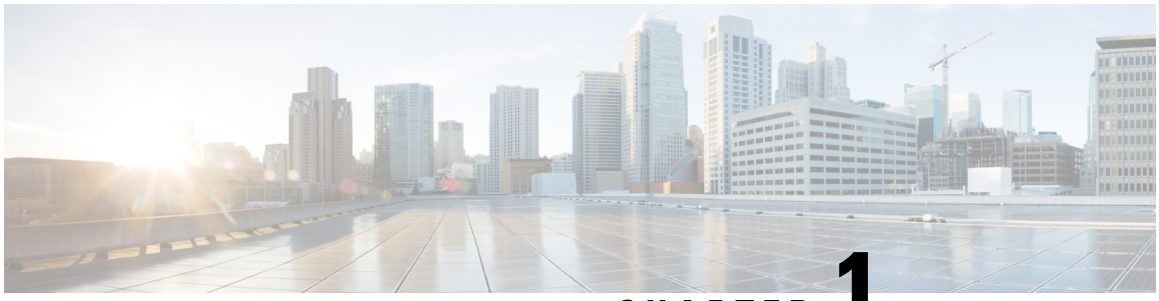
Networking Guide for Cisco Unity Connection Release 12.x

First Published: 2019-01-24

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 1

Overview of Networking Concepts

Overview of Networking Concepts

Overview

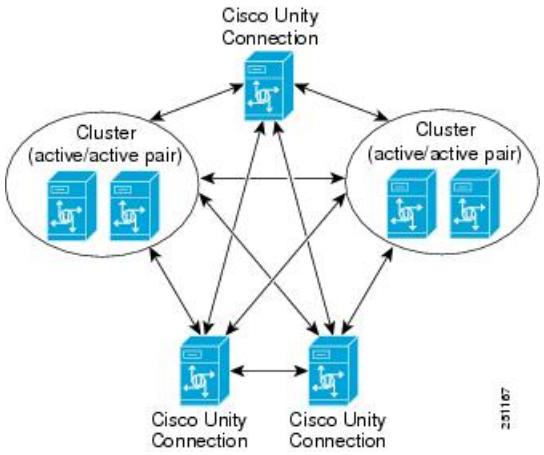
Each Cisco Unity Connection server or cluster has a maximum number of users that it can serve. When the messaging needs of your organization require more than one Unity Connection server or cluster, or combine multiple Unity Connection directories or internetwork Unity Connection with Cisco Unity, you need a way to form a Cisco voicemail organization.

A Cisco voicemail organization can be formed when you 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.

About Unity Connection Sites and Intrasite Links

You can join two or more Unity Connection servers or clusters (up to a maximum of ten) to form a well connected network, referred to as a Unity Connection site. The servers joined to the site are referred to as locations. (When a Unity Connection cluster is configured, the cluster counts as one location in the site.) Within a site, each location uses SMTP to exchange directory synchronization information and messages directly with every other location. Each location is said to be linked to every other location in the site via an intrasite link. Figure 1: A Unity Connection Site Joined by Intrasite Links Among All Locations illustrates a site of five Unity Connection locations joined by intrasite links.

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



The Unity Connection site concept was known as a Digital Network in Unity Connection release 7.x. You can join 7.x locations and 8.x locations in the same Unity Connection site (intrasite links), as long as you do not link the site to any other site (intersite links require that each Unity Connection location be at release 12.x).

Each Unity Connection server or cluster is represented in the site as a single Unity Connection location, which is created locally during installation and cannot be deleted from the server itself. When you join the server (or cluster) to an existing location in a site, a Unity Connection location is automatically created for the server (or cluster) on all other locations in the site and these locations begin to perform directory synchronization with the new location. A Unity Connection location can only belong to a single site.

About Cisco Voicemail Organizations and Intersite Links

You can use an intersite link to connect one Unity Connection site to another Unity Connection site, allowing you to scale your organization from ten locations to a maximum of 20. You can also use an intersite link to connect a Unity Connection server or site to a Cisco Unity server or Cisco Unity digital network. 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 pass between the two site gateways, thereby limiting the connectivity requirements and bandwidth usage to the link between those two site gateway locations.

Only one intersite link is supported per site. So, you can link a single Unity Connection site to a single Cisco Unity site, or a single Unity Connection site to another Unity Connection site.

About Linking Two Unity Connection Sites

When you link two Unity Connection sites with an intersite link, 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 HTTP or HTTPS protocol to exchange directory synchronization updates.

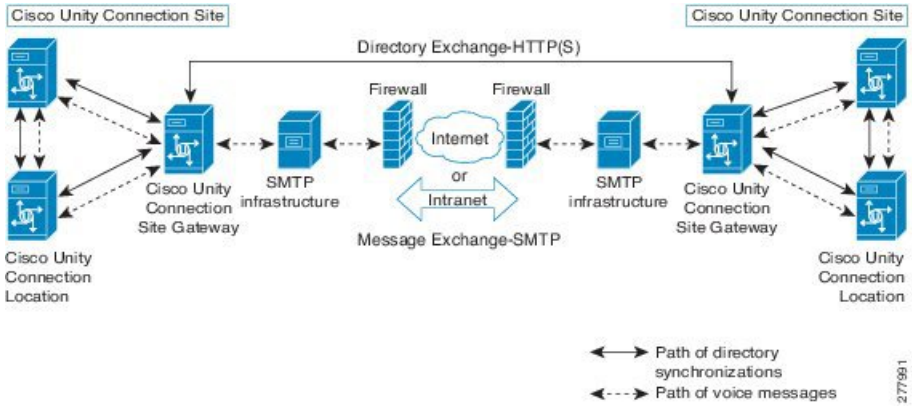
Each site gateway is also responsible for transmitting messages that are addressed to recipients at the remote site and for receiving messages that are addressed to recipients in its own site. Intersite messages are transmitted and received using SMTP.

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 continues to provide message exchange over the intersite link if the publisher server is down.

Figure 2: A Cisco Voicemail Organization Consisting of Two Unity Connection Sites Connected through an IntersiteLink illustrates the role of the site gateways and the intersite link in connecting two Unity Connection sites.

Note In order to link two Unity Connection sites, all servers in each site must be running Unity Connection version12.x.

Figure 2: A Cisco Voicemail Organization Consisting of Two Unity Connection Sites Connected through an IntersiteLink



About Linking Unity Connection and Cisco Unity Sites

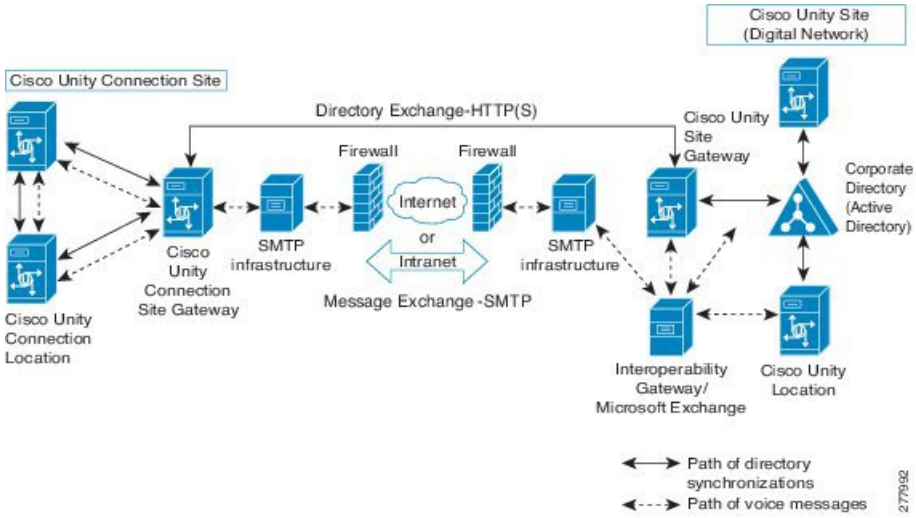
When you link a Cisco Unity site to a Unity Connection site, the gateway for each site is responsible for collecting information about all changes to the local site directory, and for polling the remote site gateway periodically to obtain information about updates to the remote site directory. The gateways use the HTTP or 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 a Microsoft Exchange 2010 or Exchange 2007 server configured with the Hub Transport role, or on a Microsoft Exchange 2003 server. (For up-to-date version support and requirements for the Interoperability Gateway, see the *Cisco Unity Networking Options Requirements* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.)

Messages composed by Cisco Unity users that include external recipients are routed by the mail system to a folder that the Interoperability Gateway periodically checks. The Interoperability Gateway picks up a message to be processed from the folder, looks up and translates the sender and recipient information into the required format, adds or removes message properties as applicable, converts and encrypts or decrypts the audio if applicable for the destination location, performs message part and format conversion, and hands the message back to the messaging system for delivery. For several of these tasks, the Interoperability Gateway needs access to Cisco Unity directory information. To get this information, it contacts the Cisco Unity web services resource on a Cisco Unity 8.x server in the Cisco Unity site. (The Interoperability Gateway can be configured to use both a primary and secondary web services server. The site gateway can be used as the web services server, although any 8.x server in the site can be used.)

Figure 3 depicts—at a high level—the role of the Interoperability Gateway for Microsoft Exchange, the site gateways, and the intersite link in connecting Cisco Unity and Cisco Unity Connection sites. The Cisco Unity site can consist of a single Cisco Unity server, a failover pair, or a Digital Network containing multiple Cisco Unity servers or failover pairs. Likewise, the Unity Connection site can consist of a single Unity Connection server, a Unity Connection cluster, or more than one server or cluster.

Figure 3: Cisco Voicemail Organization Consisting of a Cisco Unity Site Connected to a Unity Connection Site via anIntersite Link



Note that in order to link Cisco Unity and Unity Connection sites, all servers in the Unity Connection site must be running Unity Connection 12.x. The Cisco Unity site gateway must be running Cisco Unity 8.x. Other Cisco Unity servers in the Cisco Unity site may be running Cisco Unity 5.0 and later with Microsoft Exchange provided that the applicable engineering special is installed to add Unity Connection Networking support. For additional details and requirements, see the *Cisco Unity Networking Options Requirements* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.)

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.

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.

Unity Connection 12.x supports up to 10 VPIM locations and 100,000 VPIM contacts in the Unity Connection directory. These same limits apply either to the directory of a single Unity Connection server or cluster pair, or to the global directory in a site.

If you deploy VPIM in a Unity Connection networking site, you should designate a single Unity Connection location in the site as the bridgehead to handle the configuration of VPIM locations and contacts. 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 site. 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. Likewise, messages from VPIM contacts are received by the bridgehead and relayed to the home server of the Unity Connection recipient.

If you deploy VPIM in a Cisco Voicemail Organization, you must independently configure each site for VPIM. VPIM locations and contacts are not replicated across intersite links, and site gateways do not relay VPIM messages to other sites.

For detailed information about VPIM networking, see the "VPIM Networking" chapter.

Directory Synchronization

Each location in a Unity Connection site or Cisco Voicemail Organization has its own directory of users and other objects that were 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 and sites is referred to as the global directory.

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

- Replication Within a Unity Connection Site
- Replication Between Two Unity Connection Sites

Replication Within a Unity Connection Site

Within a Unity Connection site, each location replicates the objects and object properties shown in Table 1: Replicated Objects in a Unity Connection Site from its directory to every other location:

Table 1: Replicated Objects in a Unity Connection Site

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
System contacts	All properties
System distribution lists	All properties, including list membership
Partitions	All properties
Search spaces	All properties, including membership

Replicated Object	Replicated Properties
Unity Connection location	• Display name • Host address • SMTP domain name • Unity Connection version
VPIM location	All properties except Contact Creation settings (contact creation is handled on the Unity Connection location that homes the VPIM location)

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.

