Overview of HTTPS Networking

Overview of HTTPS Networking

Overview

When the messaging needs of your organization require more than one Cisco 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 HTTPS Networking, connects different Unity Connection servers and clusters in a network.

Note

- In Unity Connection, legacy networking is also supported to connect multiple Unity Connection servers in a network. However, it is recommended to 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.

The main objective of HTTPS networking is to increase the scalability of Unity Connection deployments. The architecture of HTTPS networking is scalable both in terms of number of Unity Connection locations and the total directory size.

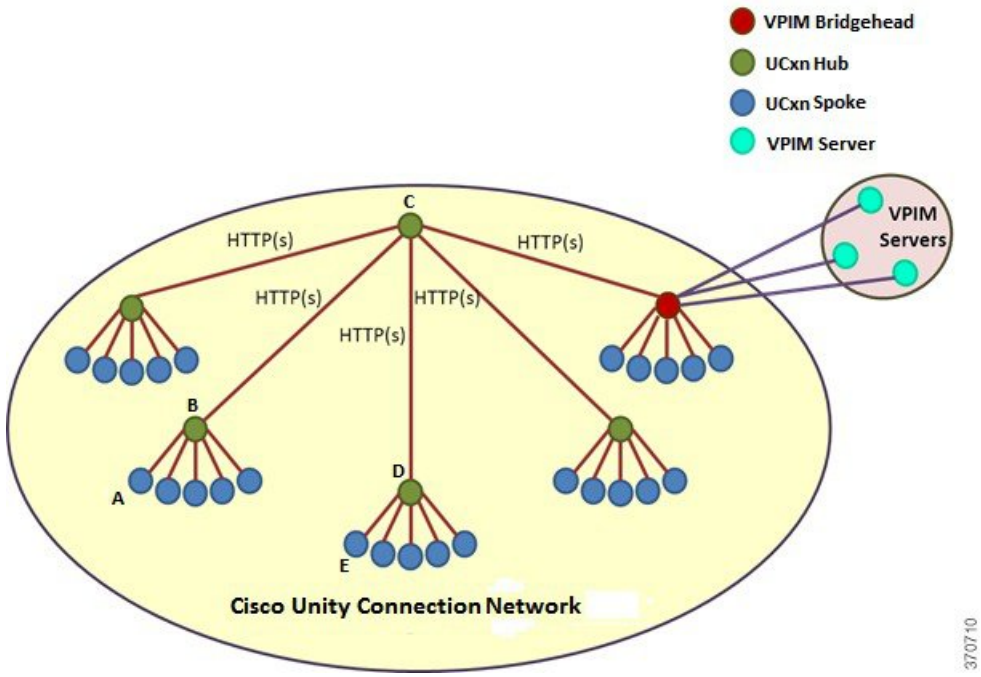
About Unity Connection HTTPS Links

You can join two or more Unity Connection servers or clusters to form a well-connected network, referred to as an HTTPS network. The servers that are joined to the network are referred to as locations. (When a Unity Connection cluster is configured, the cluster counts as one location in the network.) Within a network, each location uses HTTPS protocol to exchange directory information and SMTP protocol to exchange voice messages with each other.

The locations in an HTTPS network are linked together through an HTTPS link. The topology used in HTTPS networking is hub and spoke topology, which plays an important role in increasing scalability of directory size and number of Unity Connection locations. In hub-spoke topology, there are two types of locations: hub location and spoke location. The Unity Connection location which has more than one HTTPS links is known

as hub location. However, the Unity Connection location which has only one HTTPS link is known as spoke location. Figure 1 illustrates a network of multiple Unity Connection locations joined by HTTPS links.

Figure 1: A Cisco Unity Connection 15 Network Joined by HTTPS Links Among All Locations



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 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.

About VPIM Networking

Unity Connection 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) protocol.

VPIM Networking is supported for use with Cisco Business Edition.

Unity Connection supports up to 100 VPIM locations and 150,000 VPIM and System contacts in the Connection directory. These limits apply either to the directory of a single Unity Connection server or cluster pair, or to the global directory in a network.

Note To support 150K contacts on a single Unity Connection server, you need to dedicate the server as VPIM bridgehead only.

If you deploy VPIM in an HTTPS network, you can designate one or more Unity Connection locations in the network as VPIM bridgehead(s) to handle the configuration of VPIM locations and contacts depending upon your requirements. The VPIM location data and all contacts at the VPIM location (including automatically created contacts) are replicated from the bridgehead to other locations within the network. When a VPIM message is sent by a user who is homed on a Unity Connection location other than the bridgehead, the message first passes to the bridgehead, which handles forwarding the message to the destination server. Similarly, the messages from VPIM contacts are received by the bridgehead and relayed to the home server of the Unity Connection recipient.

