation preferences) is managed by Unity Connection and stored only in the local Unity Connection database.

  Note that no passwords or PINs are copied from the LDAP directory to the Unity Connection database. If you want Unity Connection users to authenticate against the LDAP directory, see the LDAP Authentication, on page 87

Table 3: Mapping of LDAP Directory Attributes to Cisco Unity Connection User Fields

LDAP Directory Attribute	Cisco Unity Connection User Field
One of the following: • samAccountName • mail • employeeNumber • telephoneNumber • userPrincipleName	Alias
givenName	First Name
One of the following: • middleName • initials	Initials
SN	Last Name

manager	Manager
department	Department
One of the following: • telephoneNumber • ipPhone	Corporate Phone
One of the following: • mail • samAccountName	Corporate Email Address
title	Title
homePhone	Home (imported but not currently used, and not visible in Unity Connection Administration)
mobile	Mobile (imported but not currently used, and not visible in Unity Connection Administration)
pager	Pager (imported but not currently used, and not visible in Unity Connection Administration)
One of the following: • msRTCSIP-primaryuseraddress • mail • none	Directory URI
display name	Display Name

When clustering (active/active high availability) is configured, all user data, including data imported from the LDAP directory, is automatically replicated from the Unity Connection publisher server to the subscriber server. In this configuration, the Cisco DirSync service runs only on the publisher server.

Note Extension field are not updated with changes to the LDAP phone number. As a result, you can change the LDAP phone number as required, including specifying a completely different number, and the extension is not overwritten the next time that Connection synchronizes data with the LDAP directory.

Creating Unity Connection Users

On a Unity Connection system that is integrated with an LDAP directory, you can create Unity Connection users by importing data from the LDAP directory, converting existing Unity Connection users to synchronize with the LDAP directory, or both. Note the following:

- When you create Unity Connection users by importing LDAP data, Unity Connection takes the values specified in Table 10-1 from the LDAP directory and fills in the remaining information from the Unity Connection user template that you specify.
- When you convert existing users, existing values in the fields in Table 10-1 are replaced with the values in the LDAP directory.

- For any user that you want to import from the LDAP directory, the value in the LDAP attribute that maps to the Unity Connection Alias field cannot match the value in the Unity Connection Alias field for any Unity Connection object (standalone users, users already imported from an LDAP directory, users imported from Cisco Unified Communications Manager via AXL, contacts, distribution lists, and so on).
- After you have synchronized Unity Connection with the LDAP directory, you can continue to add Unity Connection users who are not integrated with the LDAP directory. You can also continue to add Unity Connection users by importing users from Cisco Unified Communications Manager via an AXL Server.
- After you have synchronized Unity Connection with the LDAP directory, new LDAP directory users are not automatically imported into Unity Connection, but must be imported manually.
- After a user has been imported from LDAP, the user page in Cisco Unity Connection Administration identifies the user as an “Active User Imported from LDAP Directory.”
- Subsequently when changes are made to user data in the corporate directory, Unity Connection fields that are populated from the LDAP directory are updated with the new LDAP values during the next scheduled resynchronization.

Filtering LDAP Users

You may want additional control over which LDAP users you import into Cisco Unity Connection for a variety of reasons. For example:

- The LDAP directory has a flat structure that you cannot control sufficiently by specifying user search bases.
- You only want a subset of LDAP user accounts to become Unity Connection users.
- The LDAP directory structure does not match the way you want to import users into Unity Connection. For example:
  - If organizational units are set up according to an organizational hierarchy but users are mapped to Unity Connection by geographical location, there might be little overlap between the two.
  - If all users in the directory are in one tree or domain but you want to install more than one Unity Connection server, you need to do something to prevent users from having mailboxes on more than one Unity Connection server.

In these cases, you may want to use create filters to provide additional control over user search bases. Note the following:

- You can create as many LDAP filters as you want, but you can only have one active filter per Unity Connection directory configuration, up to 20 per server or cluster.
- When you create LDAP directory configurations in Unity Connection, you specify both a user search base and an LDAP filter. As applicable, create filters that integrate with the user search bases that you specify for the maximum of twenty LDAP directory configurations that you can create.
- Each filter must adhere to the LDAP filter syntax specified in RFC 4515, “Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters.”
- The filter syntax is not validated when you create the filter. Instead, it is validated when you specify the filter in an LDAP directory configuration.

- If you add a filter and add it to an LDAP directory configuration that you have already synchronized with the LDAP directory, or if you change a filter that is already in use in an LDAP directory configuration, you must do the following steps for the LDAP users that are specified by the new or updated filter to be accessible to Connection:

  1. Deactivate and reactivate the Cisco DirSync service. In Cisco Unified Serviceability, select **Tools > Service Activation**. Uncheck the check box next to **Cisco DirSync**, and select **Save** to deactivate the service. Then check the check box next to **Cisco DirSync**, and select **Save** to reactivate the service.

  2. In Unity Connection Administration, in the LDAP directory configuration that accesses the filter, perform a full synchronization (select **Perform Full Sync Now**).

- If you change a filter to one that excludes some of the users who were previously accessible, the Unity Connection users who are synchronized with the now-inaccessible LDAP users are converted to standalone Unity Connection users over the next two scheduled synchronizations or within 24 hours, whichever is greater. The users are still able to sign in to Unity Connection by phone, callers can still leave messages for them, and their messages are not deleted. However, they are not able to sign in to Unity Connection web applications while Unity Connection is breaking synchronization for these users. After the synchronization has been broken, their web-application passwords are the passwords that were assigned when their Unity Connection accounts were created.

Unity Connection Multi-Forest LDAP Synchronization

A Unity Connection deployment using a multi-forest LDAP infrastructure can be supported using Active Directory Lightweight Directory Services (AD LDS) as a single forest view integrating with the multiple disparate forests. The integration also requires the use of LDAP filtering. For more information, refer to the document on “How to Configure Unified Communications Manager Integration Directory Integration in a Multi-Forest Environment” available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example019186a0080b2b103.shtml.

LDAP Authentication

Some companies want the convenience of single sign-on credentials for their applications. To authenticate sign-ins to Unity Connection web applications against user credentials in an LDAP directory, you must synchronize Unity Connection user data with user data in the LDAP directory as described in the LDAP Synchronization.

Only passwords for Unity Connection web applications (Cisco Unity Connection Administration for administration, Cisco Personal Communications Assistant for end users), and for IMAP email applications that are used to access Unity Connection voice messages, are authenticated against the corporate directory. You manage these passwords using the administration application for the LDAP directory. When authentication is enabled, the password field is no longer displayed in Cisco Unity Connection Administration.

For telephone user interface or voice user interface access to Unity Connection voice messages, numeric passwords (PINs) are still authenticated against the Unity Connection database. You manage these passwords in Unity Connection Administration; users manage PINs using the phone interface or the Messaging Assistant web tool.

The LDAP directories that are supported for LDAP authentication are the same as those supported for synchronization. See the “Requirements for an LDAP Directory Integration” section in the System Requirements for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Configuring LDAP Authentication

Configuring LDAP authentication is much simpler than configuring synchronization. You specify only the following:

- **A user search base.** If you created more than one LDAP configuration, when you configure authentication, you must specify a user search base that contains all of the user search bases that you specified in your LDAP configurations.
- **The administrator account in the LDAP directory that Unity Connection uses to access the search base.** You should use an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set never to expire. (If the password for the administrator account changes, Unity Connection must be reconfigured with the new password.) You enter the full distinguished name for the administrator account; therefore the account can reside anywhere in the LDAP directory tree.
- **One or more LDAP servers.** You can specify up to three LDAP directory servers that Unity Connection uses when attempting to authenticate. Unity Connection tries to contact the servers in the order that you specify. If none of the directory servers responds, authentication fails. You can use IP addresses rather than host names to eliminate dependencies on Domain Name System (DNS) availability.

Working of LDAP Authentication

When LDAP synchronization and authentication are configured in Cisco Unity Connection, authenticating the alias and password of a user against the corporate LDAP directory works as follows:

1. A user connects to the Cisco Personal Communications Assistant (PCA) via HTTPS and attempts to authenticate with an alias (for example, jsmith) and password.
2. Unity Connection issues an LDAP query for the alias jsmith. For the scope for the query, Unity Connection uses the LDAP search base that you specified when you configured LDAP synchronization in Cisco Unity Connection Administration. If you chose the SSL option, the information that is transmitted to the LDAP server is encrypted.
3. The corporate directory server replies with the full Distinguished Name (DN) of user jsmith, for example, "cn=jsmith, ou=Users, dc=vse, dc=lab".
4. Unity Connection attempts an LDAP bind using this full DN and the password provided by the user.
5. If the LDAP bind is successful, Unity Connection allows the user to proceed to the Cisco PCA.

If all of the LDAP servers that are identified in a Unity Connection LDAP directory configuration are unavailable, authentication for Unity Connection web applications fails, and users are not allowed to access the applications. However, authentication for the phone and voice user interfaces continue to work, because these PINs are authenticated against the Unity Connection database.

When the LDAP user account for a Unity Connection user is disabled or deleted, or if an LDAP directory configuration is deleted from the Unity Connection system, the following occurs:

1. Initially, when Unity Connection users try to sign in to a Unity Connection web application, LDAP authentication fails because Unity Connection is still trying to authenticate against the LDAP directory.

If you have multiple LDAP directory configurations accessing multiple LDAP user search bases, and if only one configuration was deleted, only the users in the associated user search base are affected. Users in other user search bases are still able to sign in to Unity Connection web applications.

2. At the first scheduled synchronization, users are marked as "LDAP inactive" in Unity Connection.

   Attempts to sign in to Unity Connection web applications continue to fail.

3. At the next scheduled synchronization that occurs at least 24 hours after users are marked as "LDAP inactive," all Unity Connection users whose accounts were associated with LDAP accounts are converted to Unity Connection standalone users.

   For each Unity Connection user, the password for Unity Connection web applications and for IMAP email access to Unity Connection voice messages becomes the password that was stored in the Unity Connection database when the user account was created. (This is usually the password in the user template that was used to create the user.) Unity Connection users do not know this password, so an administrator must reset it.

   The numeric password (PIN) for the telephone user interface and the voice user interface remains unchanged.

Note the following regarding Unity Connection users whose LDAP user accounts were disabled or deleted, or who were synchronized via an LDAP directory configuration that was deleted from Unity Connection:

- The users can continue to sign in to Unity Connection by phone during the period in which Unity Connection is converting them from an LDAP-synchronized user to a standalone user.
- Their messages are not deleted.
- Callers can continue to leave messages for these Unity Connection users.

Note LDAP phone numbers are converted to Unity Connection extensions only once, when you first synchronize Unity Connection data with LDAP data. On subsequent, scheduled synchronizations, values in the Connection Extension field are not updated with changes to the LDAP phone number. As a result, you can change the LDAP phone number as required, including specifying a completely different number, and the extension is not overwritten the next time that Connection

Additional Considerations for Authentication and Microsoft Active Directory

When you enable LDAP authentication with Active Directory, you should configure Unity Connection to query an Active Directory global catalog server for faster response times. To enable queries against a global catalog server, in Unity Connection Administration, specify the IP address or host name of a global catalog server. For the LDAP port, specify either 3268 if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server, or 3269 if you are using SSL.

Using a global catalog server for authentication is even more efficient if the users that are synchronized from Active Directory belong to multiple domains, because Unity Connection can authenticate users immediately without having to follow referrals. For these cases, configure Unity Connection to access a global catalog server, and set the LDAP user search base to the top of the root domain.

A single LDAP user search base cannot include multiple namespaces, so when an Active Directory forest includes multiple trees, Unity Connection must use a different mechanism to authenticate users. In this configuration, you must map the LDAP userPrincipalName (UPN) attribute to the Unity Connection Alias field. Values in the UPN attribute, which look like email addresses (username@companyname.com), must be unique in the forest.

Note When an Active Directory forest contains multiple trees, the UPN suffix (the part of the email address after the @ symbol) for each user must correspond to the root domain of the tree where the user resides. If the UPN suffix does not match the namespace of the tree, Unity Connection users cannot authenticate against the entire Active Directory forest. However, you can map a different LDAP attribute to the Unity Connection Alias field and limit the LDAP integration to a single tree within the forest.

For example, suppose an Active Directory forest contains two trees, avvid.info and vse.lab. Suppose also that each tree includes a user whose samAccountName is jdoe. Unity Connection authenticates a sign-in attempt for jdoe in the avvid.info tree as follows:

1. The user jdoe connects to the Cisco Personal Communications Assistant (PCA) via HTTPS and enters a UPN (jdoe@avvid.info) and password.
2. Unity Connection performs an LDAP query against an Active Directory global catalog server using the UPN. The LDAP search base is derived from the UPN suffix. In this case, the alias is jdoe and the LDAP search base is “dc=avvid, dc=info.”
3. Active Directory finds the Distinguished Name corresponding to the alias in the tree that is specified by the LDAP query, in this case, “cn=jdoe, ou=Users, dc=avvid, dc=info.”
4. Active Directory responds via LDAP to Unity Connection with the full Distinguished Name for this user.
5. Unity Connection attempts an LDAP bind using the Distinguished Name and the password initially entered by the user.
6. If the LDAP bind is successful, Unity Connection allows the user to proceed to the Cisco PCA.