When a replicated object that is homed on a Unity Connection location is added, modified or deleted, the location sends an object change request containing details about the change to all other locations. The object change requests for a given location are ordered and tracked with a number known as the Unique Sequence Number (USN). For each change, the location increments the USN by one, and notes the change in its database. When a remote location receives an object change request with a USN value that is one higher than the previous request it received from the sender, it updates its copy of the Unity Connection directory accordingly, and increments its tracked copy of the USN for the sender. If a remote location misses one or more changes and receives a change request with a USN that is more than one higher than the previous request it received from this location, it can retrieve the missed changes by requesting the USN values that it missed.

In addition to the USN, each location has another associated number known as the Replication Set. The Replication Set value is used to track the set of changes to which a USN belongs. The Replication Set value is automatically changed during an upgrade, restore, or rollback operation. This ensures that any changes to the database as a result of the operation are replicated to the network. For example, if Location A receives a message with replication set 10 and USN 5 from Location B, and then receives a message with replication set 9and USN 5 from Location B, it knows to ignore the message with replication set 9 because it is a lower number and the message predates the message with replication set 10. If Location A receives another message from Location B with replication set 10 and USN 5 again, Location A knows this is a duplicate message and can ignore it.

When a bulk operation is in progress on a location, replication is paused on that location until the operation completes.

Replication Between Two Unity Connection Sites

As shown in Table 2: Objects Replicated from One Unity Connection Site to Another, the same objects and object properties are replicated between two Unity Connection sites as within a single Unity Connection site, with the following exceptions:

- System contacts are not replicated between sites.

- For each site, you can select whether to synchronize all system distribution lists that are homed on the remote site. Also, for each individual list, you can select whether the list is offered for replication to the remote site.
- System distribution list membership is not replicated between sites.
- VPIM locations (and contacts) are not replicated between sites.

Table 2: Objects Replicated from One Unity Connection Site to Another

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 [1] • SMTP address and SMTP proxy addresses
System distribution lists [2]	• Alias • Display name • Extension • Partition • Recorded name[1]
Partitions	All properties
Search spaces	All properties
Unity Connection locations	• Display name • Host address • SMTP domain name • Unity Connection version

[1] For each site, you can select whether to synchronize recorded names for remote site objects.
[2] A local site system distribution list is only synchronized by the remote site if the Include Distribution Lists When Synchronizing Directory Data check box is checked for the intersite link on the remote site gateway, and the Replicate to Remote Sites Over Intersite Links check box is checked for the list.

Just as with intrasite links, you can use replicated objects from a remote site just as you would use local objects, except that call handler owners must be local users, and objects that belong to a partition can only belong to local partitions.

Intersite replication is accomplished by means of a Feeder service and a Reader service running on each site gateway. The Reader service periodically polls the remote site gateway 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 site gateway, 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 on a site gateway, you can access the schedules on the Tools > Task Management page selecting either the Synchronize Directory With Remote Network task or the Synchronize Voice Names With Remote Network task. Alternatively, you can access either task using the Related Links field on the Edit Intersite Link page.

When the Synchronize Voice Names With Remote Network task is enabled, the reader process recorded name files for remote users and system distribution lists (if applicable). Once a recorded name is created for a remote object on the local site, it is updated only if the remote and local filenames for the recorded name differ. If, for example, you change the outgoing codec for recorded names on the remote site gateway, the local site does 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 site gateway and then do a full resynchronization using the Clear Recorded Names button and the Resync All button on the Search Intersite Links page in Unity Connection Administration.Replication Between Cisco Unity and Unity Connection Sites

When you link a Cisco Unity site and a Unity Connection site, a contact (known as a Unity Connection Networking subscriber in the Cisco Unity Administrator) is added to the Cisco Unity directory and to Active Directory for each Unity Connection user. Likewise, a user (known as a Cisco Unity user in Cisco Unity Connection Administration) is added to the Unity Connection site global directory for each Cisco Unity user. Unity 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.

A system distribution list may be replicated from one site to another if the local site is configured to pull lists from the remote site, and if the list itself is configured to allow replication to other sites. 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.

Table 3: Objects Replicated Between Cisco Unity and Unity Connection Sites lists the objects that are replicated between Cisco Unity and Unity Connection sites, and the object properties that are replicated.

Table 3: Objects Replicated Between Cisco Unity and Unity Connection Sites

Replicated Object	Replicated Properties
Unity Connection users with mailboxes	• Alias • First name, last name, display name, alternate names • Extension, cross-server transfer extension, and alternate extensions [3] • Directory listing status • Recorded name [4] • SMTP address and SMTP proxy addresses
Cisco Unity users	• Alias • First name, last name, display name, alternate names • Extension, transfer extension, and alternate extensions • Directory listing status • Recorded name [4]
System distribution lists [5]	• Alias • Display name • Extension [3] • Recorded name [4]
Locations	• Display name • Host address • SMTP domain name

[3] Unity Connection extensions are replicated to Cisco Unity only if they do not conflict with existing objects in the dialing domain as defined on the Cisco Unity site gateway.
[4] For each site, you can select whether to synchronize recorded names for remote site objects.
[5] A system distribution list is only synchronized from another site if the intersite link is configured to allow synchronization of remote lists, and the list itself is configured to allow replication to other sites.

Intersite replication is accomplished by means of a Feeder service and a Reader service running on each site gateway. The Reader service periodically polls the remote site gateway 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 the Unity Connection site gateway, 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 on a site gateway, you can access the schedules on the Tools > Task Management page selecting either the Synchronize Directory With Remote Network task or the Synchronize Voice Names With Remote Network task. Alternatively, you can access either task using the Related Links field on the Edit Intersite Link page.

On the Cisco Unity site gateway, you can enable or disable synchronization of recorded names, and configure the interval at which the Reader polls the Unity Connection Feeder for directory updates and recorded names. Note that unlike the Unity Connection Reader, which has separate configurable schedules for polling directory data and recorded names, the Cisco Unity Reader polls for both (if recorded name synchronization is enabled) during each cycle.

When the Synchronize Voice Names With Remote Network task is enabled, the Reader processes the recorded name files for remote users and system distribution lists (if applicable). When a recorded name has been created for a remote object on the local site, it is updated only if the remote and local filenames for the recorded name differ. If, for example, you change the outgoing codec for recorded names on the remote site gateway, the local site does not update its files because the change does not affect filenames. In order to pull updated copies of recorded names from Cisco Unity to Unity Connection, you must clear all existing recorded names from the Unity Connection site gateway using the Clear Recorded Names button on the Networking > Links > Search Intersite Links page in Unity Connection Administration. In order to pull updated copies of recorded names from Unity Connection to Cisco Unity, use the Clear Voice Names button on the Network > Unity Connection Networking Profile page in the Cisco Unity Administrator.

Directory Size Limits

The Unity Connection global directory (the entire collection of local and replicated objects) is subject to certain size limits. The same limits apply both to a single Unity Connection site or to a Cisco Voicemail Organization of linked sites (regardless of whether a Unity Connection site is linked to another Unity Connection site or to a Cisco Unity site). In a Cisco Voicemail Organization, exceeding the limits affects the ability to link sites together, and to replicate additional directory objects across the intersite link when the sites have been linked. In Unity Connection 12.x, there are separate limits on the number of users and contacts and on the number of system distribution lists.

The size limits at the time of Unity Connection 12.x are:

- A combined total of 100,000 users and system contacts (both contacts associated with a VPIM location and those not associated with a location)
- 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 12.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/12x/requirements/12xcucsysreqs.html.

When you attempt to link a Unity Connection site to another Unity Connection site or to a Cisco Unity site, both the user and system contact limit and the system distribution list limit are checked by the Unity Connection site gateway. If the combined number of users and contacts on the gateway after the link is created would exceed the user and contact limit, or the combined number of system distribution lists on the gateway would exceed the list limit, you cannot link the sites. (Note that the global directory sizes of two sites do not necessarily match after they are linked because contacts are not replicated across the intersite link. However, each Unity Connection site is still subject to the maximum size limits, which include system contacts.)

Consider the following example of the user and system contact limit check. Unity Connection site A has 40,000 users and 5,000 system contacts, and Unity Connection site B has 50,000 users and 15,000 contacts. If you linked these sites together, the global directory on Unity Connection site A would have 95,000 user and contact objects (40,000 plus 5,000 plus 50,000). However, the global directory on Unity Connection site B would have a total of 105,000 user and contact objects (50,000 plus 15,000 plus 40,000). Attempting to join these two sites would fail because the user and contact limit is exceeded on site B. However, attempting to join Unity Connection site A with a Cisco Unity site that has 50,000 users and 15,000 networking contacts would succeed, because the Unity Connection site global directory of 95,000 user and contact objects would not exceed the 100,000 user and system contact limit.

In addition to checking the limits at the time two sites are joined, each Unity Connection site gateway also checks the user and system contacts limit and the system distribution lists limit each time the Reader service runs. If the limits have been exceeded by five percent or more, the Reader service is no longer able to create new directory objects for remote site objects. It continues to make changes to existing objects or delete them if they are removed from the remote site. This state is therefore known as “delete mode.” In order to get the Reader out of delete mode, you must remove a sufficient quantity of objects of the appropriate type to get to less than five percent above the limit (for example, remove remote users, local users, or local system contacts if the user and system contact limit has been exceeded, or remove local or remote system distribution lists if the system distribution list limit has been exceeded.)

Messaging

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

How Messages to System Distribution Lists are Handled Within a Unity Connection Site

Because system distribution lists are replicated among locations in a Unity Connection site, 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 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 on the list, the sending location delivers the message to each location that homes these remote users. If there are VPIM users on 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 a Unity Connection site, 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.

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 site that contains the All Voicemail Users list of each Unity Connection location.

How Messages to System Distribution Lists are Handled Between Sites

With intersite networking (either between Unity Connection sites or between Cisco Unity and Unity Connection sites), replication of system distribution lists is optional, and when lists are replicated, only the information needed to address a message to the list is replicated. Therefore, when a user addresses a message to a system distribution list that is homed in another site, the message is routed to the remote site gateway (if the remote site is a Unity Connection site) or to the Interoperability Gateway for Microsoft Exchange (if the remote site is a Cisco Unity site). At this point, the system distribution list recipient is handled as though the message originated within the remote site.

It is possible to nest system distribution lists such that a local list contains remote lists as members. For example, you could nest the All Voicemail Users distribution list from one site within the All Voicemail Users list of the other site. (If you are networking Cisco Unity with Unity Connection, note that Unity Connection users may be automatically created as members of the All Subscribers list or other lists depending on the template that you specify when creating the intersite link.) When you nest a remote list as a member of a local list, you should follow the given practices:

- Avoid nesting local lists as members of the remote list.
- Do not allow the local list to replicate to the remote site.

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 4: Cross-Server Features.

Table 4: 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).

The cross-server features can be enabled both within a site and across the entire Cisco voicemail organization. For more information and instructions on enabling the cross-server features, see the "Cross-Server Sign-In, Transfers, and Live Reply" chapter.

Addressing and Dial Plan Considerations

See the following sections for addressing and dial plan considerations in specific networking situations:

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.