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 15*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/networking/guide/b_15cucnetx.html.

Directory Synchronization

Each location in an HTTPS network has its own directory of users and other objects that are created on the location and are said to be "homed" on that location. The collection of objects and object properties that are replicated among locations is referred to as the global directory.

See the following section for details on the specific objects and object properties that are replicated during directory synchronization:

- Replication Within HTTPS Network

Replication Within HTTPS Network

Within HTTPS network, the objects and object properties that are replicated during directory synchronization are shown in Table 1: Replicated Objects in a Cisco Unity Connection HTTP(S) Network:

Table 1: Replicated Objects in a Cisco Unity Connection HTTP(S) Network

Replicated Object	Replicated Properties
Users with mailboxes	• Alias • First name, last name, display name, alternate names • Extension, cross-server transfer extension, and alternate extensions • Directory listing status • Partition • Recorded name • SMTP address and SMTP proxy addresses • Phone Numbers
System and VPIM contacts	All properties
System distribution lists	All properties, including list membership
Partitions	All properties
Search spaces	All properties, including membership
Unity Connection location	• Display name • Host address • SMTP domain name • Unity Connection version • Encryption Key • Subscriber's Base feed URL • Maximum DL count • Maximum Users count • Destination Type • Maximum Contact Count

Replicated Object	Replicated Properties
VPIM location	• Display name • Dial ID • Partition • Search Scope • SMTP Domain Name • IP Address • Recorded Names • Remote Phone Prefix

In most cases, you can use replicated objects just as you would use local objects; for example, you can assign a remote user to be the message recipient of a system call handler, or configure the search scope of a user to use a remote search space. Note the following exceptions:

- System call handler owners must be local users.
- Objects that belong to a partition (users, contacts, handlers, system distribution lists, and VPIM locations) can only belong to local partitions. You can, however, add a remote partition to a local search space.

In HTTPS networking, the directory replication is accomplished by means of a Feeder service and a Reader service running on each location in the network. The Reader service periodically polls the remote location for any directory changes since the last poll interval. The Feeder service checks the change tracking database for directory changes and responds to poll requests with the necessary information.

On each location in a network, you can configure the schedule on which the Reader polls the remote Feeder for directory data, and the schedule on which it polls for recorded names. In Cisco Unity Connection Administration interface of a Unity Connection location, you can access the schedules on the **Tools > Task Management** page by selecting either the **Synchronize Directory With Local Network** task or the **Synchronize Voice Names With Local Network** task.

Note The tasks are not available unless HTTPS networking is configured on the system.

When the **Synchronize Voice Names With Local Network** task is enabled, the Reader processes recorded name files for remote users, contacts, VPIM locations, and system distribution lists (if applicable). Once a recorded name is created for a remote object on the Unity Connection location, it is updated only if the remote and local filenames for the recorded name differ. For example, if you change the outgoing codec for recorded names on the remote location, the local Unity Connection location do not update its files because the change does not affect filenames. In order to pull updated copies of recorded names in this case, you must clear all existing recorded names from the local Unity Connection location and then do a full resynchronization using the **Clear Recorded Names** button and the **Resync All** button on the **Search HTTPS Links** page in Unity Connection Administration.

Overview of High Availability in HTTPS Networking

This section describes the concept of high availability of Unity Connection in terms of directory synchronization. Unity Connection can be configured as a cluster node comprising of the publisher and subscriber servers. In the HTTPS networking, when the publisher server of a cluster location is up and running, it is responsible for the synchronization of directory information. However, if the publisher server is down, the subscriber server takes the role of synchronizing directory information. This concept of maintaining a backup Unity Connection server for the situations when the primary server is down is known as high availability.

Depending upon the component of a cluster (publisher or subscriber) with which the directory synchronization is being performed, the directory synchronization can be of the following types:

- Standard - Specifies that the directory synchronization is done by the publisher server with the connected locations.
- Alert - Specifies that the publisher server is unreachable and subscriber server is responsible for providing directory information to the connected locations. However, the subscriber server has the directory information stored that is last synchronized with the publisher server when it was running.

Behavior of Cluster in Standard mode

The following is the behavior of Unity Connection cluster and Reader/Feeder services on the cluster in Standard mode:

- By default, a Unity Connection cluster is in Standard mode
- The Reader service remains running on the publisher server.
- The Feeder service runs on the publisher as well as subscriber server. By default the Feeder service of the publisher server responds to the directory synchronization request.

Behavior of Cluster in Alert mode

The following is the behavior of Unity Connection cluster and Reader/Feeder services on the cluster in Alert mode:

- The publisher server is inaccessible.
- The Reader service remains inactive on the publisher as well as subscriber server.
- The Feeder remains running on the subscriber server and responds to the directory synchronization requests.