Comparison LDAP Integrated Users and Users Created by Importing Data from Cisco Unified CM

An alternative to integrating Unity Connection with an LDAP directory is to create users by importing data from Cisco Unified Communications Manager as described in the “Importing Users through AXL” section of the “Users” chapter of the *System Administration Guide for Cisco Unity Connection, Release 11.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.

Note the following:

- If you import users from Cisco Unified CM and if Cisco Unified CM is integrated with the LDAP directory, Unity Connection does not automatically have access to LDAP synchronization or authentication. If you want Unity Connection users to authenticate against the LDAP directory, you must integrate Unity Connection with the LDAP directory, too.
- If you import users from Cisco Unified CM, updates to Cisco Unified CM data do not automatically replicate to the Unity Connection server, so you must remember to use the Synch Users page in Cisco Unity Connection Administration to manually synchronize Unity Connection user data with Cisco Unified CM

user data from time to time. If you integrate Unity Connection with an LDAP directory, you can define a synchronization schedule that specifies when data in the Unity Connection database is automatically resynchronized with data in the LDAP directory.

Note that when you add users to the LDAP directory, you still need to manually import them into Unity Connection; automatic synchronization only updates the Unity Connection database with new data for existing users, not new data for new users.

- When you integrate Unity Connection with an LDAP directory, you can configure Unity Connection to authenticate passwords for web applications against the LDAP database. When you import data from Cisco Unified CM, you must maintain passwords for Unity Connection web applications in Unity Connection and maintain passwords for Cisco Unified CM web applications in Cisco Unified CM.

CHAPTER 11

Integrating Cisco Unity Connection with Phone System

- Calls to a user extension that does not answer are forwarded to the personal greeting of the user.
- Calls to a user extension that is busy are forwarded to the busy greeting of the user.
- Unity Connection receives caller ID information from the phone system (if available).
- A user has easy access to messages by pressing a button on the phone and entering a password.
- Unity Connection identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated.
- Messages left for a user activate the message waiting indicator (MWI) on the extension.

See the following sections for detailed information:

Working of a Phone System Integration

- Lines and cables necessary to make physical connections (for PIMG/TIMG integrations) or a network connection (in Cisco Unified Communications Manager, Cisco Unified Communications Manager

Express, SIP proxy servers, and QSIG-enabled phone systems). Depending on the type of integration, the phone system connects through different combinations of lines. See the applicable section for more information:

- Settings in the phone system and in Unity Connection. For more information, see the Settings in the Phone System in Unity Connection, on page 96
- Call information exchanged by the phone system and Unity Connection. For more information, see the Call Information Exchanged by Phone System and Unity Connection, on page 96
- Call control (signals used to set up, monitor, and tear down a call) to determine and control the status of the call. For more information, see the Call Control, on page 97

Integration with Cisco Unified Communications Manager

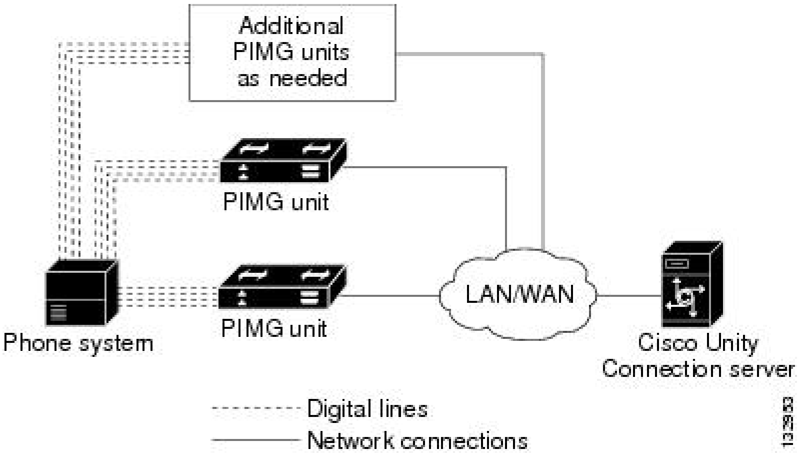
Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and SIP proxy servers use network connections that carry all communication to and from Cisco Unity Connection. Figure shows the network connections used in an integration with Cisco Unified CM.

See the Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP) for additional information.

Digital Integration with Digital PIMG Units

The phone system sends call information, MWI requests, and voice connections through the digital lines, which connect the phone system to the PIMG units (media gateways). The PIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initiation Protocol (SIP). Figure 11-2 shows the connections used in a digital integration using digital PIMG units.

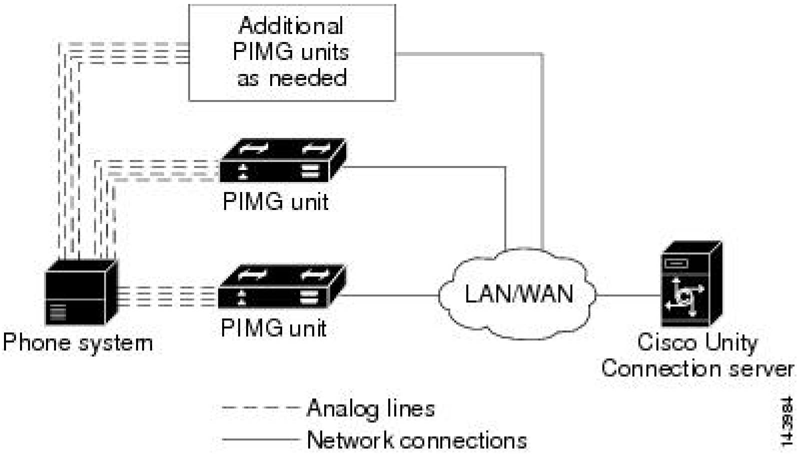
Figure 11: Connections for a Digital Integration Using Digital PIMG Units



DTMF Integration with Analog PIMG Units

The phone system sends call information, MWI requests, and voice connections through the analog lines, which connect the phone system to the PIMG units (media gateways). The PIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initiation Protocol (SIP). Figure 11-3 shows the connections for a DTMF integration using analog PIMG units.

Figure 12: Connections for a DTMF Integration Using Analog PIMG Units



Serial (SMDI, MCI, or MD-110) Integration with Analog PIMG Units

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master PIMG unit (media gateways). Voice connections are sent through the analog lines between the phone system and the PIMG units. The PIMG units communicate with the Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the connections for a serial integration using analog PIMG units.

Figure 13: Connections for a Serial (SMDI, MCI, or MD-110) Integration Using Analog PIMG Units

Note When you use multiple PIMG units, one PIMG unit must be designated the master PIMG unit, which is connected to the serial cable from the phone system. It is not possible to “daisy chain” the serial ports on the PIMG units.

You can add a secondary master PIMG unit to an integration. For details, see the “Adding a Secondary Master PIMG Unit” chapter of the *PIMG Integration Guide for Cisco Unity Connection Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/pimg/b_11xcucintpimg.html.

TIMG Serial (SMDI, MCI, or MD-10) Integration

The TIMG integration uses one or more TIMG units between circuit-switched phone systems and IP networks. On the circuit-switched phone system side, there is a T1-CAS interface. On the IP side, there is a SIP interface, which is how Cisco Unity Connection communicates with the TIMG units. To Unity Connection, the integration is essentially a SIP integration. Unity Connection communicates with the TIMG units over the IP network using SIP and RTP protocols. The TIMG units communicate with the circuit-switched phone system over the phone network using serial protocols (SMDI, MCI, or MD-110).

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master TIMG unit. Voice connections are sent through the T1 digital lines between the phone system and the TIMG units. The TIMG units communicate with the Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the connections for a serial integration using TIMG units.

TIMG In-Band Integration

The phone system sends call information, MWI requests, and voice connections through the T1 digital lines, which connect the phone system and the TIMG units. The TIMG units communicate with the Cisco Unity Connection server through the LAN or WAN using Session Initialization Protocol (SIP). Figure shows the required connections for an in-band integration using TIMG units.

PIMG/TIMG Integrations and Cisco Unified Communications Manager Using Cisco Unified SIP Proxy

The Cisco Unified SIP Proxy allows the PIMG/TIMG integrations and Cisco Unified Communications Manager to share the same voice messaging ports on Unity Connection by acting as a SIP proxy. The Cisco Unified SIP Proxy uses a SIP trunk integration with Unity Connection. Figure shows the connections. For more information, see the application notes for Cisco Unified SIP Proxy at
http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/interOp_sipProxy.html.

Settings in the Phone System in Unity Connection

For an integration to be successful, Unity Connection and the phone system must know the connections to use (for example, IP addresses and channels) and the expected method of communication (for example, IP packets, serial packets, and DTMF tones). Certain integrations require specific codes or extensions for turning MWIs on and off.

There are required settings for Unity Connection, and programming for the phone system, that must be made in order to enable the integration. For information on these settings, see the applicable Cisco Unity Connection integration guide at
http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Call Information Exchanged by Phone System and Unity Connection

The phone system and Unity Connection exchange call information to manage calls and to make the integration features possible. With each call, the following call information is typically passed between the phone system and Unity Connection:

- The extension of the called party.
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the phone system supports caller ID).
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls). There is also a reason code for Direct Calls.

Cisco Unified Communications Manager SCCP and SIP trunk integrations can also provide the following call information:

- Called number
- First redirecting number
- Last redirecting number

Note Unity Connection can use either the first redirecting number or last redirecting number, depending on the setting of the Use Last (Rather than First) Redirecting Number for Routing Incoming Call check box on the System Settings > Advanced > Conversations page in Cisco Unity Connection Administration.

If the phone system sends the necessary information and if Unity Connection is configured correctly, an integration can provide the following integration functionality:

- Call forward to personal greeting
- Call forward to busy greeting
- Caller ID
- Easy message access (a user can retrieve messages without entering an ID because Unity Connection identifies the user based on the extension from which the call originated; a password may be required)
- Identified user messaging (Unity Connection identifies the user who leaves a message during a forwarded internal call, based on the extension from which the call originated)

Call Control

The phone system uses a set of signals to set up, monitor, and release connections for a call. Cisco Unity Connection monitors call control signals to determine the state of the call, and uses these signals to respond appropriately to phone system actions and to communicate with the phone system. For example, a caller who is recording a message might hang up, so Unity Connection detects that the call has ended and stops recording.

Depending on the phone system, the following types of call control signals are used:

Table 4: Call Control Signals

Cisco Unified Communications Manager	For Skinny Call Control Protocol (SCCP) integrations, Cisco Unified Communications Manager generates SCCP messages, which are translated by Cisco Unity Connection. For SIP trunk integrations, Cisco Unified CM sends SIP messages, and Unity Connection sends SIP responses when a call is set up or terminated.
Circuit-switched phone system through PIMG/TIMG units	The phone system sends messages to the PIMG or TIMG units (media gateways), which send the applicable SIP messages to Unity Connection. Unity Connection sends SIP responses when a call is set up or terminated, and the PIMG or TIMG units communicate with the phone system.

Sample Path for a Call from the Phone System to a User

The following steps give an overview of a sample path that an external call can take when traveling from the phone system to a user.

1. For Cisco Unified Communications Manager, when an external call arrives, the gateway sends the call over the LAN or WAN to Cisco Unified CM. Cisco Unified CM routes the call to the Cisco Unity Connection voice mail pilot number.

   For circuit-switched phone systems, when an external call arrives via the PSTN, TI/PRI, DID or LS/GS analog trunks, the phone system routes the call to the Cisco Unity Connection voice mail pilot number.

2. The phone system routes the call to an available Cisco Unity Connection voice messaging port.
3. Unity Connection answers the call and plays the opening greeting.
4. During the opening greeting, the caller enters an extension. For example, the caller enters 1234 to reach a person at that extension.
5. Unity Connection notifies the phone system that there is a call for extension 1234.
6. Depending on whether Unity Connection is set up to perform a release transfer or a supervised transfer, the following occurs:

Release transfer (blind transfer)	Unity Connection passes the call to the phone system, and the phone system sends the call to extension 1234 without waiting to determine whether the line is available. Then the phone system and Unity Connection drop out of the loop. In this configuration, if the customer wants Unity Connection to take a message when a line is busy or unanswered, each phone must be configured to forward calls to Unity Connection when the line is busy or unanswered.
Supervised transfer	While Unity Connection holds the call, the phone system attempts to establish a connection with extension 1234. If the line is available, the phone system connects the call from Unity Connection to extension 1234. The phone system and Unity Connection drop out of the loop, and the call is connected directly from the original caller to extension 1234. If the line is busy or unanswered, the phone system gives that information to Unity Connection, and Unity Connection performs the operation the user has specified. For example, Unity Connection takes a message.

General Integration Issues

For a detailed list of the requirements for a specific integration, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

If Unity Connection is configured for a cluster, see the Balancing the Load of Calls Unity Connection Servers Handle, on page 126 and the Configuration for Dial-Out Voice Messaging Ports, on page 128.

In addition, consider the following list of integration issues:

- Phone systems integrate with Unity Connection only through a network connection.
- The number of voice ports supported with Cisco Unity Connection depends upon the Unity Connection platform specifications. Install only the number of ports that are needed, so that system resources are not allocated to unused ports, and do not exceed the port limitations set for the platform.