Considerations for Intersite Networking Between Cisco Unity and Unity Connection

See the following sections:

Unity Connection Search Spaces and Cisco Unity Users

When you link a Cisco Unity site and a Unity Connection site, a partition is automatically created in the Unity Connection directory for each Cisco Unity server, and all Cisco Unity users and system distribution lists that are homed on the server are placed in the partition. However, the partition is not automatically added to search spaces on the Unity Connection locations. In order for Unity Connection users to have permission to address messages to Cisco Unity users, you must add the partition to the search spaces used by those Unity Connection users. Note that the order a partition appears in a search space is important if users address messages by extension. If, for example, Unity Connection and Cisco Unity users have overlapping 4-digit extensions and you want Unity Connection users to be able to reach other Unity Connection users by their 4-digit primary extension and reach Cisco Unity users by a unique 7-digit alternate extension, make sure that the Cisco Unity partition appears after any Unity Connection partitions that contain the overlapping 4-digit extensions.

Cisco Unity Dialing Domains and Unity Connection Users

A dialing domain is a collection of servers that access the same directory and that are integrated with the same phone system or phone system network. A dialing domain is a grouping scheme that allows Cisco Unity to handle call transfers and addressing by extension from one server to another. Within the dialing domain, extensions must be unique just as the phone extensions in the phone system must be unique.

When you link a Cisco Unity site and a Unity Connection site, the Unity Connection user and system distribution list objects that are created in the Cisco Unity directory belong to the dialing domain that is configured on the Cisco Unity site gateway. Because the Unity Connection search space and partition design accommodates overlapping extensions and may include users who have a primary extension and alternate extensions in different partitions, you must select how to map Unity Connection extensions to the Cisco Unity dialing domain. To do so, for each Unity Connection location, you specify a single partition that Cisco Unity pulls extensions from. (In Cisco Unity Connection Administration, you configure the Local Partition That Cisco Unity Users Can Address to By Extension field on the Edit Location page for the local location.) For example, consider a Unity Connection user, Kelly Bader, who has two extensions—a primary extension (4441) in the “Sales Partition” and an alternate extension (2025555) in the “Chicago Partition.” If the partition that maps extensions to the dialing domain for Kelly’s home server location is “Chicago Partition,” Cisco Unity users can address to Kelly by entering extension 2025555; they do not address to her by entering extension 4441. If the partition that maps to the dialing domain for Kelly’s location is changed to “Sales Partition,” Cisco Unity users can address to Kelly by entering extension 4441 but not by entering extension 2025555. (In either case, Cisco Unity users can address to Kelly by name rather than by extension.)

If the extension of a Unity Connection user conflicts with an existing extension in the dialing domain, and the user has alternate extensions available in the partition that Cisco Unity pulls from, Cisco Unity attempts to assign one of the alternate extensions of the user as the extension of the corresponding contact object. If there are no alternate extensions available or if the alternate extensions all conflict with existing extensions in the dialing domain, the new object is created without an extension, and can only be addressed by name. Similarly, if the object does not have any extension in the partition that maps to the dialing domain, the new object is created without an extension.

Combining Cisco Unity Unified Messaging and Unity Connection Integrated Messaging When Users Have Accounts in the Same Active Directory Deployment

When you link a Cisco Unity Unified Messaging site with a Unity Connection site and users in both sites have email accounts in the same Active Directory environment, the contacts that Cisco Unity creates for Unity Connection users can complicate the user experience when users address messages via ViewMail for Outlook or other email clients.

Consider as an example the following two users:

- Pat Jones, a Cisco Unity user with a Unified Messaging account that uses the alias pjones@example.com. Pat uses Microsoft Outlook and Cisco Unity ViewMail for Outlook to access email and voice messages in one mailbox.
- Robin Smith, a Unity Connection user who also has a separate Microsoft Exchange email account with alias rsmith@example.com. Robin uses Microsoft Outlook and Unity Connection ViewMail for Outlook to access email in the Exchange mailbox and voice messages in the Unity Connection mailbox.

Prior to linking the Cisco Unity and Unity Connection sites, the contacts list that Pat and Robin use in Outlook contains one entry for Pat Jones as pjones@example.com and one for Robin Smith as rsmith@example.com. Robin also has rsmith@example.com defined as an SMTP proxy address in Unity Connection in order to send voice messages with Unity Connection ViewMail for Outlook and receive messages that are addressed using the Outlook contacts list. (Before the two sites are linked, however, Pat and Robin cannot use their ViewMail clients to send voice messages to each other).

Once the two sites are linked, Cisco Unity adds an additional contact to Active Directory for Robin Smith. By default, this contact has a display name of "Robin Smith - Voicemail" to distinguish it from Robin's Exchange account. (The -Voicemail display name suffix is configurable.) The contact has an SMTP address in the format UCI_<alias>_BH-<Unity Connection location identifier>@<domain generated according to Exchange Contact-creation policies>. Cisco Unity users can and should use this contact when addressing voice messages via ViewMail. Voice messages addressed to Unity Connection user email accounts rather than to their contacts are delivered as emails with voice attachments and do not light the user message waiting indicator or otherwise be accessible via Unity Connection.

If another Unity Connection user tries to address a voice message to the "Robin Smith - Voicemail" contact in the contacts list, this message is returned as undeliverable by default, because Unity Connection does not recognize the UCI_<alias>_BH-<Unity Connection location identifier>@<Cisco Unity site gateway domain> address as belonging to a Unity Connection user. To mitigate this issue, you can add the address as an SMTP proxy address for the user. (You can use Active Directory Users and Computers to export a list of Unity Connection contacts, then add SMTP proxy addresses to Unity Connection users in bulk using the Bulk Administration Tool. For information on using the Bulk Administration Tool, see the "Bulk Administration Tool" section of the "Tools" chapter of the *System Administration Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

With the SMTP proxy address in place for Robin, other Unity Connection users can send voice messages to the "Robin Smith - Voicemail" contact. However, if a Unity Connection user tries to address an email to the contact, the email is returned as undeliverable.

Cisco Unity users have one entry in Active Directory even after the sites are linked. Users in either site can address voice messages to the entry in ViewMail for Outlook.

Note that if you select to synchronize one or more Unity Connection system distribution lists into a Cisco Unity Unified Messaging deployment, an Active Directory group is created for each list, which users can see in the contacts list. The group is created with the same configurable suffix ("- Voicemail" by default) added to the display name. As with the user contact entries, Unity Connection users who try to address messages to the group receives a non-delivery receipt in response. However, in this case, you cannot currently mitigate the issue for synchronized distribution lists using SMTP proxy addresses because you cannot configure SMTP proxy addresses for lists. To work around the issue, you have a couple of options:

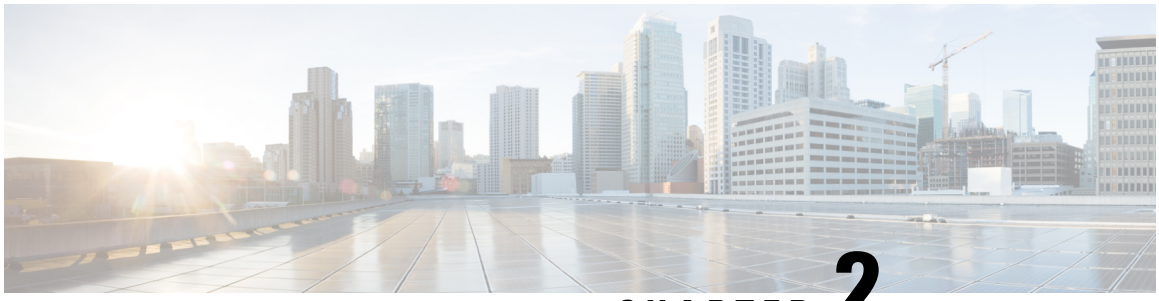
- Do not synchronize Unity Connection system distribution lists to the Cisco Unity site. Instead, create any lists that Cisco Unity users need directly on the Cisco Unity site, adding Unity Connection contacts as members when necessary.

- Use multiple contact lists in Microsoft Exchange to segment addressing between Cisco Unity and Unity Connection users so that Unity Connection users do not have access to the addresses of groups that Cisco Unity creates for Unity Connection lists.

Note that while Unity Connection users should not address messages to Unity Connection system distribution lists using the group address-book entry, they can address messages to Unity Connection lists by entering the list address in the format <list alias>@<Unity Connection server SMTP domain>.

Migrating Users From Cisco Unity to Unity Connection

When intersite networking is configured between Cisco Unity and Unity Connection, you can gradually migrate Cisco Unity users to Unity Connection 12.x. For more information, 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 12x*, available at: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html.



CHAPTER 2

Setting Up Networking Between Cisco Unity Connection Servers

Setting Up a Unity Connection Site

This section describes the prerequisites for setting up a Cisco Unity Connection site, and provides a high-level task list of all of the tasks that you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with Unity Connection site concepts, you should first read the "Overview of Networking Concepts" chapter and then review the task list and procedures before beginning the setup.

You can link up to ten Unity Connection locations in a single site. If you have more than 10 locations, set up two sites and link them together. (In order to link sites, all servers in each site must be running Unity Connection version 12.x. You cannot link more than two sites together.) For procedures, see the Linking Two Unity Connection Sites.

Prerequisites for Setting Up a Unity Connection Site

Before starting the setup, verify that the following prerequisites have been met on each server that joins the site (for clusters, verify these prerequisites for the publisher server):

- The server meets the requirements listed in the "Requirements for Intrasite Networking" section of the System Requirements for Cisco Unity Connection *Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.
- Unity Connection is already installed.
- The servers networked together are directly accessible through TCP/IP port 25 (SMTP), or SMTP messages are routable through an SMTP smart host.
- For Unity Connection clusters, 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 addition, before setting up a Unity Connection site, you should be familiar with the concepts in the "Dial Plan" section of the "Call Management" chapter of the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Task List for Setting Up a Unity Connection Site

Use this task list to set up a networking site between Unity Connection servers or clusters. The cross-references take you to detailed procedures.

If you have a Unity Connection cluster, do the tasks only on the publisher server.

1. Make decisions about your networking deployment approach and gather information needed to configure the site. See the Making Deployment Decisions and Gathering Needed Information for Setting Up a Site.
2. Check the display name of each server that you are joining to the site, and modify it if it is not unique, or if you want to select a more descriptive name. Also check the SMTP domain of each server that you are joining to the site, and modify it if it is not unique. See the Verifying Each Unity Connection Server has a Unique Display Name and SMTP Domain.

   If the display name of a server matches the display name of another server on the site, the server cannot join the site. Likewise, if the SMTP domain matches the SMTP domain of another server on the site, the server cannot join the site.
3. Start by linking two Unity Connection servers together to create a site, then link additional servers to any location in the site. See the Linking Unity Connection Servers with an Intrasite Link.
4. If any servers in the site require a smart host to transmit and receive SMTP messages from other servers (for example, because a firewall separates the servers, or because the servers are part of a Unity Connection cluster), configure the smart host, and configure the applicable locations to route through the host. See the Configuring a Smart Host.

Note For each Unity Connection cluster that you have added to the site, you must configure all other locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down. (You also configure the smart host to resolve the SMTP domain of the cluster to both the publisher and subscriber servers.)

5. For each cluster that you have added to the network, add the IP address of the subscriber server to the IP address access list on every other location on the network; this ensures that other locations can receive message traffic from the subscriber server if the publisher server is down. See the Configuring SMTP Access for Cluster Subscriber Servers.
6. Verify that replication is complete among locations. See the Checking Replication Status Within a Site.
7. Configure search spaces at each location to allow users who are homed at the location to address to users at other locations. See the Configuring Search Spaces for Unity Connection Sites.
8. Secure the site so that message transmissions are not misdirected. See the Securing the Unity Connection Site.
9. Optionally, set up cross-server features. See the "Cross-Server Sign-In, Transfers, and Live Reply" chapter.

