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 14*. 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/14/administration/guide/b_14cucsag.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.

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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Video Messaging

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 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.
- "Video Messaging" chapter of *Design Guide for Cisco Unity Connection Release 14*.
- “Requirement for using Video Messaging” section of the *System Requirements for Cisco Unity Connection, Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.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 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/unified_messaging/guide/b_14cucumgx.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

You can also configure Connection to synchronize voice messages in Unity Connection user mailbox with the Microsoft Office 365 and Gmail server.

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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/unified_messaging/guide/b_14cucumgx.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user_setup/guide/b_14cucuwsx.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.
- **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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.
- Jabber - Unity Connection 14 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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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/14/quick_start/guide/b_14cucqsgminiinbox.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 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/REST-API/CUPI_API/b_CUPI-API.html.

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 14* available https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/troubleshooting/guide/b_14cuctsg.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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.

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 about all of the administrative tools, see the "Tools" chapter of the System Administration Guide for Cisco Unity Connection, Release 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14* 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. Licenses are managed by **Cisco Smart Software Licensing**. Using Cisco Smart Software Licensing, you can manage all the licenses associated with an organization through a single interface, which is Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite. Cisco Smart Software Licensing provides the visibility of your licenses ownership and consumption. Unity Connection must be registered with the Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite to use various licensed feature.

Unity Connection remains in the Evaluation Mode until it registers with the Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite.

Unity Connection provides Specific License Reservation feature that allows you to reserve the licenses or entitlements from your virtual account and associate them with the product instance.The product instance can use the reserved licenses without communicating usage information to CSSM.

For information on Unity Connection licenses, see the "Managing Licenses"chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html.

Branding Customization in Unity Connection

Unity Connection introduces a feature **Branding Customization** by which the appearance of Unity Connection web applications can be modified based on the organizational requirements. This feature allows an Operating System Administrator to customize company logo, background colors, border colors and font colors of Unity Connection web applications. **Branding** can be applied on the following web applications of Unity Connection:

- Cisco Unity Connection Administration
- Cisco Personal Communications Assistant
- Web Inbox

Note In Web Inbox, only company logo can be modified.

For more information on Branding customization in Unity Connection, see the "Software Upgrades" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.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.

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 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.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 14, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.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.

- **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 14*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html

- **Secure messages**—Unity Connection supports secure messaging. For more information, see the Secure Messages, on page 14 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,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/quick_start/guide/b_14cucqssamlsso.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 • Cisco Unified Communications OS Administration • Disaster Recovery System
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.

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.

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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.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 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.htmland the "Configuring an Email Account to Access Unity Connection Voice Messages" chapter of the User Workstation Setup Guide for Cisco Unity Connection *Release 14*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/user_setup/guide/b_14cucuwsx.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 14,* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html.

Cipher Management for Secure Interfaces

Cisco Unity Connection supports **Cipher Management** that allows administrator to control set of ciphers that are used for every TLS and SSH connection. You can configure the ciphers for various secure interfaces of Cisco Unity Connection.

For more information on Cipher Management, see the "Security" chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.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.

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 14 Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.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 14 Supported Platforms List* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.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 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/multiple/b_cuc14intmultiple.html.

For the requirements of the phone system integration, see the System Requirements for Cisco Unity Connection *Release 14* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html.

For supported deployment models, see the "Overview of Cisco Collaboration System Components and Architecture" chapter of the *Cisco Collaboration System 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, available at 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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

For information on number of Jabber endpoints that Unity Connection supports with single inbox users for specific OVA, see the "Scaling Platform" section of the Supported Platforms Guide for Cisco Unity Connection, Release 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/supported_platforms/b_14cucspl.html