For more information on supported platforms, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

For additional information about configuring voice messaging ports, see the “Planning the Usage of Voice Messaging Ports in Cisco Unity Connection” chapter in the applicable Cisco Unity Connection integration guide at
http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Deployment Models for Integrations with Cisco Unified Communications Manager

Cisco Unity Connection and Cisco Unified Communications Manager deployment models, including single-site messaging, centralized messaging, and distributed messaging, can be combined to suit customer requirements. When choosing a deployment model, you must consider a range of issues, for example:

- Centralized messaging allows you to consolidate servers and administration, but requires that you plan for access to voice messages in the event of WAN outages and that you perform the appropriate QOS/capacity planning for voice-messaging traffic and call traffic.
- Distributed messaging may require more servers and administrative overhead, but, combined with distributed call processing, requires less capacity on intersite WAN links.

For a detailed explanation of deployment models and their relative merits, see the “Collaboration System Components and Architecture” chapter in *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)* available at
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html.

Deploying Phones Across the WAN

Some deployment models, such as centralized messaging with distributed call processing, require placement of phones across the WAN from the Unity Connection server. When deploying phones across the WAN from the Unity Connection server, see the “Collaboration System Components and Architecture” chapter in *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)* available at
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html.

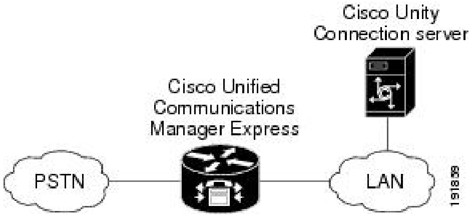
For guidance on capacity planning and call admission control (CAC) for these phones. When integrating Cisco Unity Connection with a circuit-switched phone system (TDM PBX), see the *PIMG Integration Guide* or the *TIMG Integration Guide* at
http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html for

capacity planning for the PIMG/TIMG units deployed at these remote/branch sites to support phones at these sites.

Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP)

Cisco Unity Connection supports Cisco Unified Communications Manager Express integrations through both SCCP and SIP interfaces. Figure 14: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN shows the connections.

Figure 14: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN


Cisco Unity Connection server
Cisco Unified Communications Manager Express
PSTN
LAN
191839

See Table 5: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express) for information on the differences in these integration methods.

Table 5: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express)

Feature	SCCP	SIP
Communication method	SCCP	SIP trunk
Cisco Unity Connection cluster (active/active high availability)	Supported	Supported
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM Express versions	All versions	Versions 3.4 and later
Cisco Unified CM Express authentication and encryption	Not supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Unity Connection and Cisco Unified Communications Manager Express versions, see the *Compatibility Matrix for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html

For information on how to integrate Unity Connection with Cisco Unified CM Express, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Unity Connection with Cisco Unified CM Express, see the Integrating Using SIP, on page 113.

Cisco Unified Communications Manager Authentication and Encryption for Unity Connection Voice Messaging Ports

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Unity Connection and Cisco Unified Communications Manager. Possible threats include:

- Man-in-the-middle attacks, in which an attacker intercepts and changes the data flowing between Cisco Unified CM and Unity Connection voice messaging ports.
- Network traffic sniffing, in which an attacker captures phone conversations and signaling information that flow between Cisco Unified CM, the Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM.
- Changing the call signaling between the Unity Connection voice messaging ports and Cisco Unified CM.
- Changing the media stream between Unity Connection voice messaging ports and endpoints, for example, phones or gateways.
- Identity theft of the Unity Connection voice messaging port, in which a non-Unity Connection device presents itself to Cisco Unified CM as a Unity Connection voice messaging port.
- Identity theft of the Cisco Unified CM server, in which a non-Cisco Unified CM server presents itself to Unity Connection voice messaging ports as a Cisco Unified CM server.

Cisco Unified Communications Manager Security Features

Cisco Unified Communications Manager Release 4.1(3) or later for SCCP integrations or Cisco Unified Communications Manager Release 5.x or later for SIP trunk integrations can secure the connection with Cisco Unity Connection against security threats. The Cisco Unified CM security features that Unity Connection can take advantage of are described in Table 6: Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity Connection.

Table 6: Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity Connection

Security Feature	Description
Signaling authentication	Uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Modification of the call signaling. • Identity theft of the Unity Connection voice messaging port. • Identity theft of the Cisco Unified CM server.
Device authentication	Validates the identity of the device. This process occurs between Cisco Unified CM and the Unity Connection voice messaging ports when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Modification of the media stream. • Identity theft of the Unity Connection voice messaging port. • Identity theft of the Cisco Unified CM server.

Security Feature	Description
Signaling encryption	Uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP and SIP signaling messages that are sent between the Unity Connection voice messaging ports and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and the Unity Connection voice messaging ports. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and the Unity Connection voice messaging ports.
Media encryption	Uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711 to ensure that only the intended recipient can interpret the media streams between the Unity Connection voice messaging ports and endpoints (for example, phones or gateways). Only audio streams are encrypted. Media encryption creates a media master key pair for the devices, delivers the keys to Unity Connection and the endpoint, and secures the delivery of the keys while the keys are in transport. Unity Connection and the endpoint use the keys to encrypt and decrypt the media stream. This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and the Unity Connection voice messaging ports. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, the Unity Connection voice messaging ports, and IP phones that are managed by Cisco Unified CM. Authentication and signaling encryption are required for media encryption; that is, if the devices do not support authentication and signaling encryption, media encryption cannot occur.

Note that Cisco Unified CM authentication and encryption protects only calls to Unity Connection. Messages that are recorded on Unity Connection are not protected by Cisco Unified CM authentication and encryption but can be protected by the Unity Connection secure messaging feature.

For more information on secure messaging, see the "Securing User Messages in Cisco Unity Connection" chapter of the Security Guide for Cisco Unity Connection *Release 11.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

The security features (authentication and encryption) between Unity Connection and Cisco Unified CM require the following for SCCP integrations:

- A Cisco Unified CM CTL file that lists all Cisco Unified CM servers that are entered in Cisco Unity Connection Administration for secure clusters.
- A Unity Connection server root certificate for each Unity Connection server that uses authentication and/or encryption. A root certificate is valid for seven years from the time it was created.
- Unity Connection voice messaging port or port group device certificates that are rooted in the Unity Connection server root certificate, and voice messaging ports or port groups that are present when registering with the Cisco Unified CM server.

The process of authentication and encryption of Unity Connection voice messaging SCCP ports occurs as follows:

1. Each Unity Connection voice messaging port connects to the TFTP server, via TFTP port 69, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Unity Connection voice messaging port establishes a network connection to the Cisco Unified CM TLS port. By default, the TLS port is 2443, though the port number is configurable.
3. Each Unity Connection voice messaging port establishes a TLS connection to the Cisco Unified CM server, at which time the device certificate is verified and the voice messaging port is authenticated.
4. Each Unity Connection voice messaging port registers with the Cisco Unified CM server, specifying whether the voice messaging port also uses media encryption.

The process of authentication and encryption of Unity Connection voice messaging SIP port groups occurs as follows:

1. Each Unity Connection voice messaging port group connects to the TFTP server, via TFTP port 69, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Unity Connection voice messaging port group establishes a network connection to the Cisco Unified CM TLS port. By default, the TLS port is 2443, though the port number is configurable.
3. Each Unity Connection voice messaging port group establishes a TLS connection to the Cisco Unified CM server, at which time the device certificate is verified and the voice messaging port group is authenticated.
4. Each Unity Connection voice messaging port group registers with the Cisco Unified CM server, specifying whether the voice messaging port group also uses media encryption.

Data is Encrypted

When a call is made between Cisco Unity Connection and Cisco Unified CM, the call-signaling messages and the media stream are handled in the following manner:

- If both endpoints are set for encrypted mode, the call-signaling messages and the media stream are encrypted.
- If one endpoint is set for authenticated mode and the other endpoint is set for encrypted mode, the call-signaling messages are authenticated. But neither the call-signaling messages nor the media stream are encrypted.
- If one endpoint is set for non-secure mode and the other endpoint is set for encrypted mode, neither the call-signaling messages nor the media stream are encrypted.

Cisco Unified Communications Manager Cluster Security Mode Settings in Unity Connection

The Security Mode settings in Cisco Unity Connection Administration determine how the ports handle call-signaling messages and whether encryption of the media stream is possible. Table 7: Security Mode Settings for Voice Messaging Ports in an SCCP Integration describes the effect of the Security Mode settings on the Telephony Integrations > Port > Port Basics page for each port in an SCCP integration.

Table 7: Security Mode Settings for Voice Messaging Ports in an SCCP Integration

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text and are connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted.
Authenticated	The integrity of call-signaling messages is ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages is not ensured because they are sent as clear (unencrypted) text. In addition, the media stream is not encrypted. **Note** You can ensure the integrity of call-signaling messages for the audio a calls using the authenticated TLS port.

Setting	Effect
Encrypted	The integrity and privacy of call-signaling messages is ensured because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream can be encrypted. **Caution** Both endpoints must be registered in encrypted mode for the media stream to be encrypted. However, when one endpoint is set for non-secure or authenticated mode and the other endpoint is set for encrypted mode, the media stream is not encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream is not encrypted.

Disabling and Re-enabling Security

The authentication and encryption features between Cisco Unity Connection and Cisco Unified CM can be enabled and disabled by changing the Security Mode for all Cisco Unified CM clusters to Non-Secure, and by changing the applicable settings in the Cisco Unified Communications Manager Administration.

Authentication and encryption can be reenabled by changing the Security Mode to Authenticated or Encrypted.

Note After disabling or re-enabling authentication and encryption, it is not necessary to export the Unity Connection server root certificate and copy it to all Cisco Unified CM servers.

Multiple Clusters with Different Security Mode Settings

When Cisco Unity Connection has multiple Cisco Unified CM phone system integrations, each Cisco Unified CM phone system integration can have different Security Mode settings. For example, one Cisco Unified CM phone system integration can be set to Encrypted, and a second Cisco Unified CM phone system integration can be set to Non-Secure.

Settings for Individual Voice Messaging Ports

For troubleshooting purposes, authentication and encryption for Cisco Unity Connection voice messaging ports can be individually enabled and disabled. At all other times, the Security Mode setting for all individual voice messaging ports in a Cisco Unified CM port group should be the same.

Packetization

The Real-Time Transport Protocol (RTP) is used to send and receive audio and video packets over the IP network. Each discrete packet has a fixed-size header, but the packets themselves can vary in size, depending on the size of the audio stream to be transported (which varies by codec) and the packetization setting. This variable size function helps utilize network bandwidth more efficiently. Reducing the number of packets that are created per call sends fewer total bytes over the network.

Packetization is set in the Cisco Unified CM Service Parameters, in the Preferred G711 Millisecond PacketSize and Preferred G729 Millisecond PacketSize parameters. Cisco Unity Connection supports any packet size up to 30ms for G.711 audio, and any packet size up to 60 ms for G.729a audio. The default setting is 20ms for both; there may be latency issues with lower settings.

DSCP is a priority setting on each packet. DSCP helps intermediary routers manage network congestion and lets them know which packets to prioritize ahead of others. Following Cisco AVVID standards, Unity Connection marks the SCCP and SIP packets (call control) with a default DSCP value of 24 (the TOS octet is 0x60), and the RTP packets (audio and video traffic) with a default DSCP value of 46 (the TOS octet is 0xB8). Thus, the RTP audio and video packets can be assigned priority over other packets using the router settings. Note that even though Cisco Unified CM allows you set different DSCP values, when integrated with Unity Connection, the DSCP values set by Unity Connection always take precedence. The marking of both SCCP and SIP packets is configurable in Unity Connection on the System Settings > Advanced > Telephony Configuration page in Cisco Unity Connection Administration.

With each new audio stream (once per call), Cisco Unified CM tells Unity Connection which packet size to use, and Unity Connection sets the DSCP priority for the stream. The entire stream (call) stays at the specified packet size and priority. For example, an audio stream could be broken up into packets of 30ms each. A 30ms G.729a audio stream would be 30 bytes plus the header per packet, and a 30ms G.711 stream would be 240 bytes plus the header per packet. For information on setting Cisco Unified CM Service Parameters, see the Cisco Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Note You can change the codecs that Unity Connection advertises on the Telephony Integrations > Port Group > Edit Codec Advertising configuration page in Cisco Unity Connection Administration.

For a discussion of supported advertised or “on the line” audio codecs and system-level recording audio codecs, see the Audio Codecs, on page 23.

Port Group Configuration for Cisco Unified Communications Manager Cluster Failover

For Cisco Unified Communications Manager SCCP integrations, when a Cisco Unified CM cluster is configured and Cisco Unified CM failover occurs as calls are in progress, the voice messaging ports may experience a delay registering with the secondary Cisco Unified CM server.

Unity Connection ports can register more quickly after Cisco Unified CM failover occurs if the port groups are configured as follows:

- You create two port groups for the SCCP integration:
    - The first port group contains half the voice messaging ports for the Cisco Unified CM integration (including answering and dialout ports) configured as described in the applicable chapter of the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 11.x*.
    - The second port group contains the remaining half of the ports for the Cisco Unified CM integration (including answering and dialout ports) as described in the applicable chapter of the same guide.

Note The *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 11.x.* is available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/cucm_sccp/b_cucintcucmskinny.html.