Usually the publisher is down for a very short period of time and the directory synchronization occurs in the Alert mode. During the Alert mode, the connected nodes have limited access to directory synchronization with the subscriber. The limited access means that the connected nodes can fetch only the directory information that was last synchronized with the publisher when it was running. When the publisher comes up, the nodes that are directly connected to the publisher synchronize the updated directory information through the publisher. Therefore, the key benefit of the Alert mode is that the connected nodes remain synchronized with the subscriber server even when the publisher is down.

Note In an HTTPS network, if the publisher server of a Unity Connection cluster is down, then the Unity Connection cluster moves to "Alert" mode. However, this mode is reflected on the Cisco Unity Connection Administration interface of the connected nodes only after the completion of directory synchronization on the connected nodes.

In the Alert mode, the Feeder service running on the subscriber server of a cluster node has the capability to provide directory information to the directly connected nodes. In addition, the Reader service running on the nodes that are directly connected to a cluster node has the capability to fetch directory information from the subscriber server when the publisher is down.

Note When a cluster node is in split brain condition, the Reader service installed on the cluster node remains in inactive state. For more information see *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html.

Directory Size Limits

The Unity Connection global directory (the entire collection of local and replicated objects) is subject to certain size limits. However, it also generates an RTMT alert so that administrator can take appropriate action. In Unity Connection, there are separate limits on the number of users, the number of contacts, and the number of system distribution lists.

The size limits are:

- 100,000 Users.
- 150,000 Contacts
- 100,000 system distribution lists
- 25,000 users per system distribution list
    - 1.5 million total list members across all system distribution lists
    - 20 levels of nesting (where one system distribution list is included as a member of another list)

Note Additional directory object limits exist, and the directory object limits may have been updated since the time of release. For detailed and up-to-date limit information, see the *System Requirements for Cisco Unity Connection Release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html.

In HTTPS network, you are allowed to link up to 25 Unity Connection locations. However, whenever the Reader service installed on the Unity Connection locations runs, it checks the limit for the replication objects, such as users or contacts. If the number of replication objects exceeds its maximum limit, the Reader service moves to "Warning" mode. In the Warning mode, you can still create new directory objects for remote location objects but you might face performance issues. Therefore, it is recommended to get the Reader service out of

Warning mode to avoid such issues. In order to move the Reader out of "Warning" mode, you must remove enough number of objects of the appropriate type to bring the number less than the maximum limit.

Consider the following example of the user limit check. Unity Connection location A has 80,000 users, and Unity Connection location B has 90,000 users. Now, after joining the two locations, when the Reader service on Unity Connection A and Unity Connection B runs, both the locations move to the "Warning" mode as the total number of users becomes 170,000 (maximum limit is 100,000). To bring the two locations to the normal mode, you need to remove some users either from Unity Connection A or from Unity Connection B.

Messaging

See the following section for details on how messaging is handled in specific networking situations:

- Handling the Messages to System Distribution Lists Within an HTTPS Network

Handling the Messages to System Distribution Lists Within an HTTPS Network

Because system distribution lists are replicated among locations in a Cisco Unity Connection network, a user can address messages to any system distribution list at any location, as long as the list is reachable in the user search scope.

When a user addresses a message to a system distribution list, the local Cisco Unity Connection location parses the distribution list membership. The sending location delivers the message directly to local users on the list. If there are remote Unity Connection users in the distribution list, the sending location delivers the message to each location that homes the remote users. If there are VPIM users in the list, the sending server either delivers the message to the VPIM destination if the VPIM location is homed locally, or passes it to the server on which the location is homed and that server handles forwarding the message to the destination server.

Unity Connection includes the following predefined system distribution lists: **All Voicemail Users, Undeliverable Messages,** and **All Voicemail-Enabled Contacts**. Each Unity Connection server in your organization has a distinct version of each of these lists. If you have not changed the names of these lists to be unique, during initial replication each server automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names.

By default, the predefined lists on each Unity Connection location have the same recorded name, and the **All Voicemail Users** and **All Voicemail-Enabled Contacts** lists have the same extension at each location (the Undeliverable Messages list by default is not assigned an extension, because users do not typically address messages to this list). When setting up an HTTPS Unity Connection network, you should consider modifying the recorded name of each **All Voicemail Users** list and each **All Voicemail-Enabled Contacts** list; if you do not, users can hear a confusing list of choices when they address messages by name to one of these lists. When users address by extension to a list whose extension overlaps that of another list, they reach the first list that is located when Unity Connection searches the partitions of the user search space in order.

Make sure to synchronize the distribution list immediately after changing the membership of the distribution list to avoid facing issues, for example NDR, and in sending voice messages to the changed distribution list.