10. Test the site. See the Testing the Intrasite Setup.
11. Optionally, set up a site-wide All Users distribution list. See the Creating a Site-Wide All Voicemail Users Distribution List.
12. If any servers in the site were previously configured as VPIM locations on other servers in the network, clean up the unused VPIM locations. See the Cleaning Up Unused Unity Connection VPIM Locations and Contacts.
13. If you have not already done so, set up VPIM Networking to connect the Unity Connection locations to any other VPIM-compatible voice messaging systems. See the "VPIM Networking" chapter.
14. Optionally, create a mapping of which users are homed on which location. See the Mapping Users to Their Home Locations.
15. Optionally, if you have a large site that includes locations running Unity Connection 12.x, review the advanced settings available on the System Settings > Advanced > Intrasite Networking page in Cisco Unity Connection Administration in case you need to tune the communications between the Unity Connection Digital Networking Replication Agent services on these locations.

Also note that the Limit Number of Simultaneous Incoming Connections and Limit Number of Simultaneous Outgoing Connections fields on the System Settings > SMTP Configuration > Server page in Unity Connection Administration affect the replication agent (and also affect intrasite messaging between users as well as other features that use SMTP for message transmission).

Procedures for Setting Up a Unity Connection Site

Making Deployment Decisions and Gathering Needed Information for Setting Up a Site

Before you begin setting up a site, be sure to plan for the following, and gather the applicable information:

- If your network includes voice messaging servers that do not meet the prerequisites for joining a Unity Connection site but support the Voice Profile for Internet Mail (VPIM) protocol (for example, Cisco Business Edition, Unity Connection 2.x servers, Cisco Unity 4.x and 5.x, or other VPIM-compatible systems), use VPIM Networking to connect them.

  Follow the given approaches:

  - Unless your servers are already configured for VPIM, set up the site first, then set up VPIM Networking.
  - Select a single Unity Connection location in the site to handle the configuration of VPIM locations and contacts. This location is referred to as the "bridgehead." The VPIM location and contact objects are replicated from the bridgehead to all digitally networked Unity Connection locations so that those locations can address VPIM messages; the networked locations then forward the messages to the bridgehead for delivery to the remote voice messaging server. 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.
  - If you have already configured VPIM locations on multiple systems that are joining a site, delete duplicate VPIM locations from all but one server before setting up the site. For instructions, see the "Removing a VPIM Location" section.
  - If you are migrating a VPIM location to a Unity Connection site (for example, because you used VPIM Networking to connect two or more Unity Connection 2.x servers and have upgraded the

servers to Unity Connection 12.x) set up the Unity Connection site first. After the directory is fully replicated and you have tested message exchange between the Unity Connection locations, remove the VPIM locations and VPIM contacts that represent the migrated servers and their users. The task list reminds you when to do this task.

- By default, every Unity Connection location (server or cluster) includes several predefined system distribution lists, which you can modify but not delete. If you have not renamed these lists so that the list names are unique on each location, or if you have added additional lists whose names are identical across locations, during initial replication each location automatically adds the remote server name to the display name of any remote lists whose names overlap with local list names. (The default lists are All Voicemail Users, Undeliverable Messages, and All Voicemail-Enabled Contacts.) This can cause confusion when local users try to address to those remote lists.

  To solve this problem, you can use one of the following approaches:

  - If you want to maintain separate lists on each location, you can modify the name of each list on its home location so that it is unique (for example "All Voicemail Users on <Location Name>") and notify your users of the new list names for each server. If you select this approach, you should also modify the recorded name of each list to indicate its source.
  - Alternatively, after setting up the site, you can create a master list that includes all users on all networked locations. The task list includes instructions on when and how to do this task.

- If you want to synchronize Unity Connection user data with user data in an LDAP directory, you should configure Unity Connection for integration with the LDAP directory prior to setting up the site, to simplify testing and troubleshooting.
- Make note of the following information about each server that is joining the network:
  - The IP address or fully qualified domain name (FQDN) of the server.
  - The user name and password of a user account that is assigned to the System Administrator role.
  - The dial strings that other servers use to call this server, if cross-server sign-in or transfer is configured on other servers to hand off calls to this server.

Verifying Each Unity Connection Server has a Unique Display Name and SMTP Domain

Each Unity Connection server that you join to a Unity Connection site must have a unique display name. The display name must be unique both among Unity Connection locations and among VPIM locations. If the display name is not unique, the server cannot join the site. For new Unity Connection installations, the display name is typically the same as the host name of the server; however, if you changed the display name or upgraded the server from Unity Connection 2.x (which uses "Local VMS" as the default display name), you may need to change the display name so that it does not overlap with other locations on the network.

Tip Select a display name for each server that is descriptive and that helps you identify the location when it is listed among all locations in the organization in Cisco Unity Connection Administration.

Each Unity Connection server that you join to the site must also have a unique SMTP domain, both among Unity Connection locations and among VPIM locations. By default, the SMTP domain is configured during installation to include the hostname of the server, in order to insure that it is unique. However, if the SMTP

domains of multiple servers have been modified to the same value, you must change the domains to unique values before joining the servers in a site.

If you are migrating a server from VPIM Networking to intrasite or intersite networking, it is likely that the display name or SMTP domain of the server overlaps with the VPIM location configured for the server. If the domain name overlaps, you need to disrupt messaging to the VPIM location while doing the migration—either by changing the SMTP domain of the VPIM location, or by removing the VPIM location. (To remove the VPIM location, see the "Removing a VPIM Location" section.)

Do the following procedure to Verify each Unity Connection server :

Step 1 Check the Display Name of the first server:

a) In Cisco Unity Connection Administration on the first server, expand **Networking and** select **Locations**.
b) On the Search Locations page, note the Display Name of the local server. Make a list of all Display Names that you can consult later.

Step 2 Check the SMTP domain of the first server:

a) Expand **System Settings > SMTP Configuration and** select **Server**.
b) On the SMTP Server Configuration page, note the SMTP Domain of the local server.

Step 3 Check the Display Name and SMTP Domain Name of all VPIM locations homed on the local server:

a) Expand Networking and select **VPIM**.
b) On the Search VPIM Locations page, note the Display Name of each VPIM location.
c) Select the first VPIM location in the table. On the Edit VPIM Location page, note the SMTP Domain Name of the VPIM location.
d) Select **Next** and note the SMTP Domain Name of the next VPIM location.
e) Repeat Step 3d. for each remaining VPIM location.

Step 4 Repeat Step 1 through Step 3 on each location that is joined to the site.

Step 5 If the Display Name of a location conflicts with that of another location, or you want to modify a name to be more descriptive, change one of the display names:

- To change the Display Name of a Unity Connection location, follow Step 6.
- To change the Display Name of a VPIM location, follow Step 7.
- If the Display Names are all unique, skip to Step 9.

Step 6 Change the Display Name of the Unity Connection location:

a) On the server for which you want to change the Display Name, expand **Networking and** select **Locations**.
b) Select the Display Name of the local server.
c) On the Edit Location page, modify the Display Name value, and select **Save**.

Step 7 To change the Display Name of a VPIM location:

a) On the server on which the VPIM location is homed, expand **Networking** and select **VPIM**.
b) On the Search VPIM Locations page, select the Display Name of the location that you want to change.
c) On the Edit VPIM Location page, edit the Display Name value and select **Save**.

Step 8 If there are any remaining Display Name conflicts, repeat Step 5 as necessary to resolve each conflict.

Step 9 If the SMTP domain of a server conflicts with that of another location, change one of the domain names:

- To change the SMTP Domain of a Unity Connection location, follow Step 10.

- To change the SMTP Domain Name of a VPIM location, follow Step 11.

Step 10 To change the SMTP Domain of a Unity Connection location:

a) Expand **System Settings > SMTP Configuration**, then select **Server**.
b) On the SMTP Server Configuration page, select **Change SMTP Domain**, change the value of the SMTP Domain field, and select **Save**.
c) Select **OK** to confirm the change.

Step 11 To change the SMTP Domain Name of a VPIM location:

a) On the server on which the VPIM location is homed, expand **Networking** and select **VPIM**.
b) Select the Display Name of the VPIM location for which you want to change the SMTP Domain Name.
c) On the Edit VPIM Location page, change the value of the SMTP Domain Name field, and select **Save**.

Changing the SMTP Domain Name of a VPIM location may disrupt messaging with the remote voice messaging system.

Step 12 If there are any remaining SMTP domain conflicts, repeat Step 9 as necessary to resolve each conflict.

Linking Unity Connection Servers with an Intrasite Link

To create a Unity Connection site, you start by linking two servers together via an intrasite link. Each server becomes a location in the new site. (When a Unity Connection cluster is linked to a site, the cluster counts as one location in the site.)

When you add a Unity Connection server to an existing Unity Connection site of two or more locations, you link the server to a single location in the site; the server that you are adding receives a list of all the other locations in the site, exchanges information with each location, and begins replicating directory information with each location.

This section contains two procedures. You should start by doing the first procedure; if Cisco Unity Connection Administration does not indicate that the servers have successfully been linked in the first procedure, do the second procedure. Then, repeat the process for each additional server that you are adding to the site.

Note You can use these procedures to join two Unity Connection 12.x servers or to join a Unity Connection 12.x server with a Unity Connection 7.x server. The names of the pages and fields changed between 7.x and 8.x; the 7.x names appear in parenthesis at the end of each step where the terminology differs.

Automatically Joining Two Unity Connection Servers

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking** > **Links** > **and** select **Intrasite Links**. (In Cisco Unity Connection 7.x, expand **Networking**, then select **Unity Connection Locations**.)

Step 2 Select **Join Site**. (In Unity Connection 7.x, select **Join Unity Connection Network**.)

Step 3 On the Join Site page, select **Automatically Join the Site**. (In Unity Connection 7.x, on the Join Unity Connection Network page, select **Automatically Join the Network**.)

Step 4 In the Remote Location field, enter the IP address or fully-qualified domain name (FQDN) of the Unity Connection server to connect to in order to create the site.

Step 5 In the Remote User Name field, enter the user name of an administrator at the location specified in the Remote Location field. The administrator user account must be assigned the System Administrator role.

Step 6 In the Remote Password field, enter the password for the administrator specified in the Remote User Name field.

Step 7 Select **Auto Join Site**. (In Unity Connection 7.x, select **Auto Join Network**.)

Step 8 When prompted, select **OK** to confirm. If the status message indicates that you have successfully joined the network and need to activate and start the Unity Connection Digital Networking Replication Agent, continue with Step 9. Otherwise, skip the rest of this procedure and continue with the Manually Joining Two Unity Connection Servers.

Step 9 On either server, in Cisco Unity Connection Serviceability, select **Tools** > **Service Management**. (For information on using Cisco Unity Connection Serviceability, see the *Administration Guide for Cisco Unity Connection Serviceability Release 12.x*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/serv_administration/b_12xcucservag.html.)

Step 10 In the Server list, select the Unity Connection server, and select **Go**.

Step 11 Under Optional Services, locate the Connection Digital Networking Replication Agent and select **Activate**.

Step 12 Repeat Step 9 through Step 11 on the other server.

Manually Joining Two Unity Connection Servers

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking**> **Links** > **and** select **Intrasite Links**. This server is referred to as the first server for the remainder of the procedure, and the other server is referred to as the second server. (In Unity Connection 7.x, expand **Networking**, then select **Unity Connection Locations**.)