- On the Telephony Integrations > Port Group > Port Group Basics > Edit Servers page, you list the Cisco Unified CM servers in different orders:
  - For the first port group, the Cisco Unified CM servers are listed in the order specified in the applicable chapter of the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection Release 11.x*.
  - For the second port group, the Cisco Unified CM servers are listed in the reverse order.

Internet Protocol Version 6 (IPv6) Support with Cisco Unified Communications Manager Integrations

Cisco Unity Connection supports IPv4, IPv6, or dual-stack (IPv4 and IPv6) addressing with Cisco Unified Communications Manager phone system integrations via SCCP or SIP. When IPv6 is enabled, Connection can obtain an IPv6 address either through router advertisement, through DHCP, or by manually configuring an address either in Cisco Unified Operating System Administration or using the command-line interface.

For SCCP integrations with Cisco Unified CM, if Unity Connection is configured to listen for incoming IPv4 and IPv6 traffic, you can configure the addressing mode that Unity Connection uses for call control signaling for each port group to use either IPv4 or IPv6. (This mode is also used when connecting to a TFTP server.)

For SIP integrations with Cisco Unified CM, if Unity Connection is configured to listen for incoming IPv4 and IPv6 traffic, you can configure the addressing mode that Unity Connection uses for call control signaling for each port group to use either IPv4 or IPv6. (This mode is also used when connecting to a TFTP server.) In addition, you can configure the addressing mode that Unity Connection uses for media for each port group to use either IPv4 or IPv6.

IPv6 support is disabled by default. You can enable IPv6 and configure IPv6 address settings either in Cisco Unified Operating System Administration or in the CLI. For information on enabling and configuring IPv6 when setting up a new Cisco Unified CM integration, see the applicable Cisco Unity Connection integration guide at
http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

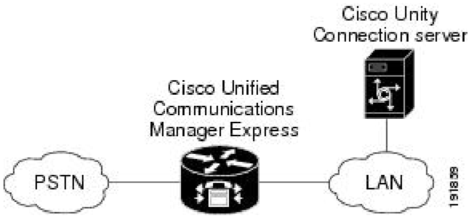
Note the following considerations when deploying IPv6 for Cisco Unified CM integrations:

- The CTL file required for security features (authentication and encryption) between Unity Connection and Cisco Unified CM for SCCP integrations uses IPv4 addressing. Therefore, in order to use authentication and/or encryption with SCCP, you must use either IPv4 or dual-stack addressing.
- Some versions of Cisco Adaptive Security Appliance (ASA) do not support application inspection for IPv6 traffic for Unified Communications application servers and endpoints. You should not be using IPv6 for Unified Communications if you are using a Cisco ASA version that does not provide this support. See the documentation for your version of Cisco ASA to determine whether application inspection is supported in your deployment.

Integrating with Cisco Unified Communications Manager Express (Using SCCP or SIP)

Cisco Unity Connection supports Cisco Unified Communications Manager Express integrations through both SCCP and SIP interfaces. Figure 15: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN shows the connections.

Figure 15: Cisco Unity Connection SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN



See Table 8: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express) for information on the differences in these integration methods.

Table 8: Differences Between SCCP and SIP Integration Methods (Integration with Cisco Unified Communications Manager Express)

Feature	SCCP	SIP
Communication method	SCCP	SIP trunk
Cisco Unity Connection cluster (active/active high availability)	Supported	Supported
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM Express versions	All versions	Versions 3.4 and later
Cisco Unified CM Express authentication and encryption	Not supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Unity Connection and Cisco Unified Communications Manager Express versions, see the *Compatibility Matrix for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html

For information on how to integrate Unity Connection with Cisco Unified CM Express, see the applicable Cisco Unity Connection integration guide at
http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Unity Connection with Cisco Unified CM Express, see the Integrating Using SIP, on page 113.

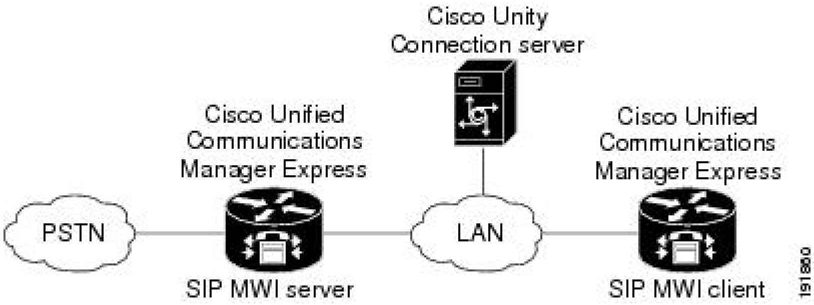
Multiple Cisco Unified Communications Manager Express Version Support

A single Cisco Unity Connection server can support multiple versions of Cisco Unified CM Express. The version of Unity Connection being used must support all versions of Cisco Unified CM Express. See the *Compatibility Matrix for cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html .

Multiple Cisco Unified Communications Manager Express Routers Integrating with a Single Cisco Unity Connection Server

A single, centralized Unity Connection server can be used by multiple Cisco Unified CM Express routers. This configuration requires that one Cisco Unified CM Express router be on the same LAN as the Unity Connection server, and that this Cisco Unified CM Express router register all Unity Connection voice messaging ports. This Cisco Unified CM Express router (the SIP MWI server) is a proxy server that relays SIP MWI messages between the Unity Connection server and all other Cisco Unified CM Express routers (the SIP MWI clients). Note that Unity Connection voice messaging ports register only with the SIP MWI server (the Cisco Unified CM Express router that is on the same LAN as the Unity Connection server), not with the SIP MWI clients. See Figure 11-9.

Figure 16: Connections between Multiple Cisco Unified CM Express Routers and a Single Cisco Unity Connection Server



For information on configuring Unity Connection to support multiple Cisco Unified CM Express routers, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

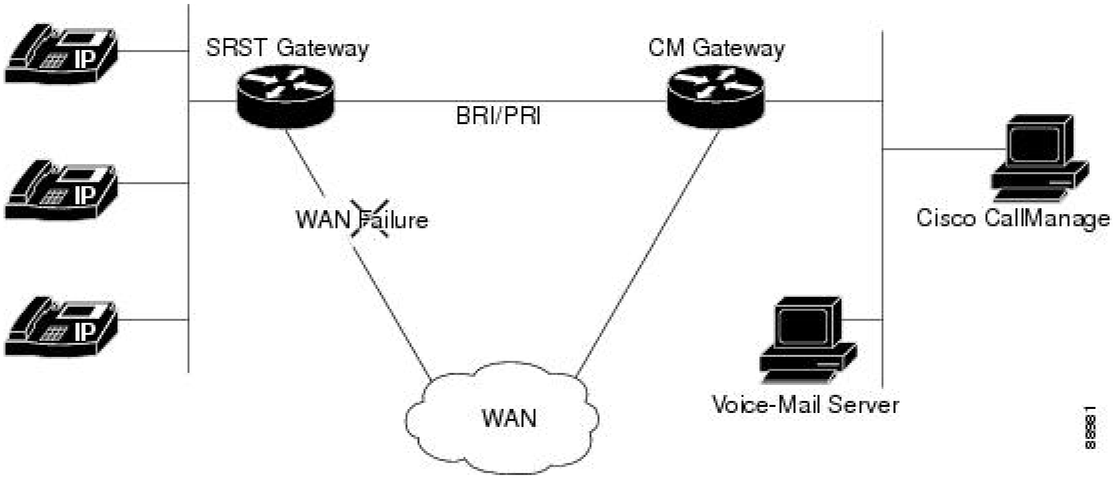
Integrating Unity Connection with Multiple Versions of Cisco Unified CM and Cisco Unified Communications Manager Express

A single Cisco Unity Connection server can support multiple versions of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. The Unity Connection version must support all versions of Cisco Unified CM and/or Cisco Unified CM Express. See the Compatibility Matrix for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

Integrating Unity Connection with Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)

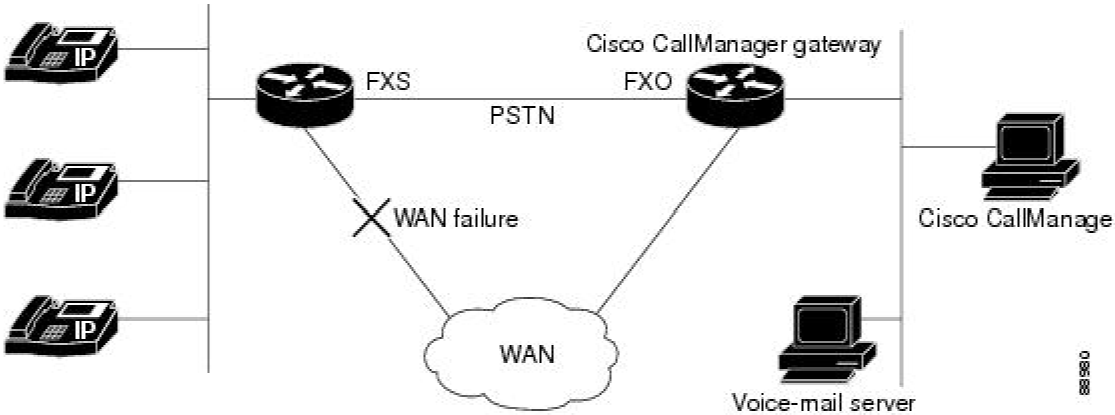
Cisco Unified Survivable Remote Site Telephony (SRST) can direct calls to Unity Connection during Cisco Unified CM fallback. When the WAN is down and Unity Connection has Basic Rate Interface (BRI) or Primary Rate Interface (PRI) access to the Cisco Unified SRST system, Unity Connection uses ISDN signaling (see Figure 11-10).

Figure 17: Cisco Unified Communications Manager Fallback with BRI or PRI



When the WAN is down and Unity Connection has foreign exchange office (FXO) or foreign exchange station (FXS) access to a public switched telephone network (PSTN), Unity Connection uses in-band dual tone multifrequency (DTMF) signaling (see Figure 11-11).

Figure 18: Cisco Unified Communications Manager Fallback with PSTN



In both configurations, phone message buttons remain active and calls to busy or unanswered numbers are forwarded to Unity Connection. The installer must configure access from the dial peers to the voice-mail system, and establish routing to Unity Connection for busy and unanswered calls and for the message button.

If Unity Connection is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for Unity Connection so it can access the correct voice-mail system mailbox.

When using Cisco Unified SRST with Unity Connection, the integration has the following limitations during a WAN outage:

- **Call forward to busy greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Unity Connection, the busy greeting cannot play.
- **Call forward to internal greeting**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Unity Connection, the internal greeting cannot play. Because the PSTN provides the calling number of the FXO line, the caller is not identified as a user.
- **Call transfers**—Because an access code is needed to reach the PSTN, call transfers from Unity Connection to a branch office fails.
- **Identified user messaging**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a user at a branch office leaves a message or forwards a call, the user is not identified. The caller appears as an unidentified caller.
- **Message waiting indication**—MWIs are not updated on branch office phones, so MWIs do not correctly reflect when new messages arrive or when all messages have been listened to. The resynchronizing of MWIs after the WAN link is re-established.
- **Message notification**—Because an access code is needed to reach the PSTN, message notifications from Unity Connection to a branch office fails.
- **Routing rules**—When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call arrives from a branch office to Unity Connection (either a direct or forwarded call), routing rules fail.

When the Cisco Unified SRST router uses PRI or BRI connections, the caller ID for calls from a branch office to Unity Connection may be the full number (exchange plus extension) provided by the PSTN and therefore may not match the extension of the Unity Connection user. In this case, you can let Unity Connection recognize the caller ID using alternate extensions.

When using Cisco Unified SRST, Redirected Dialed Number Information Service (RDNIS) must be supported.

For information on setting up Cisco Unified SRST routers, see the "Integrating Voice Mail with Cisco Unified SRST" chapter of the applicable *Cisco Unified SRST System Administrator Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html.

Impact of Non-Delivery of RDNIS on Voice Mail Calls Routed Using AAR

RDNIS must be supported when using Automated Alternate Routing (AAR).

AAR can route calls over the PSTN when the WAN is oversubscribed. However, when calls are rerouted over the PSTN, RDNIS can be affected. Incorrect RDNIS information can affect voice mail calls that are rerouted over the PSTN by AAR when Cisco Unity Connection is remote from its messaging clients. If the RDNIS information is not correct, the caller does not reach the mailbox of the dialed user but instead hears the automated attendant prompt, and might be asked to reenter the extension number of the party the caller wants to reach. This behavior is primarily an issue when the phone carrier is unable to ensure RDNIS across the network. There are numerous reasons why the carrier might not be able to ensure that RDNIS is properly sent.

Check with your carrier to determine whether it provides guaranteed RDNIS delivery end-to-end for your circuits. The alternative to using AAR for oversubscribed WANs is simply to let callers hear reorder tone in an oversubscribed condition.

Integrating Unity Connection with Cisco Unified Communications Manager Express in SRST Mode

Cisco Unity Connection supports a topology with centralized call processing and distributed messaging, in which your Unity Connection server is located at a remote site or branch office and registered with Cisco Unified CM at a central site.

When the WAN link fails, the phones fall back to the Cisco Unified CM Express-as-SRST device. Unity Connection can also fall back to the Cisco Unified CM Express-as-SRST device, which lets users at the remote site access their voice messages and see message waiting indicators (MWIs) during a WAN outage. Note that MWIs must be resynchronized from the Unity Connection server whenever a failover happens from Cisco Unified CM to Cisco Unified CM Express-as-SRST or vice versa.