Tip Distribution lists can be nested such that a distribution list contains other lists. You can create one master **All Voicemail Users** distribution list for a network that contains the **All Voicemail Users** list of each Unity Connection location.

Cross-Server Sign-In, Transfers, and Live Reply

In order to limit replication traffic and keep the directory size manageable, only a subset of user information is replicated from the home location of the user to other locations. For this reason, only the user home location has information about call transfer settings, greetings, and other specific details for the user. In order for a location to properly handle calls destined for a user on a different location, the location that receives the call must hand off the call to the home location of the user. The purpose of the cross-server features is to make the user experience in a networked environment almost the same as in a single server environment, as shown in Table 2: Cross-Server Features.

Table 2: Cross-Server Features

Feature	Description
Cross-server sign-in	Cross-server sign-in allows administrators to provide users who are homed on different locations with one phone number that they can call to sign in. When calling from outside the organization, users-no matter which is their home server-call the same number and are transferred to the applicable home server to sign in.
Cross-server transfer	Cross-server transfer enables calls from the automated attendant or from a directory handler of one server to be transferred to a user on another server, according to the call transfer and screening settings of the called user.
Cross-server live reply	Cross-server live reply allows users who listen to their messages by phone to reply to a message from a user on another server by calling the user (according to the call transfer and screening settings of the called user).

For more information and instructions on enabling the cross-server features, see the "Cross-Server Sign-In, Transfers, and Live Reply in HTTPS Networking" chapter.

Addressing and Dial Plan Considerations

Addressing Options for Non-Networked Phone Systems

If your organization has a separate phone system for each location, users at one location dial a complete phone number, not just an extension, when calling someone at another location. When users sign in to send messages to users on another networked location, the number that they enter when addressing a message by extension depends on whether the numbering plans overlap across locations.

When user extensions on one location overlap with user extensions on another location, you can provide unique extensions for each user by setting up alternate extensions for each user account. For each user, enter a number for the alternate extension that is the same as the full phone number for the user, and make sure that the alternate extension is in a partition that is a member of the search spaces that users at other locations use. Once this has been set up, when users sign in to send messages, the number that they enter when addressing messages is the same number that they use when calling.

When numbering plans do not overlap across networked locations-that is, when user extensions are unique across locations-users can enter an extension when addressing a message to a user who is associated with another location. Optionally, as a convenience for users in this circumstance, you may select to add alternate

extensions to each user account, so that users do not need to remember two different numbers-one for calling a user directly, and one for addressing a message. However, if you do not set up alternate extensions, be sure to tell users to use the extension instead of the full phone number when addressing messages to users who are associated with another location.

Note that alternate extensions have other purposes beyond their use in networking, such as handling multiple line appearances on user phones.

Identified User Messaging

When a user calls another user, and the call is forwarded to the greeting of the called user, the ability of Unity Connection to identify that it is a user who is leaving a message is referred to as identified user messaging. Because Unity Connection is able to identify the caller as a user:

- Unity Connection plays the internal greeting of the called user when the caller leaves a message.
- Unity Connection plays the recorded name of the user who left the message when the recipient listens to the message.
- Unity Connection allows the recipient to record a reply.

It is important to note the difference between the following two circumstances:

- A user signs in to Unity Connection and then records and sends a message. In this circumstance, when the user has signed in, Unity Connection can identify the message as being from the user, regardless of which location the message recipient is homed on. In this case, the phone system is not involved and the recipient phone does not ring. Instead, the message is sent via networking message exchange (using SMTP).
- A user places a phone call to another user, and then leaves a message. This circumstance is the basis of identified user messaging.

As long as identified user messaging is enabled on a Unity Connection location, Unity Connection is able to identify both local and remote users. Note, however, that for identified user messaging to work in both cases, the initial search scope of the call must be set to a search space that locates the correct user based on the calling extension, regardless of whether the caller is a local or remote user.

If a user calls from an extension that is in a partition that is not a member of the search space that was set as the initial search scope for the call, the call is not identified as coming from the user. If the extension of the user overlaps with an extension in another partition that also appears in this search space, the call is identified as coming from the first object that Unity Connection finds when searching the partitions in the order that they appear in the search space.

In situations where numbering plans overlap across locations, it is therefore possible to have a user leave a message that is incorrectly identified as coming from another user with the same extension in a different partition. Because the initial search scope of the call is based on call routing rules, to avoid this situation, use the following configuration guidelines:

- Maintain a separate search space for each location in which the partition containing its users appears first in the search space. (By default, each Unity Connection server uses its own default partition and default search space, which are replicated to other locations when the server is networked.)
- On each location, set up forwarded call routing rules specific to every other location by specifying a routing rule condition that applies only to calls from that location (for example, based on the port or phone system of the incoming call). Configure the rule to set the search scope of the call to the search space in which the partition containing users at the location appears first.