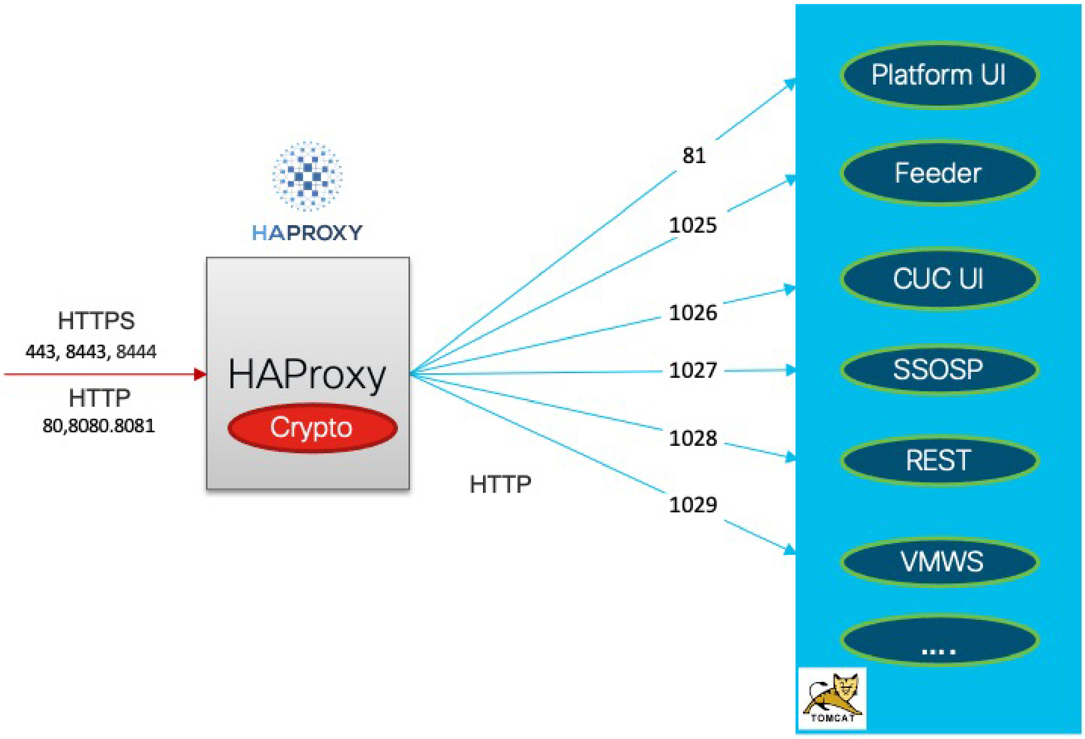
Unity Connection Clusters (Active/Active High Availability and Redundancy)

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.

System Architecture Improvements for Web Traffic

Cisco Unity Connection supports HAProxy which frontends all the incoming web traffic into Unity Connection offloading Tomcat. It is a fast and reliable solution that offers high availability, load balancing, and proxy capabilities for HTTP-based applications.

Below figure explains the architecture:



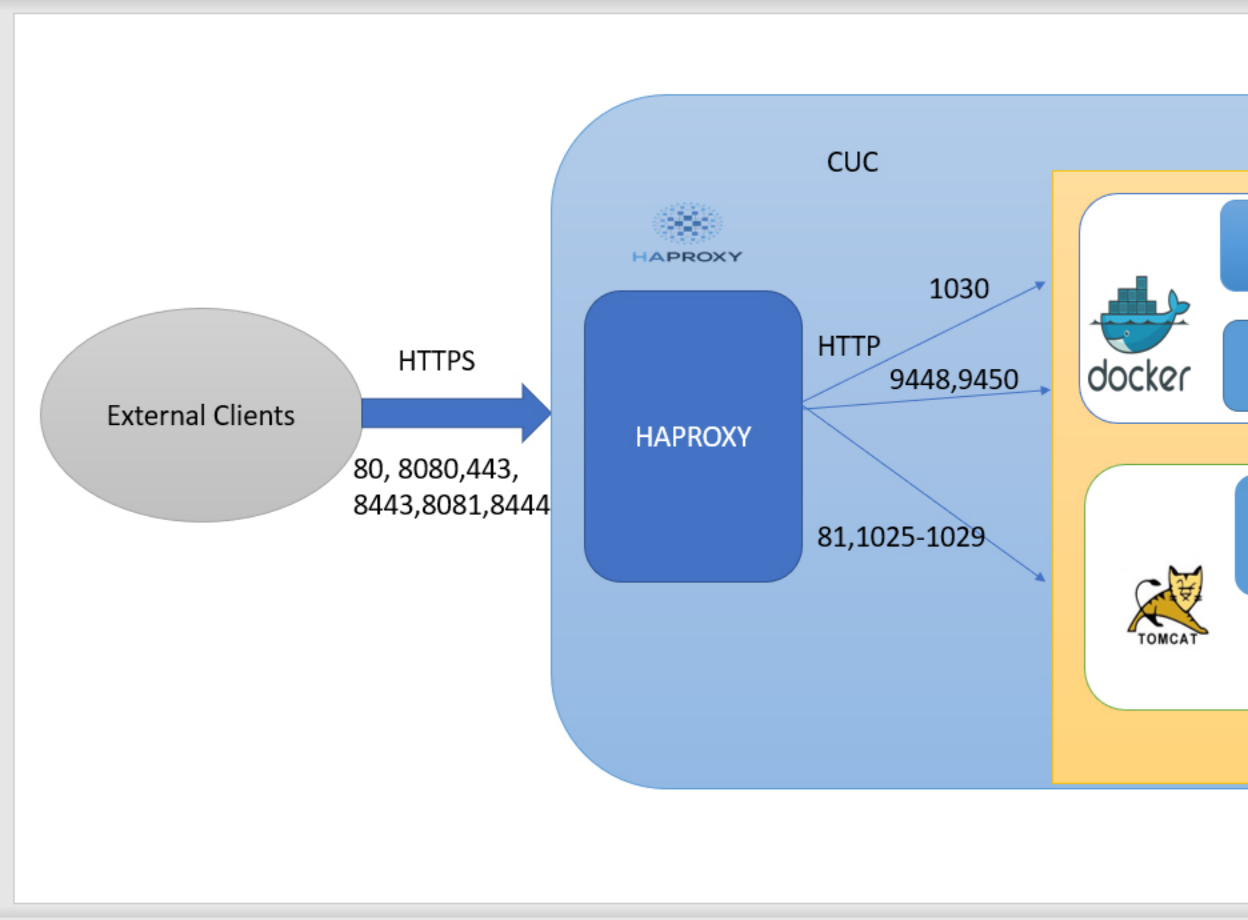
- All web applications are deployed by Tomcat.
- HAProxy handles all TLS inbound connections.
- HAProxy listens on ports 80,443,8080,8081,8443,8444.
- Tomcat listens on ports 81,1025,1026,1027, 1028, 1029.
- HAProxy sends the request internally to Tomcat via HTTP. All web applications internally receive request via http instead of https.

For more information on ports, see chapter IP Communications Required by Cisco Unity Connection in *Security Guide for Cisco Unity Connection Release 14* available at link https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

Resource control through Docker Containerization

Cisco Unity Connection Release 14 and later, supports resource control through Docker containerization. The main aim of this feature is to prevent running Tomcat web application from locking out system administrator access of the application.

Below figure explains the architecture:



- Rest Container is introduced to support this feature for handling VMREST requests from clients.
- SSOSP Container is inherited from CUCM for handling single sign-on for clients.
- All web applications like cuadmin,ciscopca,inbox,miniinbox etc will continue to deploy on Tomcat container.
- HAProxy listens on port 1030 for REST container operations.

For more information on port, see chapter IP Communications Required by Cisco Unity Connection in *Security Guide for Cisco Unity Connection Release 14* available at link https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html.

The following CLI commands have been introduced to support this feature:

- utils container-engine start

- utils container-engine stop
- utils container-engine restart
- utils container-engine status
- utils diagnose module <module-name> <container-name>

For more details about CLI commands, see chapter "Utils Commands" in *Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 14* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/14_0_1/cucm_b_cli_reference_guide_release_1401.html.

This feature provides following advantages:

- Ensures that individual services running inside containers do not consume resources significantly above designed limits.
- Restart the individual container without impacting other web applications on other containers.
- Lay groundwork for future containerization of application and services.

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 14, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/https_networking/guide/b_14cuchttpsnet.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 14* 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/14/requirements/b_14cucsysreqs.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 14 SRND* .

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.