For information on setting up this configuration, see the *Integrating Cisco Unity Connection with Cisco Unified CME-as-SRST* configuration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html.

Survivable Remote Site Voicemail

Cisco Unity Connection Survivable Remote Site Voicemail (Unity Connection SRSV) is a backup voicemail solution that works in conjunction with Cisco Unified Survivable Remote Site Telephony (SRST) for providing voicemail service to a branch during WAN outages.

Unity Connection SRSV is used in the centralized Cisco Unified Communications Manager and Cisco Unity Connection environment with multiple branch offices or small sites. It provides limited voicemail and auto-attendant features that remain in synchronization with the central Unity Connection voicemail service so that when the WAN outage or failure occurs, the Unity Connection SRSV solution can provide voicemail service to the subscribers at the branch. However, as soon as the network is restored, all the voicemails received by the branch subscribers are automatically uploaded to the central Unity Connection voicemail server.

For more information on how to configure Cisco Unity Connection SRSV at central Connection location, see the Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) for Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/srsv/guide/b_11xcucsrsvx.html.

Integrating Using SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force standard for multimedia calls over IP. SIP is a peer-to-peer, ASCII-based protocol that uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points. See Table 9: SIP Network Components.

Table 9: SIP Network Components

Component	Description
SIP proxy server	An intermediate device that receives SIP requests from a client and then forwards the requests on behalf of the client. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
Redirect server	Provides information to the client about the next hop or hops that a message should take. The client then contacts the next hop server or user-agent server directly.
Registrar server	Processes requests from user agent clients for registration of their current location. Registrar servers are often installed on the redirect or proxy server.
Phones	Acts as either a server or client. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
Gateways	Provide call control. Gateways provide many services; the most common is a translation function between SIP call endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway translates between audio and video codecs, and performs call setup and clearing on both the LAN side and the switched-circuit network side.

Cisco Unity Connection accepts calls from a proxy server. Unity Connection relies on a proxy server or call agent to authenticate calls.

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a conference (call or session) between two or more endpoints. A single call may involve several clients and servers.

Users in a SIP network are identified by:

- A unique phone or extension number.
- A unique SIP address, which is similar to an email address and uses the format sip:<userID>@<domain>. The user ID can be either a user name or an E.164 address.

When a user initiates a call, a SIP request typically goes to a SIP server (either a proxy server or a redirect server). The request includes the caller address (From) and the address of the called party (To).

SIP messages are in text format using ISO 10646 in UTF-8 encoding (like HTML). In addition to the address information, a SIP message contains a start-line specifying the method and the protocol, a number of header fields specifying call properties and service information, and an optional message body which can contain a session description.

Supported SIP Integrations

Unity Connection supports the following SIP integrations:

- SIP trunks to supported versions of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. For a list of Cisco Unified CM and Cisco Unified CM Express versions supported as SIP trunks, see SIP Trunk Compatibility Matrix: Cisco Unity Connection, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.
- Cisco SIP Proxy Server (CSPS).
- Cisco ISR voice gateways for integrating Unity Connection to a QSIG-enabled phone system (see the Integrating Unity Connection with a QSIG-Enabled Phone System Using Cisco ISR Voice Gateways, on page 121).

Third-party SIP trunks are currently not supported.

For more information on configuring SIP trunks between Unity Connection and Cisco Unified CM or Cisco Unified CM Express, see the applicable SIP trunk integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Note Cisco Unity Connection extracts Caller Id from Remote Party Id field and FROM field in SIP Invite. In addition, when the Remote Party Id option is unchecked on CUCM SIP trunk and the FROM field is set to Anonymous in a SIP header, Connection treats the caller as unknown.

Integrating with Circuit-Switched Phone Systems Using PIMG or TIMG Units

Cisco Unity Connection can integrate with circuit-switched phone systems using the PIMG or TIMG units (media gateways) between circuit-switched phone systems and IP networks.

For a list of circuit-switched phone systems supported with Unity Connection using PIMG and TIMG integrations, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Description of PIMG Integrations

The PIMG integration uses one or more PIMG units between the circuit-switched phone systems and IP network. On the circuit-switched phone system side, there are both digital (feature-set) and analog interfaces; the interface used depends on the phone system to which Cisco Unity Connection is connected. On the IP side, there is a SIP interface, which is how Unity Connection communicates with the PIMG units. To Unity Connection, the integration is essentially a SIP integration. Unity Connection communicates with the PIMG units over the IP network using SIP and RTP protocols. The PIMG units communicate with the circuit-switched phone system over the phone network using phone system-specific protocols (digital, analog, or serial).

For high-level descriptions of each PIMG integration type, and illustrations showing the network connections, see the Working of a Phone System Integration, on page 93.

Setup and Configuration

For PIMG/TIMG setup and configuration, the installer does the following steps as documented in the applicable integration guide:

1. Configure the phone system.
2. Configure the PIMG/TIMG units. PIMG/TIMG settings are somewhat phone system-specific, but less so than phone system configuration.
3. Configure Cisco Unity Connection for the integration.

For information on configuring the phone system, PIMG/TIMG units, and Unity Connection, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Firmware Updates

Note that when receiving shipment of PIMG or TIMG units, it may be necessary to update the firmware on the units. The PIMG/TIMG Administration interface provides a simple method to update the firmware files. Firmware updates are available at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240 (note that you must sign in to www.cisco.com to access the URL). For details, see the applicable integration guide.

Serial Integrations

Cisco Unity Connection supports the following serial protocols:

- SMDI
- MCI
- MD-110

The serial port on PIMG/TIMG units was originally designed as a management port rather than as a standard RS-232 serial port. Consequently, a custom serial cable (which is available from Cisco) is necessary for the data link between the phone system and the master PIMG/TIMG unit.

Increasing Port Capacity

PIMG units have eight ports. To increase system port capacity, multiple PIMG units can be stacked. For example, if 32 ports are needed, four PIMG units can be stacked.

TIMG units, which integrate with circuit-switched phone systems that support T1-CAS, have 24 T1 ports per span in a single rack-optimized unit. Single-span, dual-span, and quad-span TIMG units are available.

Unity Connection Clusters

PIMG/TIMG integrations support Unity Connection clusters (active/active high availability). Configuration changes are required both for the PIMG/TIMG units and for the Unity Connection servers, as described in the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Multiple Integration Support/Branch Office Consolidation

PIMG/TIMG units can be separated by a WAN to support circuit-switched phone systems at remote branch office sites. For example, Cisco Unity Connection could be placed at a centralized headquarters and support circuit-switched phone systems both at the headquarters and at the branch office sites.

As an example, assuming there are four phone systems from four different manufacturers (for example, Nortel, Avaya, NEC, and Siemens), four different phone system integrations could be created on the Unity Connection server to support the four phone systems. A standalone Unity Connection server supports up to 144 ports that connects to the four phone systems. For example:

- At the Seattle site, 15 PIMG units can be stacked to support 120 ports.
- At the New York site, two PIMG units can be stacked to support 16 ports.
- At the Tokyo site, one PIMG unit can be used to support four ports.
- At the Dallas site, one PIMG unit can be used to support two ports.

Note that even though the PIMG units come with eight ports, fewer than eight ports can be used on each unit.

If PIMG units are separated by a WAN to support remote phone systems, correct audio codec selection, bandwidth capacity planning, and QOS planning are required. Both the G.729a and G.711 audio codecs are supported by PIMG units and by Unity Connection. Because PIMG units are Dialogic devices rather than Cisco devices, the use of location-based CAC is not applicable. The following network and bandwidth requirements are required when placing the PIMG across a WAN:

- For the G.729a audio codec, a minimum of 32.76 Kbps (assumes Ethernet, payload of 20 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port.
- For the G.711 audio codec, a minimum of 91.56 Kbps (assumes Ethernet, payload of 160 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port.
- No network devices that implement network address translation (NAT).

When PIMG units are separated by a WAN, prioritize your call control and media traffic through proper QOS traffic, marking for voice traffic originating on the PIMG units. Set the Call Control QOS Byte and RTP QOS Byte on PIMG units to the following values:

- In the Call Control QOS Byte field, enter 104.
- In the RTP QOS Byte field, enter 184.

Note that the Call Control QOS Byte and RTP QOS Byte fields on PIMG units define a decimal value that represents QOS bit flags. These values can be interpreted as either IPv4 TOS or Differentiated Services Codepoint (DSCP). For more details, see the *Dialogic 1000 and 2000 Media Gateway Series User's Guide*, provided by Dialogic.

Integrating with Multiple Phone Systems

Unity Connection supports as many phone systems as needed up to the maximum number of ports supported per Unity Connection server or active/active server pair. See the *Multiple Phone System Integration Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/multiple_integration/b_cuc11xintmultiple.html.

Requirements for Integrations with Multiple Phone Systems

Unity Connection has the following requirements for multiple phone system integrations:

- All phone system and Unity Connection server requirements have been met. See the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
- There must be an adequate number of voice messaging ports on the Unity Connection server to connect to the phone systems.

Alternate Extensions

In addition to the primary extension for each user, you can set up alternate extensions. Alternate extensions can be used for various reasons, such as handling multiple line appearances on user phones. Alternate extensions can also make calling Cisco Unity Connection from an alternate device—such as a mobile phone, a home phone, or a phone at another work site—more convenient.

When you specify the phone number for an alternative extension, Unity Connection handles all calls from that number in the same way that it handles calls from a primary extension (assuming that ANI or caller ID is passed along to Unity Connection from the phone system). This means that Unity Connection associates the alternate phone number with the user account, and when a call comes from that number, Unity Connection prompts the user to enter a password and sign in.

URI Dialing for Alternate Extensions

Unity Connection supports dialing using URIs for alternate extensions. URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. A URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone then Cisco Unity Connection can route calls to that phone using the URI. URI dialing is available for both SIP endpoints that support URIs.

The administrator can import the end users directory URI into Unity Connection from the LDAP directory or Cisco Unified Communications Manager.

Note In HTTPS, CCI, and Diginet networking, URI for alternate extensions is replicated only on the nodes that support directory URI.

Directory URI Format

URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. The URI field has a maximum length of 40 characters.

Unity Connection supports the following formats for URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

Unity Connection supports the following formats in the user portion of a URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, \, ?, \, ', ,, ., /, "", {}, []. <>.
- The user portion is case sensitive.

Unity Connection supports the following formats in the host portion of a URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z, 0-9, hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of one character.
- The host portion is case sensitive.

Note Use lower case for URIs.

Alternate MWIs

You can set up Cisco Unity Connection to activate alternate MWIs when you want a new message for a user to activate the MWIs at up to 10 extensions. For example, a message left at extension 1001 can activate the MWIs on extensions 1001 and 1002.

Unity Connection uses MWIs to alert the user to new voice messages. MWIs are not used to indicate new email, fax, or return receipt messages.

Centralized Voice Messaging

Cisco Unity Connection supports centralized voice messaging through the phone system, which supports various inter-phone system networking protocols including proprietary protocols such as Avaya DCS, Nortel MCDN, or Siemens CorNet, and standards-based protocols such as QSIG or DPNSS. Note that centralized voice messaging is a function of the phone system and its inter-phone system networking, not voice mail. Unity Connection supports centralized voice messaging as long as the phone system and its inter-phone system networking are properly configured.

When discussing phone systems involved in centralized voice messaging, there are essentially two types:

- **Message Center PINX**—The phone system hosts the voice messaging system (the phone system is directly connected to the voice messaging system).
- **User PINX**—The phone system is remote from the voice messaging system (the phone system is not directly connected to the voice messaging system).

Centralized voice messaging provides voice messaging services to all users in a networked phone system environment. Unity Connection can be hosted on a message center PINX and provide voice messaging services to all users in an enterprise assuming the message center PINX and all user PINX phone systems are properly networked.

For a centralized voice messaging configuration to exist, a suitable inter-phone system networking protocol must exist to deliver a minimum level of feature support, such as:

- Message waiting indication (MWI).
- Transfer, which ensures that the correct calling/called party ID is delivered to the voice messaging system.
- Divert, which ensures that the correct calling/called party ID is delivered to the voice messaging system.

Other features may be required depending on how the voice messaging system is to be used. For example, if it is also serving as an automated attendant, path-replacement is needed as this feature prevents calls from hair-pinning.

Not all phone systems can serve as a message center PINX. In this case, customers may wish to consider relocating Unity Connection to Cisco Unified Communications Manager and have Cisco Unified CM act as the message center PINX with the circuit-switched phone system now acting as the user PINX.

For information on configuring Unity Connection in a centralized voice messaging environment to be hosted on Cisco Unified CM serving as the message center PINX, see the following:

- The application note *Cisco CallManager 4.1-Voicemail Interoperability: Cisco Unity 4.0(4) with Cisco CallManager 4.1(2) Configured as Message Center PINX Using Cisco Catalyst 6608 T1 Q.SIG with MGCP* at http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/414111.pdf.
- The applicable application note for configuring QSIG trunks between Cisco Unified Communications Manager and various circuit-switched phone systems on the Cisco Interoperability Portal at http://www.cisco.com/en/US/netsol/ns728/networking_solutions_products_generic_content0900aecd805b561d.html.