Step 2 Select **Join Site**. (In Unity Connection 7.x, select **Join Unity Connection Network**.)

Step 3 On the Join Site page, select **Manually Join the Site**. (In Unity Connection 7.x, select **Manually Join the Network**.)

Step 4 Select **Download** and save the first server configuration file to a location on your hard drive, or on media that you can use to copy the file to the second server.

Step 5 Browse to Unity Connection Administration on the second server.

Step 6 In Unity Connection Administration on the second server, expand **Networking**> **Links** > **and** select **Intrasite Links**. (In Unity Connection 7.x, expand **Networking**, then select **Unity Connection Locations**.)

Step 7 Select **Join Site**. (In Unity Connection 7.x, select **Join Unity Connection Network**.)

Step 8 On the Join Site page, select **Manually Join the Site**. (In Unity Connection 7.x, select **Manually Join the Network**.)

Step 9 Select **Download**, and save the second server configuration file to a location on your hard drive, or on media that you can use to copy the file to the second server.

Step 10 In the Select the Remote Configuration File to Upload field, select **Browse** and browse to the copy of the configuration file that you downloaded from the first server in Step 4.

Step 11 Select **Upload**.

Step 12 In Unity Connection Administration on the first server, in the Select the Remote Configuration File to Upload field, select **Browse** and browse to your local copy of the configuration file that you downloaded from the second server in Step 9.

Step 13 Select **Upload**.

Step 14 On either server, in Cisco Unity Connection Serviceability, select **Tools** > **Service Management**.

Step 15 In the Server list, select the Unity Connection server, and select **Go**.

Step 16 Under Optional Services, locate the Unity Connection Digital Networking Replication Agent and select **Activate**.

Step 17 Repeat Step 14 through Step 16 on the other server.

Configuring a Smart Host

SMTP is used to transmit both directory information and messages between Unity Connection locations in a site.

If any pair of locations in the site cannot transmit and receive SMTP messages directly (for example, because a firewall separates the servers), you must configure these locations to route these messages through an SMTP smart host.

In addition, for each Unity Connection cluster that you add to the site, you must configure all other network locations to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down, and configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. For example, a network has a single smart host and the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a Unity Connection site, you would join ServerA, ServerB and ServerD together to form the site. Note the following:

- On ServerA, you would configure the Unity Connection locations for ServerB (which represents cluster 1) and ServerD (which represents cluster 2) to route through the smart host.
- On Server B (the cluster 1 publisher), you would configure the Unity Connection location for ServerD (which represents cluster 2) to route through the smart host.
- On ServerD (the cluster 2 publisher), you would configure the Unity Connection location for ServerB (which represents cluster 1) to route through the smart host.
- On the smart host, you would configure the SMTP domain name of cluster 1 to resolve to the IP addresses of both ServerB and ServerC (for example, using DNS MX records). You would also configure the SMTP domain name of cluster 2 to resolve to both ServerD and ServerE.

Do the following tasks for each server that requires routing to other locations through a smart host:

1. Configure the SMTP smart host to accept messages from the Unity Connection server. If your site includes Unity Connection clusters, also configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. See the documentation for the SMTP server application that you are using.
2. Configure the Unity Connection server to relay messages to the smart host. See the Configuring Unity Connection to Relay Messages to a Smart Host.
3. Configure the Unity Connection server to route messages to the other Unity Connection locations through the smart host. See the Configuring Unity Connection to Route Inter-Location Messages through the Smart Host.

Configuring Unity Connection to Relay Messages to a Smart Host

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **SMTP Configuration** and select **Smart Host**.

Step 2 In the **Smart Host** field, enter the IP address or fully qualified domain name of the SMTP smart host server. (Enter the fully qualified domain name of the server only if DNS is configured.)

Note To avoid infinite loop of SMTP notification in the mailbox, do not enter the IP address or fully qualified domain name of the following server as SMTP smart host:

- The localhost in case of standalone server
- The publisher and subscriber server in case of a cluster
- The servers that are networked together

Step 3 Select **Save**.

Configuring Unity Connection to Route Inter-Location Messages through the Smart Host

Step 1 In Cisco Unity Connection Administration, expand Networking and select **Locations**.

Step 2 Select the name of a location that requires routing through a smart host.

Step 3 Check the **Route to This Remote Location Through SMTP Smart Host** check box.

Step 4 Select **Save**.

Step 5 Repeat Step 1 through Step 4 for each additional location that requires routing through the smart host.

Configuring SMTP Access for Cluster Subscriber Servers

When you create a site that includes a Unity Connection cluster server pair, you join only the publisher server of the pair to the site. In order for all locations on the network to communicate directly with the cluster subscriber server in the event that it has Primary status, you must configure all network locations (except for the publisher server that is clustered with the subscriber server) to allow SMTP connections from the subscriber server.

Direct SMTP connectivity is needed so that locations can continue to receive user message traffic from the cluster while the publisher server does not have Primary status, in cases where routing from the cluster to other locations is not done via a smart host. Direct SMTP connectivity with the subscriber server does not impact directory updates, because directory updates are only replicated from the publisher server.

For example, a network has the following three locations:

- ServerA, which is not a cluster member
- Cluster 1, which is made up of ServerB, a publisher, and ServerC, a subscriber
- Cluster 2, which is made up of ServerD, a publisher, and ServerE, a subscriber

In order to create a site, you would join ServerA, ServerB and ServerD together. For direct SMTP access, the following steps are required:

- On ServerA, you would need to add the IP addresses of both ServerC and ServerE (the two subscriber servers) to the IP address access list so that ServerA can communicate with either subscriber server if it has Primary status.
- On ServerB (the cluster 1 publisher), you would add the IP address of ServerE (the cluster 2 subscriber) to the IP address access list; and on ServerD (the cluster 2 publisher), you would add the IP address of ServerC (the cluster 1 subscriber) to the IP address access list.

Alternatively, you can configure each cluster location to route messages to every other location through a smart host; when you do this, the other Unity Connection locations do not need to accept SMTP connections directly from the cluster subscriber in the event that it has Primary status, because the cluster subscriber establishes the SMTP connection with the smart host rather than directly with every other location. In the example above, the alternate configuration would entail the following:

- On ServerB (the cluster1 publisher), you would configure a smart host, and configure the Unity Connection locations for ServerA and ServerD (the cluster 2 publisher) to route through the smart host.
- On ServerD (the cluster 2 publisher), you would configure a smart host, and configure the Unity Connection locations for ServerA and ServerB (the cluster 1 publisher) to route through the smart host.

For instructions on configuring routing through a smart host, see the Configuring a Smart Host. Note that when more than one cluster is joined to a single site, you should have already configured each cluster to route messages to other clusters through the smart host; in this case, all you need do in addition is to configure the cluster to route through the smart host to any servers that are not configured as clusters.

Configuring Direct SMTP Access for Cluster Subscriber Servers

Step 1 On a network location, in Cisco Unity Connection Administration, expand **System Settings** > **SMTP Configuration** and select **Server**.

Step 2 On the Edit menu, select **Search IP Address Access List**.

Step 3 Select **Add New**.

Step 4 On the New Access IP Address page, enter the IP address of a cluster subscriber server at another location on the network.

Note Do not enter the IP address of the subscriber server on the publisher server that it is paired with.

Step 5 Select **Save**.

Step 6 On the Access IP Address page, check the **Allow Unity Connection** check box.

Step 7 Select **Save**.

Step 8 Repeat Step 2 through Step 7 for each additional subscriber server on the network (other than the subscriber server that is paired with the server you are configuring).

Step 9 Repeat Step 1 through Step 8 on each network location.

Checking Replication Status Within a Site

When initial replication begins among locations, it can take a few minutes to a few hours for data to be fully replicated between all locations, depending on the size of your directory.

The Unity Connection Intrasite Links and Locations pages in Cisco Unity Connection Administration can provide information about the status of replication between locations. Do the following procedure to check replication status in Unity Connection Administration.

Tip On Unity Connection 12.x locations, you can also use the Voice Network Map tool in Cisco Unity Connection Serviceability to check replication status. With the tool, you can quickly locate replication problems in a site, and get information about the status of replication between any two locations in the site. For more details, select Help > This Page from within the tool, or see the "Understanding the Voice Network Map Tool" section of the "Using the Voice Network Map Tool" chapter of the *Administration Guide for Cisco Unity Connection Serviceability Release 12.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/serv_administration/b_12xcucservag.html.

Checking Replication Status Within a Site Using Cisco Unity Connection Administration

Step 1 In Cisco Unity Connection Administration on a server that is joined to the network, expand **Networking** > **Links** and select **Intrasite Links**.

Step 2 On the Search Intrasite Links page, in the Intrasite Links table, the Push Directory column indicates whether a directory push to the remote location from the location you are accessing is in progress. The Pull Directory column indicates whether a directory pull from the remote location is in progress.

For example, if an administrator initiates a Push Directory To request from ServerA to ServerB, the Unity Connection Administration on ServerA shows that a directory push to ServerB is in progress, and the Unity Connection Administration on ServerB shows that a directory pull from ServerA is in progress.

Caution Initial replication happens automatically. Do not initiate a directory push or pull while initial replication is in progress.

Note Once initial replication is complete, changes are automatically synchronized between locations as they occur, even when the Push Directory and Pull Directory columns display a status of Idle.

Step 3 To get more information about the status of replication with a particular remote location, expand Networking and select **Locations**, then select the display name of the location.

Step 4 On the Edit Location page, the Last USN Sent, Last USN Received, and Last USN Acknowledged fields indicate the sequence numbers of replication messages sent to and from the remote location. If the Last USN Sent value is higher than the Last USN Acknowledged value, the remote location is not currently fully synchronized with this location; in this case, the Last USN Acknowledged value should continue to increase periodically. (Note that the Last USN Sent value may also increase periodically.)

Configuring Search Spaces for Unity Connection Sites

When you initially set up a site between locations, users who are homed on one location are not able to address messages to users at other locations, because the users on each location are in separate partitions and use search spaces that do not contain the partitions of users on the other locations. After initial replication completes between the locations, you can reconfigure your search spaces to include partitions that are homed on other servers, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a remote location. (Note that while both partitions and search spaces are replicated between locations, you cannot assign users or other objects to a partition that is homed on another location.)

At a minimum, if you have not made any changes to the default partitions and search spaces on any server, at each location you can add the default partition of each remote Unity Connection location to the search space that local users are using. For example, in a network of three servers named ServerA, ServerB, and ServerC with no changes to the system defaults, in Cisco Unity Connection Administration on ServerA you would add the "ServerB Partition" and "ServerC Partition" default partitions as members of the "ServerA Search Space" default search space; in Unity Connection Administration on ServerB you would add "ServerA Partition" and "ServerC Partition" to "ServerB Search Space," and so on.

For instructions on adding partitions to search spaces, see the "Dial Plan" section of the "Call Management" chapter of the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Securing the Unity Connection Site

No user credentials are transmitted as part of intrasite communications. However, in order to protect the security of SMTP addresses that are contained in the messages, make sure that any smart hosts that are involved in SMTP message transmission between Unity Connection locations are configured to route messages properly, as it may be possible to extract SMTP addresses from the messages. See the documentation for the SMTP server application that you are using for instructions.