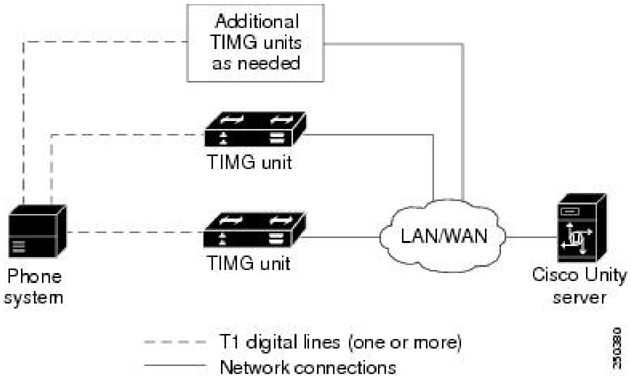
Note that if customers are deploying centralized voice messaging with Unity Connection and a circuit-switched phone system, it is up to the customer to determine whether the circuit-switched phone system can serve as a message center PINX on which Unity Connection can be hosted. If so, the customer should also confirm that there is support for the desired features, for example, MWIs, transfer, divert, and path-replacement.

Inter-cluster trunks between Cisco Unified CM clusters can be QSIG-enabled using the Annex M.1 feature, which allows Unity Connection to integrate with a single Cisco Unified CM cluster. Ports in the cluster with which Unity Connection is integrated can be dedicated to turning MWIs on and off for phones in other clusters.

Integrating Unity Connection with a QSIG-Enabled Phone System Using Cisco ISR Voice Gateways

Unity Connection supports an integration with a QSIG-enabled phone system through a Cisco ISR voice gateway. See Figure 9.

Figure 19: Connections Between the Phone System and Cisco Unity Connection



For more information on integrating Unity Connection with a QSIG-enabled phone system using Cisco ISR voice gateways, see the *QSIG-Enabled Phone System with Cisco ISR Voice Gateway Integration Guide for Cisco Unity Connection 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/sip-qsig_gw/b_cuc11xintqsig.html.

Links to Additional Integration Information

For a list of all supported versions of Cisco Unified Communications Manager and Cisco Unified CM Express, see the *Compatibility Matrix for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html

For the most current list of other supported phone system integrations, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.

Unity Connection can integrate with one or more phone systems at the same time. For details, see the *Multiple Phone System Integration Guide for Cisco Unity Connection Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/integration/guide/multiple_integration/b_cuc11xintmultiple.html.

CHAPTER 12

Cisco Unity Connection Clusters (Active/Active High Availability)

Cisco Unity Connection clusters (active/active high availability) and disaster recovery are two key customer requirements for preserving voice messaging services in the event of a system outage or disaster. For information on disaster recovery, see the Disaster Recovery System and COBRAS, on page 131 chapter.

Note The Unity Connection cluster feature is supported only with Cisco Business Edition 6000/7000.

Unity Connection Cluster Overview

Unity Connection supports a cluster configuration of two Unity Connection servers to provide high availability and redundancy. The Unity Connection servers handle calls, HTTP, and IMAP requests. If only one server in the Unity Connection cluster is functioning, the remaining server preserves the system functionality by handling all calls, HTTP requests, and IMAP requests for the Unity Connection cluster. Note that each server in the Unity Connection cluster must have enough voice messaging ports to handle all calls for the Unity Connection cluster.

The first server installed is the publisher server for the Unity Connection cluster; the second server installed is the subscriber server. These terms are used to define the database relationship during installation. The separation of roles is consistent with the Cisco Unified Communications Manager cluster schema in which there is always one publisher server and multiple subscriber servers. (Note that Unity Connection runs on the Cisco Unified CM platform). Unlike a Cisco Unified CM cluster, however, Unity Connection supports only two Unity Connection servers in the Unity Connection cluster.

Note It is recommended to perform provisioning only on the Publisher server in Active-Active mode and on Subscriber (Acting Primary) in case of cluster failover. The password change and password setting modification for User PIN/Web application should be provisioned on Publisher server in Active-Active mode.

For a network diagram of a Unity Connection cluster integrated with Cisco Unified CM, see Figure.

A Unity Connection cluster server pair supports up to 20,000 users. In this configuration, both servers can support up to 250 voice messaging ports each for a cumulative total of 500 voice messaging ports when both servers are active. If only one server is active, the port capacity is lowered to a maximum of 250 ports.

For more information on capacity planning for a Unity Connection cluster, see the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.

Note A Unity Connection cluster server pair supports up to 20,000 IMAP Idle clients (250 sessions).If the IMAP clients that connect to the Unity Connection server do not support IMAP Idle, each of these clients must be counted as 4 IMAP Idle clients. For example, deploying 4 non-IMAP Idle clients is the same as deploying 16 IMAP Idle clients. See the IMAP Clients Used to Access Unity Connection Voice Messages, on page 28 for a discussion of IMAP Idle and non-IMAP Idle clients.

Publisher Server

The publisher server is required in a Unity Connection cluster, and there can be only one publisher server in a Unity Connection cluster server pair. The publisher server is the first server to be installed, and it provides the database and message store services to the subscriber server in the Unity Connection cluster server pair.

For information on installing a Unity Connection cluster server pair, see the “Installing Cisco Unity Connection” chapter of the Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 11.x, available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

As a best practice, you should direct the majority of client traffic (for example, IMAP and the Cisco Personal Communications Assistant) and administration traffic (for example, Cisco Unity Connection Administration, the Bulk Administration Tool, and backup operations) to the publisher server in a Unity Connection cluster server pair. However, the majority of call traffic (for example, SCCP, SIP, or PIMG/TIMG) should be directed to the subscriber server in a Unity Connection cluster server pair rather than to the publisher server. Additional call traffic can be directed to the publisher server, if needed, but the call traffic should be directed to the subscriber server first.

Subscriber Server

When installing the subscriber server in a Unity Connection cluster server pair, you provide the IP address or hostname of the publisher server. After the software is installed, the subscriber server subscribes to the publisher server to obtain a copy of the database and message store. There can be only one subscriber server in a Unity Connection cluster server pair.

As a best practice, you should direct the majority of call traffic (for example, SCCP, SIP, or PIMG/TIMG) to the subscriber server in a Unity Connection cluster server pair. Additional call traffic can be directed to the publisher server, if needed, but the call traffic should be directed to the subscriber server first. Most of the client traffic (for example, IMAP and the Cisco Personal Communications Assistant) and administration traffic (for example, Cisco Unity Connection Administration, the Bulk Administration Tool, and backup operations) should be directed to the publisher server in a Unity Connection cluster server pair. Additional client and administration traffic can be directed to the subscriber server, if needed, but the client and administration traffic should be directed to the publisher server first.

Requirements for Unity Connection Cluster

For current Unity Connection cluster requirements, see the System Requirements for Cisco Unity Connection *Release 11.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Following are the requirements when both the servers in a cluster are in separate buildings or sites:

- Both servers must meet specifications according to the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.
- For a cluster with two virtual machines, both must have the same virtual platform overlay.
- Depending on the number of voice messaging ports on each Unity Connection server, the path of connectivity must have the following guaranteed bandwidth with no steady-state congestion:
  - For 50 voice messaging ports on each server—7 Mbps
  - For 100 voice messaging ports on each server—14 Mbps
  - For 150 voice messaging ports on each server—21 Mbps
  - For 200 voice messaging ports on each server—28 Mbps
  - For 250 voice messaging ports on each server—35 Mbps

  Note The bandwidth numbers above are intended as guidelines to ensure proper operation of an active-active cluster with respect to synchronization traffic between the two servers. Additional conditions such as network congestion, CPU utilization, and message size may contribute to lower throughput than expected. Call-control and call-quality requirements are in addition to the guidelines above and should be calculated using the bandwidth recommendations in the applicable *Cisco Unified Communications SRND* at http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html.

- When both the subscriber and publisher are taking calls, the maximum round-trip latency must be not more than 100 ms. When only the publisher is taking calls, subscriber is idle but replicating with publisher, the maximum round-trip latency must be not more than 150 ms.

- The network must use the following load-balancing techniques for connections to the Unity Connection servers:
    - The Unity Connection servers are assigned a common DNS name with the Unity Connection publisher server first.
    - All user client and administrator sessions connect to the Unity Connection publisher server. If the Unity Connection publisher server stops functioning, the user client and administrator sessions must connect to the Unity Connection subscriber server.
    - Phone systems must attempt to route incoming calls to the Unity Connection subscriber server. If no voice messaging ports are available to answer calls on the Unity Connection subscriber server, the phone systems must route calls to the Unity Connection publisher server.
- The TCP and UDP ports of the firewall must be open as listed in the "IP Communications Required by Cisco Unity Connection" chapter of the Security Guide for Cisco Unity Connection, Release 11.x available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.
- Both Unity Connection servers must have the same software and engineering-special versions installed.
- Both Unity Connection servers must have the same enabled features and configurations.
- Both Unity Connection servers must be configured to be in the same time zone.
- Both Unity Connection servers must connect to the same phone system(s).
- If the Unity Connection servers contain dual NICs, the two NICs on each Unity Connection server must be configured for fault tolerance using a single IP address, or one of the NICs must be disabled. Configuring the two NICs with distinct IP addresses for network load balancing is not supported.
- For selected servers supported for earlier versions of Unity Connection, a memory upgrade. To determine whether your server requires a memory upgrade, see the applicable server-specific table in the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.
- For selected servers supported for earlier versions of Unity Connection, replacement hard disks. To determine whether your server requires hard-disk replacement, see the applicable server-specific table in the *Cisco Unity Connection 11.x Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html.
- The Unity Connection cluster feature is not supported for use with Cisco Business Edition.

Balancing the Load of Calls Unity Connection Servers Handle

Although it is possible to balance the load of calls that the Unity Connection servers handle in a Unity Connection cluster, most of the call traffic should be directed to the subscriber server. This configuration follows the Cisco Unified Communications Manager cluster model of allowing call traffic only on subscriber servers.

Cisco Unified Communications Manager by Skinny Client Control Protocol (SCCP)

When integrating Unity Connection with Cisco Unified CM by Skinny Client Control Protocol (SCCP), it is possible to balance the voice traffic that the Cisco Unity Connection server pair handles using one of the following methods:

- In Cisco Unified Communications Manager Administration (on the Call Routing > Route/Hunt > Line Group page), use Top Down as the distribution algorithm for the line group that contains directory numbers of ports that answer calls on both servers in the Unity Connection cluster.

  In Unity Connection Administration, all the ports that share the same device name prefix are in a one port group. (If there are ports that share a different device name prefix, they must be in a separate port group.) Beginning with the answering port that has the lowest number in its display name, assign half the answering ports to the subscriber server so that the subscriber server answers most incoming calls. Assign the remaining answering ports to the publisher server. Then beginning with the dial-out port that has the lowest number in its display name, assign half the dial-out ports to the primary server so that the primary server handles MWIs and notification calls. Assign the remaining dial-out ports to the subscriber server.

- In Cisco Unified Communications Manager Administration (on the Call Routing > Route/Hunt > Line Group page), use Longest Idle Time as the distribution algorithm for the line group that contains directory numbers of ports that answer calls on both servers in the Unity Connection cluster.

In Unity Connection Administration, all the ports are in a single port group. The first half of the answering ports and dial-out ports are assigned to the publisher server and the remaining ports are assigned to the subscriber server in the Unity Connection cluster.

Note You can use the following CLI command to configure the “Wait for Blind Transfer Ringing Timer” counter.

run cuc dbquery unitydirdb execute procedure csp_ConfigurationModify(pFullName='System.Telephony.WaitForBlindTransferLongTimeoutMs',pvaluelong='1000')

For more information on the CLI commands, see the applicable Command Line Interface Reference Guide for Cisco Unified Communications Solutions at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Cisco Unified Communications Manager through a SIP Trunk

When integrating with Cisco Unified CM through a SIP trunk, it is possible to balance voice traffic that the Unity Connection cluster server pair handles using one of the following methods:

- Use a Route List in Cisco Unified CM.
- Use DNS-SRV – RFC 2782.
- Use a SIP gateway DNS-SRV.

TDM-Based (Circuit-Switched) Phone System through PIMG/TIMG Units

When integrating with a TDM-based (circuit-switched) phone system through PIMG/TIMG units, it is possible to balance the load of voice traffic that the Unity Connection cluster server pair handles using one of the following methods:

- Turn on load balancing on the PIMG/TIMG units.
- Use load balancing on the TDM based PBX.

Note You should turn on fault tolerance on the PIMG/TIMG units. This allows the PIMG/TIMG units to redirect calls to either server in the Unity Connection cluster if one server is unavailable to take calls.

Load Balancing Clients in a Unity Connection Cluster

Although it is possible to balance client and administration requests that the Unity Connection cluster server pair handles (for example, from the Cisco Personal Communications Assistant (PCA), IMAP, and Cisco Unity Connection Administration), most client and administration traffic should be directed to the publisher server.

In order to balance client requests, it is necessary to use DNS A-records. DNS A-records allow client DNS lookups to resolve to either server in a round-robin fashion.

Note If one server in a Unity Connection cluster server pair stops functioning and failover occurs, clients such as the Cisco PCA and IMAP clients may need to authenticate again by signing in.

You should not be using DNS to load balance with multiple A-records because this method does not account for server unavailability (for example, if one of the servers in a Unity Connection cluster server pair stops functioning). The DNS server cannot determine the availability of a server IP address that is listed in an A-record. It may be necessary for the clients to attempt DNS resolution multiple times before they connect to a functioning Unity Connection server in a Unity Connection cluster server pair.

Configuration for Dial-Out Voice Messaging Ports

Each Unity Connection server in a cluster must have voice messaging ports designated for the following dial-out functions in case either server has an outage:

- Sending message waiting indicators (MWIs).
- Performing message notifications.
- Allowing telephone record and playback (TRAP) connections.

As a best practice, you should dedicate an adequate number of voice messaging ports for these dial-out functions. These dedicated dial-out ports should not receive incoming calls and should not be enabled for answering calls.

For More Information

- For configuring Unity Connection ports and port groups to support a cluster and the various phone system integrations, see the applicable Cisco Unity Connection integration guide at http://www.cisco.com/en/US/products/ps6509/products_installation_and_configuration_guides_list.html.
- For configuring Unity Connection Clients to support a cluster, see the "Configuring Cisco Unity Connection Cluster" chapter of the Install, Upgrade, and Maintenance Guide for Cisco\\ Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

CHAPTER 13

Disaster Recovery System and COBRAS

With any disaster recovery planning, it is imperative for customers to properly back up Cisco Unity Connection in case of a disaster. There are two tools that you should use in backing up and restoring Unity Connection:

Disaster Recovery System and COBRAS

With any disaster recovery planning, it is imperative for customers to properly back up Cisco Unity Connection in case of a disaster. There are two tools that you should use in backing up and restoring Unity Connection:

Disaster Recovery System (DRS)

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform manual or regularly scheduled automatic data backups.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archived backups to a physical tape drive or remote SFTP server.

For more information on the Disaster Recovery System, see the ”Backing Up and Restoring Cisco Unity Connection Components” chapter of the Install, Upgrade, Maintenance Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/install_upgrade/guide/b_11xcuciumg.html.

Cisco Object Backup and Restore Application Suite (COBRAS)

Cisco Objected Backup and Restore Application Suite (COBRAS) is a set of tools designed to allow administrators to back up all user, call handler, interview handler, public distribution list, schedule and routing rule information and restore some or all of that information onto another Cisco Unity Connection server. It is specifically designed to allow for partial restores, restores onto different versions or products than was backed up, and for “merges” of data from multiple system backups.

For extensive information on using COBRAS, see the COBRAS Help at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

CHAPTER 14

Video Messaging

Beginning with Unity Connection 11.5(1) and later, in addition to audio message, a user or an outside caller can also send video message to another user using video enabled endpoint. To record and send a video message, make sure that:

- Video messaging is enabled in Unity Connection for the user.
- Endpoint is video enabled.

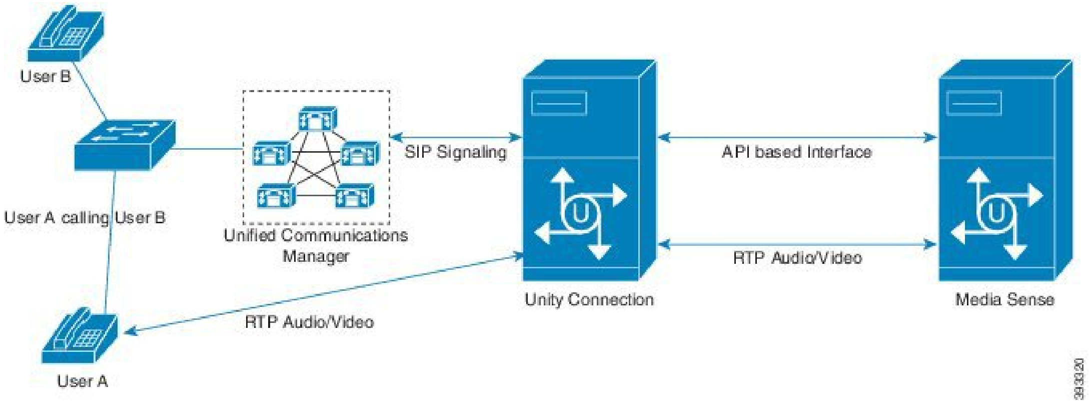
For more information on supported video endpoints, see the Video Compatibility Matrix section of the *Compatibility Matrix for Cisco Unity Connection* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/compatibility/matrix/b_cucclientmtx.html.

A user or an outside caller can send video message to another user only in case of Ring No Answer (RNA). If a video enabled user dials a call handler extension, the call remains an audio call as the call handler neither has a video service account nor it is associated with any class of service.

Note Once a user is signed in to Unity Connection, even if the video messaging is enabled for a user, the user can not compose a video message. The user can only play the video messages received from the users or outside callers through RNA scenarios.

Consider the following figure showing the video messaging architecture when a user or outside caller sends a video message to the other user in case of RNA.

Figure 20: Video Messaging Architecture



In the above figure, a user or an outside caller that is User A dials the extension of User B but User B does not answer the call, which means RNA. Now the call is forwarded to the mailbox of User B configured on Unity connection and the video greeting of User B is played back. After the greeting is played, User A records and sends the video message to User B and the message gets stored in mailbox of User B. To access the video message sent by User A, User B sign-ins to the mailbox on Unity Connection and accesses the video message.

Note If a video messaging enabled user or outside caller records a message, it completely depends upon the endpoint if the video call will be established or not. For example, if the user records a message on Cisco 8865 or 8845 series video phone with the camera shutter closed, no video streaming happens for the message. But for other endpoints, a blank video is recorded.

For information managing video messages, see "Managing Video Messages" chapter of *User Guide for the Cisco Unity Connection Phone Interface (Release 11.x)* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/user/guide/phone/b_11xcucugphone.html.

Video messaging is also supported if the Attempt Sign-In, Sub Sign-In, Attempt Forward and Greetings Administrator routing rule is set for the user.

Video Greeting

Video greeting feature allows the user to record a greeting in video format from a video-enabled end point. A user or an outside caller can access the video greetings only when calling from a video enabled endpoint (for example, a telephone with video display) to a video enabled user mailbox in Unity Connection. However, when calling from a non video enabled endpoint, the callers can only access the audio part of the video greetings. Video greetings for outside callers is enabled through the class of service of the subscribed users.

You can record and play the following six types of personal video greetings:

- Standard
- Busy
- Alternate
- Internal
- Closed
- Holiday

Note Error greetings are played as audio only.

Platform support for Video

The video messaging is supported only with 7 vCPU OVA. Each Unity Connection server (standalone or cluster) can support up to 20 concurrent video calls.

MediaSense must also be deployed using the larger 7vCPU OVA. The MediaSense needs to be installed as a single server and cannot be part of a cluster. A Unity Connection cluster or a single server can be integrated with a MediaSense server.

Note The video messaging is supported in both co-located Unity Connection active-active cluster deployment and Unity Connection active-standby cluster deployment over the WAN. The video messaging is not supported in an active-active cluster deployment over the WAN.

The MediaSense server must be co-located with Unity Connection with 1Gbps connectivity between the servers and less than 10ms Round Trip Time (RTT) latency. Unity Connection will be profiling further for bandwidth and higher latency links in later releases to allow for a wider range of deployment options.

Note While recording a video message, if the communication between Unity Connection and MediaSense is lost, the call gets converted to audio. If a video call is converted to audio because of no response from MediaSense, it cannot be restored again as a video.

Blanking Files

Due to differing behavior of some video devices, the ‘blanking’ file is used for the video messaging feature. The blanking file fills in the video RTP stream when Unity Connection and MediaSense would otherwise not be sending video. Without the blanking file, users may either experience video window closing on the device or the last received video frame freezing on the screen.

There is a sample blanking file located at
http://www.ciscounitytools.com/Applications/MediaSense/VideoBlankingFiles/

This file needs to be uploaded to the MediaSense that Unity Connection is integrated with the following information:

Title: CiscoUnityConnectionLogo.mp4

Description: <Enter a brief description>

Filename: CiscoUnityConnectionLogo.mp4

The blanking file must be an MP4 video file with a resolution 640x360 (360p) using H.264 codec at 30 frames per second. The blanking file needs to include an empty or null audio track. MediaSense requires an audio track; however silence is preferred for the blanking file so it does not distract the user during the use of the video messaging.

Due to the Cisco Unified Communications Manager regions settings in the Video Operation section, the blanking files of video greetings and messages should be recorded at an average or constant bit rate of 600kbps to allow the administrator to better calculate the bandwidth requirements of the video messaging deployment.

Video Operation

Unity Connection 11.5(1) supports video messaging only with SIP trunk integrations. MediaSense and Unity Connection allows the recording of video greetings and messages up to 1080p (1920x1080), however this offers limited compatibility across the video-enabled phone portfolio and is not a supported configuration as MediaSense does not support transcoding video to reduce the resolution for non-1080p video devices. To restrict video greetings and messages to 360p, Unity Connection leverages the use of Communications Manager's Region configurations. The Unity Connection SIP Trunks need to be put in a region that has the following relationship settings with all other regions containing video-enabled devices that might call Unity Connection and expect video greetings and messages:

Audio Codec Preference List: (Default or Administrator's Preference)

Maximum Audio Bit Rate: 64 kbps

Maximum Session Bit Rate for Video Calls: 600kbps

Maximum Session Bit Rate for Immersive Video Calls: 600kbps

In Unity Connection 10.5(2) and later, the administrator can configure any of the following supported video resolution:

- 360p (640x360)
- 480p (720x480)
- 720p (1280x720)
- 1080p (1920x1080)

The new supported video resolutions allow Unity Connection to support various video-enabled phone portfolio, however, MediaSense does not support video transcoding. The administrator needs to configure the video region settings in Cisco Unified CM, depending on the video resolution selected in Cisco Unity Connection Administration. To configure video resolution, navigate to Cisco Unity Connection Administration> Port Group> Port Group Basics> Change Advertising> Video Resolution.

For an active-standby Unity Connection cluster deployment over a WAN connection, use the following region settings for the SIP trunk to the Unity Connection server that is not co-located with MediaSense. This disables the video greetings using the secondary node. Audio-only greetings continue to function.

Audio Codec Preference List: (Default or Administrator's Preference)

Maximum Audio Bit Rate: 64 kbps

Maximum Session Bit Rate for Video Calls: Select "None"

Maximum Session Bit Rate for Immersive Video Calls: Select “None”

These settings ensure maximum compatibility across the Cisco video-enabled phone portfolio and provide the best possible experience for using video messaging.

When recording a video greeting or message, the audio and video RTP streams are both sent directly to Unity Connection. Unity Connection saves the audio RTP stream locally as an audio-only version of the video greeting or message and forks the audio and video RTP streams to MediaSense for recording. For playback, if the device is video-enabled, Unity Connection instructs MediaSense to stream the video greeting or message to Unity Connection to be forked to the device. If MediaSense is not available or unable to playback the video greetings or messages or if the device calling Unity Connection is not video-enabled, then Unity Connection plays the audio-only portion of the video greeting or message that it recorded. The audio-only greeting or message is the audio track from the video greeting or video message. It is possible to have different greetings for audio-only callers and video-enabled callers.

Cisco VCS Interoperability

The Unity Connection team has not tested calling through a VCS or calling from devices registered to a VCS and as such, these call flows are not supported. At current, the Unity Connection team is aware of an issue with certain devices registered to a VCS where video is not negotiated and audio-only greetings are played or recorded. While not currently supported, Cisco Unified CM registered devices calling through a VCS are typically able to play and record new video messages or greetings.

Video Greetings Enabled Call Handlers

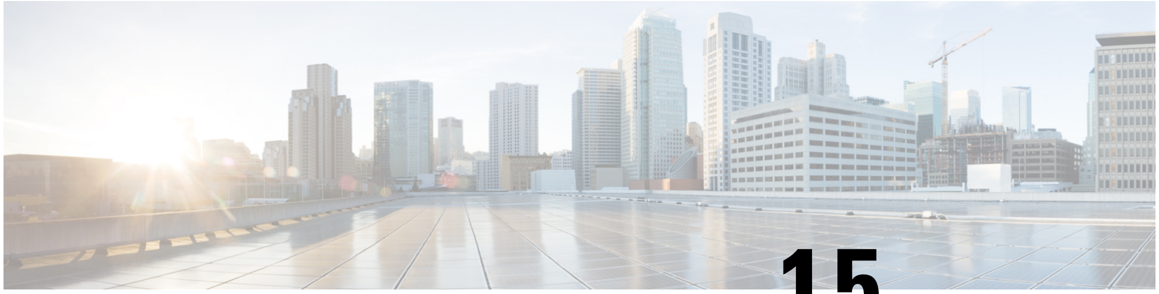
With Unity Connection 11.x, user can record video greetings for call handlers. Audio and video greeting for the call handler can be recorded by the owner assigned to the call handler only.

Limitations

Video messaging is not supported in below mentioned scenarios:

- IPv6 format
- Dispatch and Broadcast
- SCCP integration
- Voice User Interface (VUI)
- Cross-Box Transfer
- Cross-Box Login
- Directory handler
- Interview handler
- System call handler

For more information on enabling video messaging, see the Task List for Configuring Video Greetings and Massagingsection of the “Video” chapter in the System Administration Guide for Cisco Unity Connection, Release 11.x, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cucsag.html.