Testing the Intrasite Setup

To test the site configuration, create test user accounts or use existing user accounts on each Unity Connection location. When setting up user accounts in Cisco Unity Connection Administration to be used in the tests, be sure to do the following for each account:

- Record a voice name.
- Record and enable an internal greeting.
- On the User Basics page, for Search Scope, select a search space that includes the partitions of remote users.
- On the User Basics page, check the List in Directory check box.
- On the Playback Message Settings page, check the Before Playing Each Message, Play the Sender's Information check box.
- Optionally, if you plan to enable and test cross-server live reply, ensure that the account belongs to a class of service for which the Users Can Reply to Messages from Other Users by Calling Them check box is checked on the Edit Class of Service > Message Options page. (The check box is not checked by default.)

Do the following tests to confirm that the site is functioning properly:

Verifying Messaging Between Users on Different Unity Connection Locations

Step 1 Sign in to a Unity Connection location as a user.

Step 2 Follow the prompts to record and send messages to users who are associated with other Unity Connection locations.

Step 3 Sign in to the applicable Unity Connection location as the recipient user to verify that the message was received.

Step 4 Repeat Step 1 through Step 3 in the opposite direction.

Verifying Call Transfers From the Automated Attendant to Users on Other Unity Connection Locations

Step 1 From a non-user phone, call a Unity Connection location that has been configured to handle outside callers, and enter the extension of a user who is associated with another Unity Connection location.

Step 2 Verify that you reach the correct user phone.

Verifying Call Transfers from a Directory Handler to Users on Other Unity Connection Locations

Step 1 From a non-user phone, call a Unity Connection location that has been configured to handle outside callers, and transfer to a directory handler.

Step 2 Verify that you can find a user who is associated with another Unity Connection location in the phone directory, and that the directory handler transfers the call to the correct user phone.

Verifying Identified User Messaging Between Networked Users (When Identified User Messaging is Enabled)

Step 1 Verify that Unity Connection plays an internal greeting for users who leave messages, by doing the following sub-steps:

a) From a user phone, call a user who is associated with another Unity Connection location, and allow the call to be forwarded to Unity Connection.

b) Verify that the internal greeting plays.

c) Leave a test message.

Step 2 Verify that users are identified when the recipient listens to a message, by doing the following sub-steps:

a) Sign in to the applicable Unity Connection location as the recipient user and listen to the test message that you recorded in Step 1.

b) Verify that the user conversation announces who the message is from by playing the recorded voice name of the sending user.

c) After listening to the message, verify that the user conversation allows you to reply to the message.

Verifying Live Reply Between Users on Different Unity Connection Locations

Step 1 From a user phone, call a user who is associated with another Unity Connection location, and allow the call to be forwarded to voicemail.

Step 2 Leave a message.

Step 3 Sign in to the applicable Unity Connection location as the recipient user and listen to the test message that you recorded in Step 2.

Step 4 After listening to the message, verify that the user conversation allows you to live reply to the message by saying "Call sender" or using the applicable key presses for the user conversation type. (To find the key presses for a particular conversation, see the "Cisco Unity Connection Phone Menus and Voice Commands" chapter of the User Guide for the

Cisco Unity Connection Phone Interface, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/user/guide/phone/b_12xcucugphone.html.)

Step 5 Verify that the live reply call is correctly transferred to the phone of the user who left the message.

Creating a Site-Wide All Voicemail Users Distribution List

If you would like to create a master distribution list that includes all users on all servers in the site, do the following tasks:

1. On each location in the site, rename the All Voicemail Users list with a unique name (for example All Voicemail Users on <Location Name>). For instructions, see the "System Distribution Lists" chapter of the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.
2. Create a new All Voicemail Users system distribution list on one location to use as the master list.
3. Add the lists from all locations as members of the master list.
4. Put all lists except the master list in partitions that do not belong to a search space that users use, so that they cannot address to any list except the master. For example, on each location, create a new partition called Hidden DLs on <Location Name> and put the list homed at that location in that partition. (By default, new partitions are not a member of any search space.)

Tip To avoid users generate large amounts of voice message traffic using reply-all to reply to messages sent to the master list, you should use search spaces to restrict access to the master list to a small subset of users. These users can use a search space that is essentially identical to the search space that other users use, except for the addition of the partition containing the master list.

Cleaning Up Unused Unity Connection VPIM Locations and Contacts

After migrating a Unity Connection server from VPIM Networking to being a member of a site, you should delete the VPIM location for the server on any other servers in the site that were previously using VPIM Networking to exchange messages with the server. Likewise, you should delete any VPIM locations on the server that represent other Unity Connection locations in the site. In order to successfully delete the VPIM locations, you must first delete all contacts that are associated with the location.

Note that when you delete the VPIM contacts that represent Unity Connection users, the contacts are removed from distribution lists; consider reviewing and updating distribution list membership on each server to include remote users as applicable. Also consider notifying users that they need to update the membership of any private lists that include contacts on the server being migrated.

For instructions on deleting a VPIM location and the associated VPIM contacts, see the "Removing a VPIM Location"

Mapping Users to Their Home Locations

Each server or cluster handles a distinct group of users. In large organizations, it is possible that more than one server or cluster is in use at the same physical location. In this case, you need to determine which user accounts to create on each of the servers (the "home" server or location for each user), and keep a record of the mapping. This record is needed for the following reasons:

- User phones must forward calls to the system on which the users are homed.
- If user phones have a "Messages" or a speed-dial button that dials the number to access voicemail, the buttons must be configured to call the system on which the users are homed.
- If you do not configure cross-server sign-in, users must dial the pilot number of the server or cluster that they are associated with to check their messages; in this case, you need to tell users the correct number to dial when calling their home server.

To create a record of the mapping, run the Users report on each Unity Connection location. The information in this report includes the user name and primary location. For more information, see the "Reports" section of the "Advanced System Settings" chapter in the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Linking Two Unity Connection Sites

Unity Connection 12.x supports linking up to two sites with an intersite link. In order to link sites, all servers in each site must be running Unity Connection version 10.x.

You can link up to 10 Unity Connection servers and/or clusters in a single site, and link two sites together. (Only one intersite link is supported per site.) If either site consists of more than one server or cluster, set up the sites before linking them. For procedures, see the Setting Up a Unity Connection Site.

Prerequisites

- If either or both sites consist of more than one server or cluster, set up the sites according to the Setting Up a Unity Connection Site.
- Verify that each server is running Unity Connection version 12.x.
- Check the size of your directory against the limits in the System Requirements for Cisco Unity Connection.
- The two locations (one in each site) that act as the gateways between the sites must be able to route directly to each other through TCP/IP port 25 (SMTP), or SMTP messages must be routable through an SMTP smart host. In addition, both gateways must be able to route to each other via HTTP on port 80 or HTTPS on port 443.
- Identify an account that you use to access Cisco Unity Connection Administration. The account must have the Manage Servers privilege. (The System Administrator and Technician roles each have this privilege.)

Task List for Linking Unity Connection Sites

Use this task list to set up an intersite link between two Unity Connection sites (referred to as an intersite link). The cross-references take you to detailed procedures.

If you have a Unity Connection cluster, do the tasks only on the publisher server.

1. Decide which location in each site is the site gateway and determine how messages are routed between the gateways. See the Determining the Site Gateway Locations and SMTP Routing Between Gateways.

2. Check the display name of each server in each site, and modify it if it is not unique among all the locations in both sites, or if you want to select a more descriptive name. Also check the SMTP domain of each server, and modify it if it is not unique. For a procedure, see the Verifying Each Unity Connection Server has a Unique Display Name and SMTP Domain.
3. Create the link. See the "Creating the Intersite Link" section.
4. Verify that replication is complete between the sites. See the Checking the Status of Synchronization Between Unity Connection Sites and Configuring Task Schedules.
5. Configure search spaces between sites. See the Configuring Search Spaces Between Unity Connection Sites.
6. Optionally, if you select to synchronize system distribution lists in either or both directions between the gateways, configure individual distribution lists to allow or prevent replication. See the Configuring Individual System Distribution Lists for Synchronization.
7. Optionally, set up an organization-wide All Users distribution list. See the Creating an Organization-Wide All Voicemail Users Distribution List.
8. Optionally, set up cross-server features between the locations. See theCross-Server Sign-In, Transfers, and Live Reply chapter.
9. For each site, if any servers in the remote site were previously configured as VPIM locations on other servers in the local site, clean up the unused VPIM locations. See the Cleaning Up Unused Unity Connection VPIM Locations and Contacts.

Procedures for Linking Unity Connection Sites

Determining the Site Gateway Locations and SMTP Routing Between Gateways

To create an intersite link, you select a single location on each site to act as a gateway to the other site. All intersite communications (both for directory synchronization and for message exchange) pass between the two gateways, thereby limiting the connectivity requirements and bandwidth usage to the link between those two locations. In order for directory synchronization and message exchange to occur between the two sites, the gateways you select must have the following connectivity with each other:

- HTTPS (if you select to encrypt the connection) or HTTP connectivity, for directory synchronization.
- SMTP connectivity, for message exchange.

Once you have selected the gateway locations, determine how to route SMTP messages between them. In each direction, you can route messages directly or use an SMTP smart host. Use an SMTP smart host in the following situations:

- The gateways are separated by a firewall that blocks SMTP transmissions.
- Either or both of the gateways are Unity Connection clusters.

When a gateway is a cluster, you must configure the opposite gateway to route to the cluster through a smart host in order for message traffic to reach the cluster subscriber server in the event that the publisher server is down, and configure the smart host to resolve the SMTP domain of the cluster to the IP addresses of both the publisher and subscriber servers. In this case, you should route traffic in both directions through the smart host.

Creating the Intersite Link

This section contains two procedures:

- If your Unity Connection site gateways route SMTP messages directly with each other, do the "Automatically Linking Two Unity Connection Site Gateways" .

Note When you automatically link two gateways, the settings that you select are configured for both gateways. After creating the link, you can change most settings on either gateway. Or, you can use the manual procedure to configure the settings differently on each gateway.

- If your Unity Connection site gateways require a smart host for routing SMTP messages (for example, because they are separated by a firewall, or because either or both gateways are clusters), do the Manually Linking Two Unity Connection Site Gateways.

Automatically Linking Two Unity Connection Site Gateways

Step 1 In Cisco Unity Connection Administration (on either server), expand **Networking**> **Links** > **and** select **Intersite Links**.

Step 2 On the Search Intersite Links page, select **Add**.

Step 3 On the New Intersite Link page, select Link to Cisco Unity Connection Site Using Automatic Configuration Exchange Between Servers.

Step 4 In the SMTP routing warning message window, select **OK**.

Step 5 In the Hostname field, enter the IP address or fully-qualified domain name (FQDN) of the remote Unity Connection site gateway to link to.

Step 6 In the Username field, enter the user name of an administrator at the location specified in the Hostname field. The administrator account must be assigned to a role that has the Manage Servers privilege. (The System Administrator and Technician roles have this privilege.)

Step 7 In the Password field, enter the password for the administrator specified in the Username field.

Step 8 For Transfer Protocol settings, decide whether you want to enable SSL to encrypt directory synchronization traffic between the sites.

Step 9 For Synchronization Settings, check the Include Distribution Lists When Synchronizing Directory Data check box to pull information about remote system distribution lists to the local site so that users can address messages to them. (Note that only the list name and other information used in addressing are replicated.)

Note When you enable system distribution list synchronization, you cannot disable it after the link is created except by removing and recreating the intersite link.

In order for local system distribution lists to be offered to the remote site for synchronization, they must also be marked to allow synchronization. By default, Unity Connection system distribution lists are marked to allow synchronization, although this setting may have been changed. The task list alerts you when and how to enable lists for synchronization.