CHAPTER 15

Third-Party Fax Servers Integration

Third-Party Fax Servers Integration

Introduction

Cisco Unity Connection supports third-party fax servers:

- OpenText Fax Server and RightFax Edition. For more information, see the www.opentext.com
- Sagemcom Xmedius Fax SP version 6.5.5. For more information, see the www.sagemcom.com.
- Cisco Fax Server

Note For information on end-of-sale and end-of life dates for the Cisco Fax Server, see the information at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps2237/end_of_life_notice_c51-630608.html.

Overview of Third-Party Fax Servers

Unity Connection interacts with the third-party fax servers directly through Simple Mail Transport Protocol (SMTP). Inbound faxes are received by the third-party fax servers and routed to the Unity Connection server through SMTP. Similarly, faxes are routed to the third-party fax servers through SMTP for rendering and outbound faxing.

If attachments are included with a fax or an email message that is sent to the third-party fax servers, Unity Connection sends only the attachments that match the list of file name extensions that were selected during setup. third-party fax servers support.dcx, .tif, and .txt files. You can add other file extensions that are also supported by the third-party fax servers.

Note that the file name of any attachment that cannot be sent to the fax machine will appear at the bottom of the message.

Administration for Third-Party Fax Server

Administration of the fax service is performed on the third-party fax servers rather than in Cisco Unity Connection Administration. You use the third-party fax servers administration to handle the following functionality:

- Routing inbound fax messages to a user mailbox.
- Managing and logging inbound fax messages.
- Managing and logging outbound fax messages.
- Additional functionality such as running reports, creating cover pages, and evaluating least-cost routing.

Cisco Unity Connection Administration is not used in any way to administer the third-party fax servers or the services provided by the third-party fax servers.

Managing Fax Messages by Users

When you integrate third-party fax servers with Unity Connection, users are able to manage their fax messages using the clients listed in Table 10: Clients Used for Managing Fax Messages. Note that users must be added to the third-party fax servers before they can, for example, manage fax messages over the phone or from the Messaging Inbox.

Table 10: Clients Used for Managing Fax Messages

Client Application	Details
Unity Connection phone menus	Users can hear new fax messages listed with other messages when they sign-in to Unity Connection by phone. For fax messages, Unity Connection plays only the message properties (for example, the sender, date, and time) and any voice annotation. The contents of the fax itself is not played. Users can forward a fax message to another user (when the message is not marked private) or reply to a fax with a voice message (when the fax message is from another user). Users can add or change their fax number. When the system has a fax server and an outgoing fax number is configured, users can send their fax messages to a fax machine. If the fax message has attachments, Unity Connection renders only those attachments with file extensions that were specified during setup. Attachments with other file extensions are removed, and Unity Connection lists the file names at the end of the fax message.

Client Application	Details
Messaging Assistant	Users can receive notification of new fax messages by phone or pager. Although users can enable a notification device by phone, they must use the Messaging Assistant to do the following: • Set up notification of the arrival of a fax message. • Set up a notification schedule for the notification device that they choose.
Third-party IMAP clients	Third-party IMAP clients can download fax messages. To view fax messages on third-party IMAP client workstations, the workstations must have the third-party fax servers client viewer application installed, or the fax message must be supported for viewing on the client workstation. Users can forward a fax message to another user in the same way that they forward voice messages, or reply with a voice message if the fax message is from another user. In the fax message, users can use the buttons on the message toolbar to manage the message the same way that they handle email messages.

Note In order to prevent a user from sending a fax messages to a fax machine, do not configure a fax server in the Outgoing Fax Server field for the user on the User > Edit User Basics page in Cisco Unity Connection Administration. Even when prevented from sending a fax message to a fax machine, the user will still be able to receive and forward fax messages to another user.

Single Direct-Inward-Dial (DID) Number Support for Both Voice and Fax

Unity Connection supports using a single DID number to receive both voice calls and fax calls. In this configuration, incoming calls are directed to a Cisco gateway that can detect a CNG (fax) tone. When a CNG tone is detected, the gateway forwards the fax call to the third-party fax Servers. When no CNG tone is detected, the gateway forwards the voice call to the phone system.

CHAPTER 16

Overview of Cisco Unity Connection SRSV

Overview of Cisco Unity Connection SRSV

Introduction

Cisco Unity Connection Survivable Remote Site Voicemail (Unity Connection SRSV) is a backup voicemail solution that allows you to receive voice messages during WAN outages. It works in conjunction with Cisco Unified Survivable Remote Site Telephony (SRST) for providing voicemail service to a branch when the connectivity with the central Unity Connection voicemail service is lost.

Unity Connection SRSV is used in the centralized Cisco Unified Communications Manager and Cisco Unity Connection environment with multiple branch offices or small sites. It provides limited voicemail and auto-attendant features that remain in synchronization with the central Unity Connection voicemail service so that when the WAN outage or failure occurs, the Unity Connection SRSV solution can provide voicemail service to the subscribers at the branch. However, as soon as the network is restored, all the voicemails received by the branch subscribers are automatically uploaded to the central Unity Connection voicemail server.

Unity Connection SRSV solution requires the following two components:

- Unity Connection: It is deployed at the central site alongside with Cisco Unified CM to deliver powerful integrated messaging and voicemail services.
- Unity Connection SRSV: The SRSV component is natively a part of Unity Connection which is deployed at the branch site alongside with Cisco Unified CM Express or SRST. Unity Connection SRSV is hosted on Cisco Integrated Service Routers Generation 2 (ISR G2) platform using Services Ready Engine Virtualization.

Supported SRSV Topologies

Unity Connection SRSV supports several topologies based on the configuration of the router. You can deploy either original SRST or CUCME-as-SRST (also known as SRST Fallback Mode) at branch.

Note If you are running SRST at the branch site, you cannot deploy the E-SRST feature.

Following figures show three topologies supported by Unity Connection SRSV:

Figure 16-1: Shows a topology in which SRST is deployed at the branch site. If the WAN occurs or PSTN goes down, Unity Connection SRSV at the branch site provides limited voicemail support in the failover mode.

Figure 16-2: Shows a topology where CUCME-as-SRST (also known as SRST Fallback Mode) is providing call control at the branch site.

Figure 16-3: Shows a topology where multiple CUCME-as-SRST and SRSV devices are paired for load balancing at the survivable branch site. In this scenario, the administrator uses Cisco Unified Communications Manager to divide the branch users between CUCME-SRST-1 and CUCME-SRST-2. The central Unity Connection server detects that and then sends the appropriate configuration to SRSV-1 and SRSV-2 at the branch site. In the event of WAN failure, each SRSV device handles calls directed to it from the paired CUCME-as-SRST device.

Figure 21: Topology 1

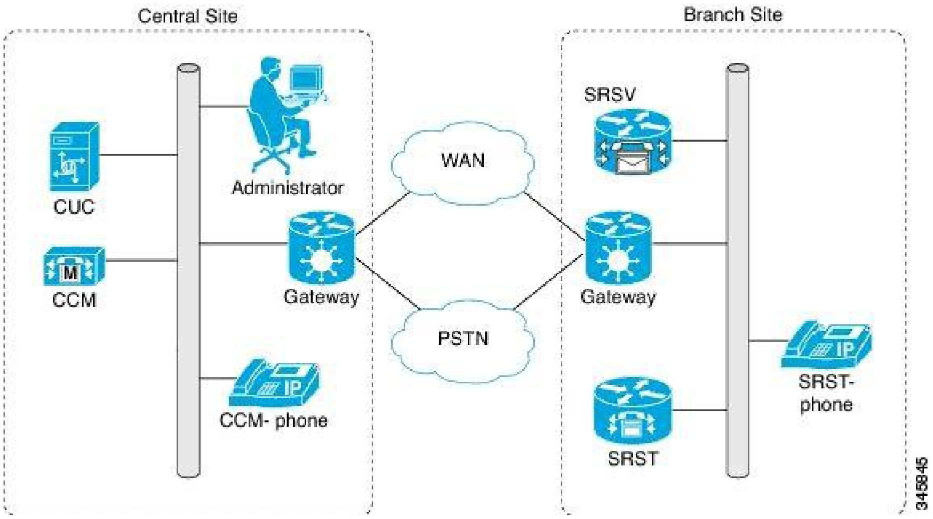


Figure 22: Topology 2

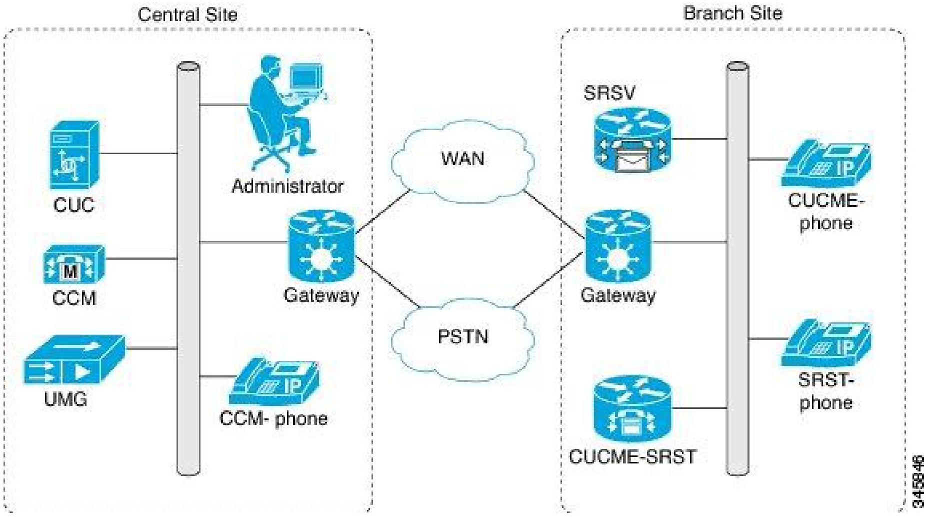
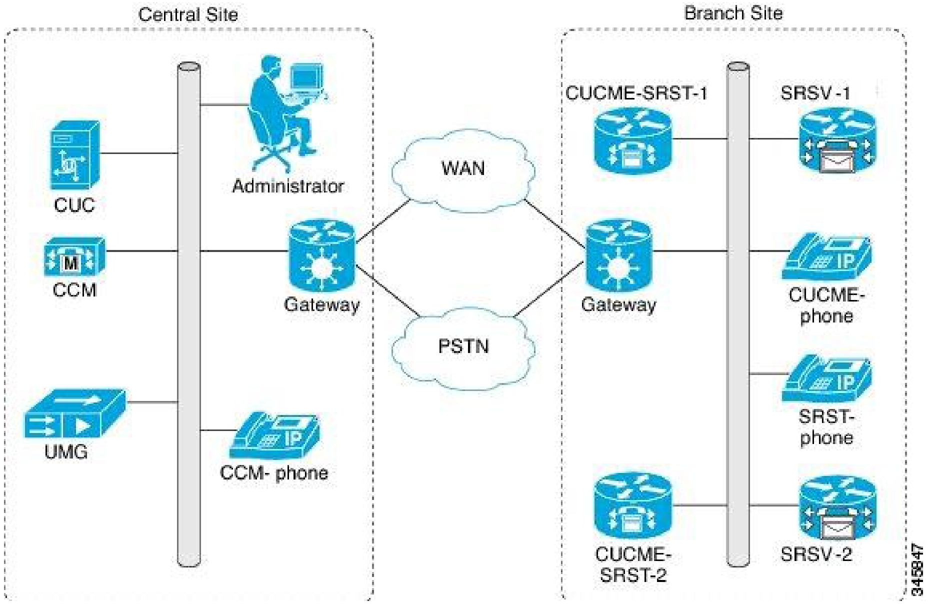


Figure 23: Topology 3



SRSV with High Availability

When you deploy SRSV and the central Unity Connection node in an HA pair, SRSV functions even if the primary server is down. There is no additional configuration needed to support this feature, it is automatically supported.

Note After recovering from a network outage, the bandwidth requirements for synchronization to the central Unity Connection server does not have any bandwidth requirements.

Scalability

Each Unity Connection SRSV branch supports 500 users per branch with a maximum of 35 branches per centralized Unity Connection server.

Software Requirements

Unity Connection SRSV requires Unity Connection minimum version 11.x for both the central Unity Connection server as well as the SRSV branches.

The Unity Connection SRSV administrator workstation must be configured as per the software requirements. For more information, see the "Software Requirements—Administrator Workstations (Unity Connection and Unity Connection SRSV)" section of the System Requirements for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/requirements/b_11xcucsysreqs.html.

Supported Hardware

Any supported Unity Connection hardware is suitable for Unity Connection SRSV. For information on the current supported platforms list for the most up to date list of supported hardware, see the "Specifications for the Virtual Platform Overlays Supported by Unity Connection SRSV" section of the Cisco Unity Connection 11.x Supported Platform List, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/supported_platforms/b_11xcucspl.html

Limitations

- No interaction between existing Unified Messaging Gateway (UMG) based SRSV and Unity Connection based SRSV
- No migration from UMG based SRSV

For a complete comparison of Unity Connection SRSV to UMG SRSV, see the comparison guide: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps2237/product_data_sheet0900aecd806bfc37.html.