Step 10 To convert recorded names from this site to a different encoding when synchronizing them with the remote site, check the **Convert Outgoing Recorded Names to** check box, and select the codec to use.

Note If you select a codec at this step, the same codec is configured on both gateways, which means that recorded names are sent in a format that differs from the recording format for at least one of the two gateways. If this is not your intention, do not change the setting now. You can change the setting later on the Edit Intersite Link page on either gateway.

Step 11 By default, two tasks that each run on their own schedule for data and recorded name directory synchronization from the remote site are enabled immediately after you create the intersite link. To disable either type of directory synchronization until you manually edit and enable the applicable synchronization task, uncheck the **Enable Task to Synchronize Directory Data After the Join** or **Enable Task to Synchronize Recorded Names After the Join** check boxes.

Step 12 Select **Link**.

Step 13 When prompted, select **OK** to confirm.

Manually Linking Two Unity Connection Site Gateways

Step 1 In Cisco Unity Connection Administration (on either site gateway), expand **Networking**> **Links** and select **Intersite Links**. This server is referred to as the first site gateway for the remainder of the procedure, and the other gateway is referred to as the second site gateway.

Step 2 On the Search Intersite Links page, select **Add**.

Step 3 On the New Intersite Link page, select **Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files**.

Step 4 Select **Download** and save the first site gateway configuration file to a location on your hard drive, or on media that you can use to copy the file to the second site gateway.

Step 5 Browse to Unity Connection Administration on the second site gateway.

Step 6 In Unity Connection Administration on the second site gateway, expand **Networking**, expand **Links**, then select **Intersite Links**.

Step 7 On the Search Intersite Links page, select **Add**.

Step 8 On the New Intersite Link page, select **Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files**.

Step 9 Select **Download**, and save the second site gateway configuration file to a location on your hard drive, or on media that you can use to copy the file to the second site gateway.

Step 10 In the Remote Site Configuration File field, select **Browse** and browse to the copy of the configuration file that you downloaded from the first site gateway in Step 4.

Step 11 For Transfer Protocol settings, decide whether you want to enable SSL to encrypt the data passed between the site gateways when the local reader service synchronizes with the remote gateway (local reader requests and remote feeder responses).

Step 12 For Synchronization Settings, check the Include Distribution Lists When Synchronizing Directory Data check box to pull information about remote system distribution lists to the local site so that users can address messages to them. (Note that only the list name and other information used in addressing are replicated.)

Note When you enable system distribution list synchronization, you cannot disable it after the link is created except by removing and recreating the intersite link.

In order for local system distribution lists to be offered to the remote site for synchronization, they must also be marked to allow synchronization. By default, Unity Connection system distribution lists are marked to allow synchronization, although this setting may have been changed. The task list alerts you when and how to enable lists for synchronization.

Step 13 To convert recorded names from this site to a different encoding when synchronizing them with the remote site, check the **Convert Outgoing Recorded Names to** check box, and select the codec to use.

Step 14 By default, two tasks that each run on their own schedule for data and recorded name directory synchronization from the remote site are enabled immediately after you create the intersite link. To disable either type of directory synchronization until you manually edit and enable the applicable synchronization task, uncheck the **Enable Task to Synchronize Directory Data After the Join** or **Enable Task to Synchronize Recorded Names After the Join** check boxes.

Step 15 For Intersite Routing, select the appropriate option:

- Route to this Remote Site Through—Enter the specific IP address or fully-qualified domain name of a smart host that can properly route messages sent to addresses at the SMTP domain of the remote site gateway.
- Route to this Remote Site Through SMTP Smart Host (If One Is Defined)—Routes outgoing messages to the host defined on the System Settings > SMTP Configuration > Smart Host page. If you select this option, the smart host must be defined, and must be able to properly route messages sent to addresses at the SMTP domain of the remote site gateway. If the smart host is not defined, a non-delivery receipt (NDR) is sent to the message sender.
- Route to this Remote Site Through the Remote Site Gateway—Routes outgoing messages directly to the remote site gateway SMTP server. Do not use this option if the remote gateway is a cluster, or if the gateways are separated by a firewall.

Step 16 Select **Link**.

Step 17 In Unity Connection Administration on the first site gateway, in the Select the Remote Configuration File to Upload field, select **Browse** and browse to your local copy of the configuration file that you downloaded from the second server in Step 9.

Step 18 Repeat Step 11 through Step 15 on the first site gateway.

Step 19 Select **Link**.

Checking the Status of Synchronization Between Unity Connection Sites and Configuring Task Schedules

When initial synchronization begins between site gateways, it can take a few minutes to a few hours for data to be fully replicated to each gateway, and from there to all locations in the site, depending on the size of your directory.

On each site gateway, there are two tasks which control the schedule on which the Reader polls the remote Feeder for directory data, and the schedule on which it polls for recorded names. By default, the tasks run every 15 minutes. If you unchecked the Enable Task to Synchronize Directory Data After the Join or Enable Task to Synchronize Recorded Names After the Join check boxes while linking the sites, you must configure the schedule and enable the task before synchronization can begin.

You can use the Edit Intersite Link page and the Task Schedule page in Cisco Unity Connection Administration to determine whether synchronization is progressing successfully or has completed. Do the following procedure to check synchronization status between sites, and to configure schedules for the two synchronization tasks.

Step 1 In Cisco Unity Connection Administration on a site gateway, expand **Networking** > **Links** and select **Intersite Links**.

Step 2 On the Search Intersite Links page, select the Display Name of the intersite link.

Step 3 On the Edit Intersite Link page, check the values of the following fields:

- Time of Last Synchronization—Indicates the time stamp of the last time the local reader service attempted to poll the remote site gateway feeder service for directory changes on the remote site, regardless of whether a response was received.
- Time of Last Error—Indicates the time stamp of the last time the local reader service encountered an error while attempting to poll the remote site gateway feeder service. If the value of this field is 0, or if the Time of Last Synchronization value is later than the Time of Last Error value, replication is likely to be progressing without problems.
- Object Count—Indicates the number of objects (users, system distribution lists if applicable, partitions, search spaces and Unity Connection locations) that the local site gateway has synchronized from the remote site.

Step 4 View the Remote Site Directory Synchronization Task, and enable it or change the schedule, if necessary:

a) From the Edit Intersite Link page, in the Related Links box in the upper right corner of the page, select **Remote Site Directory Synchronization Task** and select **Go**.
b) On the Task Schedule page, enable the task if it has not yet been enabled, and modify the schedule so that the task runs at the desired interval or time.
c) Select **Save**.
d) To view the task execution history, select **Edit > Task Definition Basics**. On this page you can determine whether the task has not started, is in progress, or has completed. If the task has completed you can select either the Time Started or Time Completed to view the detailed task results.

Step 5 From the Task Definition Basics page, select **Task Definition** > **Task Definitions** to go to the list of all tasks.

Step 6 View the Synchronize Voice Names With Remote Network task, and enable it or change the schedule, if necessary:

a) On the Task Definitions page, select **Synchronize Voice Names With Remote Network**.
b) Select **Edit > Task Schedules**.
c) On the Task Schedule page, enable the task if it has not yet been enabled, and modify the schedule so that the task runs at the desired interval or time.
d) Select **Save**.
e) To view the task execution history, select **Edit > Task Definition Basics**. On this page you can determine whether the task has not started, is in progress, or has completed. If the task has completed you can select either the Time Started or Time Completed to view the detailed task results.

Configuring Search Spaces Between Unity Connection Sites

When you initially set up a link between the sites, users who are homed on a location in one site are not able to address messages to users at locations in the other site, because the users are in separate partitions and use search spaces that do not contain the partitions of users on the locations in the other site. After initial replication completes between the sites, you can reconfigure your search spaces to include partitions that are homed on the remote site, and you can change the search scope of users, routing rules, call handlers, directory handlers, and VPIM locations to use a search space that is homed on a location in the remote site. (Note that while both partitions and search spaces are replicated between locations, you cannot assign users or other objects to a partition that is homed on another location.)

At a minimum, if you have not made any changes to the default partitions and search spaces on any server, at each location you can add the default partition of each remote site location to the search space that local users are using. For example, in an organization where site 1 contains ServerA, ServerB, and ServerC and site 2 contains Server D, with no changes to the system defaults, in Cisco Unity Connection Administration on ServerA, ServerB, and ServerC you would add the “ServerD Partition” default partition as a member of the “ServerA Search Space,” “ServerB Search Space,” and “ServerC Search Space” default search spaces,

respectively; in Unity Connection Administration on ServerD you would add “ServerA Partition, “ServerB Partition,” and “ServerC Partition” to “ServerD Search Space,” and so on.

For instructions on adding partitions to search spaces, see the “Dial Plan” section of the “Call Management” chapter of the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Configuring Individual System Distribution Lists for Synchronization

If you checked the Include Distribution Lists When Synchronizing Directory Data check box in Step 9 of the “Automatically Linking Two Unity Connection Site Gateways” or Step 12 of the "Manually Linking Two Unity Connection Site Gateways", information about system distribution lists created on the remote site can be pulled to the local site. However, in order for information about an individual list to be offered to another site, the Replicate to Remote Sites Over Intersite Links check box must be checked on the Edit Distribution List Basics page for a list. By default, Replicate to Remote Sites Over Intersite Links is checked, so individual Unity Connection system distribution lists are marked for synchronization by default. However, in order to allow contacts as members of a system distribution list, you must uncheck Replicate to Remote Sites Over Intersite Links, so if you have lists that have been configured to allow contacts as members, they are not offered for replication to the remote site.

To disable synchronization for an individual list, uncheck Replicate to Remote Sites Over Intersite Links check box. To enable synchronization for an individual list, remove any contacts that have been added as members and check the Replicate to Remote Sites Over Intersite Links check box. To enable or disable synchronization for multiple lists at once, you can use either Bulk Edit or the Bulk Administration Tool.

Creating an Organization-Wide All Voicemail Users Distribution List

If you would like to create a master distribution list that includes all users on all servers in both sites, do the following tasks:

1. On each location in each site, if you have not done so already, rename the All Voicemail Users list with a unique name (for example All Voicemail Users on <Server Name>). For instructions, see the “System Distribution Lists” chapter of the *System Administration Guide for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.
2. Select one location in the organization to host the master list. Create a new All Voicemail Users system distribution list on one location to use as the master list.
3. Add the lists from all locations in both sites as members of the master list.

Note In order to add lists from the remote site, the gateway of the site on which the master list is homed must have the Include Distribution Lists When Synchronizing Directory Data check box checked on the Edit Intersite Link page, and the lists from each location in the remote site must have the Replicate to Remote Sites Over Intersite Links check box checked on the Edit Distribution List Basics page.

4. Put all lists except the master list in partitions that do not belong to a search space that users use, so that they cannot address to any list except the master. For example, on each location, create a new partition called Hidden DLs on <Server Name> and put the list homed at that location in that partition. (By default, new partitions are not a member of any search space.)

Notable Behavior in Networked Unity Connection Servers

No Results Found When a Directory Handler Search Scope is Set to a Remote System Distribution List in Intersite Networking

If you set the Search Scope of a directory handler to System Distribution List and select a list that is homed on the remote site, no results are returned when callers reach the handler and attempt a search. This happens because list membership is not replicated across intersite links. (This behavior does not apply to voice-enabled directory handlers, which do not have the option to use a system distribution list as the search scope.)

Users Receiving Multiple Copies of Message Sent to Multiple Distribution Lists in Intersite Networking

When a message is sent to multiple distribution lists, under some circumstances, when the message traverses an intersite link, users who are members of more than one of the lists may receive multiple copies of the message.

Networked Broadcast Messages Not Supported

Broadcast messages cannot be sent to multiple locations within a site or between sites.

Networked Dispatch Messages Not Supported

Dispatch messaging is not supported across locations. Dispatch messages addressed to recipients at other locations within a site are delivered to remote users as regular messages. Dispatch messages addressed to remote site recipients are not delivered. You should configure dispatch messaging only when the message recipient is a system distribution list that does not include users on other networked locations.

Manual Resynchronization Runs Both Directory and Voice Name Synchronization Tasks

The Resync All button on the Search Intersite Links page starts the Synchronize Directory With Remote Network task. When that task completes, it automatically starts the Synchronize Voice Names With Remote Network task. These tasks normally run independently on separate schedules.

Replication with Unity Connection Clusters

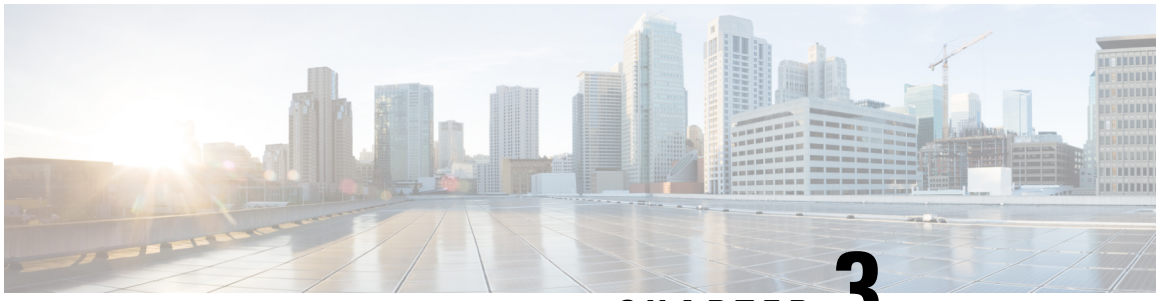
When you add a Cisco Unity Connection cluster to a site or link two sites, you create the intrasite or intersite link only on the publisher server of the pair. Directory updates made on a cluster subscriber server are replicated only from the cluster publisher server. If all locations in the site (and all intersite gateways, if applicable) are properly configured, voice messages continue to be sent to and from the cluster even when the subscriber server has Primary status or the publisher server is shut down. However, in order to keep the directory current on the publisher server, the publisher server should not remain shut down for an extended period of time.

Adding Remote Users as Private Distribution List Members

When creating private lists, users can add members from other locations if allowed by their search scope, in which case the same set of users who are reachable when addressing a message or placing a call can also be added as members of a private list. Private lists are not replicated to other locations; when a user addresses a message to a private list, the home location of the user expands the distribution list and addresses messages to each individual recipient on the list.

Consider notifying users in the event that the following members are inadvertently removed from their lists:

- When you delete a Unity Connection location, remote users at that location are removed from all private lists.
- When a VPIM contact becomes a Unity Connection user, the contact is removed from all private lists.



CHAPTER 3

Setting Up Networking Between Cisco Unity and Cisco Unity Connection

Setting Up an Intersite Link Between Cisco Unity and Unity Connection Gateways

This section describes the prerequisites for setting up an intersite link to connect a Cisco Unity server, failover pair, or Digital Network to a Unity Connection server, cluster, or site, and provides a high-level task list of all of the tasks that you need to complete for the setup in the order in which they should be completed. If you are unfamiliar with intersite link concepts, you should first read the "Overview of Networking Concepts" chapter and review the task list and procedures before beginning the setup.

Prerequisites for Linking Cisco Unity to a Digital Network

- At least one Cisco Unity release 12.x server is already installed and connected to the network as applicable for your installation. You can link a single Cisco Unity server or a single Cisco Unity Digital Network to Unity Connection.
- Your Cisco Unity and Microsoft Exchange environment must be meet the requirements listed in the "Cisco Unity Connection Networking Requirements" section of the *Networking Options Requirements*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.
- The Cisco Unity server that acts as the gateway to the Unity Connection site must be able to route directly to the Unity Connection site gateway via HTTP on port 80 or HTTPS on port 443.

Prerequisites for Linking Unity Connection to a Digital Network

- You can link a single Unity Connection 12.x server or cluster or a single Unity Connection site to a single Cisco Unity server, failover pair, or Digital Network. To link a Unity Connection site, all servers in the site must be running version 12.x.
- If you are linking a Unity Connection site, the site has been set up according to the "Setting Up a Unity Connection Site".
- The Unity Connection site must meet the requirements listed in the "Requirements for Intersite Networking" section in the *System Requirements for Cisco Unity Connection Release 12.x* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.
- You have access to an account that has the Manage Servers privilege on the Unity Connection server that serves as the gateway. (The System Administrator and Technician roles each have this privilege.)
- The Unity Connection server acts as the gateway to the Cisco Unity site must be able to route directly to the Cisco Unity site gateway via HTTP on port 80 or HTTPS on port 443.

Task List for Setting Up an Intersite Link Between Cisco Unity and Unity Connection Gateways

1. Make decisions about your network topology and gather information needed to configure the intersite link. See the Making Deployment Decisions and Gathering Important Information.
2. Determine the Cisco Unity domain name used for messaging with Unity Connection. See the Determining Cisco Unity Interoperability Domain Name.
3. Prepare the Cisco Unity gateway by configuring settings on the primary location page, checking permissions, and extending the Active Directory schema. See the Preparing Cisco Unity Gateway.
4. If you have previously installed the Interoperability Gateway for Microsoft Exchange, do the following to ensure that it is properly configured:
   - If the Interoperability Gateway is installed on Exchange 2010 or 2007, check the foreign connector configuration and configure a Send Connector and a Receive Connector. See the Configuring a Previously Installed Interoperability Gateway for Unity Connection Interoperability on Exchange 2010 or 2007.
5. If you have not previously installed the Interoperability Gateway for Microsoft Exchange, install and configure it. (If you are currently using or plan to use VPIM Networking or Trusted Internet locations on Cisco Unity, configure the Interoperability Gateway to handle these types of networking as well as Unity Connection interoperability.) 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), available at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs.html.
6. If you uninstalled the Cisco Unity Voice Connector in task 4. and you still require the Voice Connector to handle Bridge Networking and/or AMIS Networking, reinstall it with only those options configured. See the "Installing the Voice Connector" section of the applicable *Release Notes for Cisco Unity Voice*

Connector for Microsoft Exchange, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

7. Configure the Unity Connection gateway to accept SMTP connections from the Exchange server that delivers messages from Cisco Unity. See the Configuring SMTP Access on the Unity Connection Gateway.
8. Download the Cisco Unity gateway configuration file. See the Downloading Cisco Unity Gateway Configuration File.
9. On the Cisco Unity site gateway, set up a template to use when importing Unity Connection users into Cisco Unity. See the Setting Up a Template for Unity Connection Users on the Cisco Unity Gateway.
10. Begin linking the gateways by creating the intersite link in Cisco Unity Connection Administration on the Unity Connection gateway. See the Creating the Intersite Link on the Unity Connection Gateway.
11. Finish linking the gateways by creating the intersite link on the Cisco Unity gateway. See the Creating the Intersite Link on the Cisco Unity Gateway.
12. Configure partitions and search spaces so that Cisco Unity Connection users can address to Cisco Unity users and vice versa. See the Configuring Partitions and Search Spaces for Cisco Unity and Unity Connection Interoperability.
13. Optionally, if you select to synchronize system distribution lists in either or both directions between the gateways, configure individual distribution lists to allow or prevent replication. See the Configuring Individual System Distribution Lists for Synchronization.
14. Optionally, extend identified subscriber messaging on the Cisco Unity servers to include Unity Connection Networking subscribers. See the Extending Identified Messaging to Include Unity Connection Networking Subscribers .
15. Optionally, set up cross-server sign-in, transfers, and live reply. See the "Cross-Server Sign-In, Transfers, and Live Reply" chapter.

Making Deployment Decisions and Gathering Important Information

Before you begin setting up Cisco Unity-Unity Connection interoperability, be sure to plan for the following, and gather the applicable information:

- If you have configured VPIM on your Cisco Unity servers using the Cisco Unity Voice Connector and its associated transport event sink, you must migrate your VPIM configuration to use the Interoperability Gateway for Microsoft Exchange rather than the Voice Connector. The Interoperability Gateway and the Voice Connector transport event sink cannot coexist when Cisco Unity is configured for interoperability with Cisco Unity Connection. If you are installing the Interoperability Gateway for the first time, be sure to configure it for both VPIM and Cisco Unity Connection Networking. The task list tell you when to uninstall the Voice Connector. (If you still require the Voice Connector to handle Bridge Networking and/or AMIS Networking, you reinstall it to handle those options.)
- Select a single location on each site to act as a gateway to the other site. The gateways you select must have HTTP or HTTPS connectivity in order for directory synchronization to occur.
    - When selecting the Cisco Unity site gateway, if possible, select the server with the highest resources, lowest user count, and smallest amount of call activity. In particular, Platform Overlay 1 servers have CPU, memory, disk and MSDE/SQL Express limits that lower the ability of the server to handle synchronization overhead.

- When selecting the Cisco Unity location, consider that all locations from the Unity Connection site belongs to the same Dialing Domain as the Cisco Unity site gateway.

Determining Cisco Unity Interoperability Domain Name

In order for messages to be exchanged between Cisco Unity Connection and Cisco Unity, you need to decide on the domain name that Unity Connection uses when addressing messages to Cisco Unity users. The domain name uniquely identifies the messaging system. The domain name is configured as follows:

- On the SMTP Domain Name field on the Network > Primary Location page in the Cisco Unity Administrator on the Cisco Unity gateway.
- On the Interop Domain FQDN field in the Interoperability Gateway Administrator.

Additionally, based on the Interop Domain FQDN, the domain name is configured as follows:

- If you install the Interoperability Gateway on an Exchange 2010 or 2007 server:
  - As the SMTP AddressSpace domain on the Interoperability Gateway Foreign Connector. (This value is set automatically, based on the Interop Domain FQDN, when the Interoperability Gateway Foreign Connector is created or modified using the Interoperability Gateway Administrator.)
  - As the DomainName on the Interoperability Gateway Accepted Domain. (This value is set automatically, based on the Interop Domain FQDN, when the Interoperability Gateway Accepted Domain is created or modified using the Interoperability Gateway Administrator.)
- If you install the Interoperability Gateway on an Exchange 2003 server:
  - As the SMTP Address Space domain in the Interoperability Gateway SMTP Connector.
  - As the SMTP Email Address Policy on the Interoperability Gateway Recipient Policy.

If you have previously installed the Interoperability Gateway for Microsoft Exchange to handle VPIM or Trusted Internet subscribers on Cisco Unity, use the interoperability domain that was selected during that process, unless it matches the Cisco Unity Connection gateway SMTP domain.

If you have not previously installed the Interoperability Gateway to handle other networking features, the interoperability domain name can be whatever you would like it to be. As a best practice, however, you should use a name that follows the format <Name>.<DomainName>, where <Name> is a descriptive term and <DomainName> is the domain name of your organization, for example, interop.mydomain.com. Note however that the interoperability domain name that you select must meet the following requirements:

- It should not match any SMTP domain used in the Exchange organization to which Cisco Unity belongs for any purpose other than for routing messages through the Interoperability Gateway for Microsoft Exchange.
- It must not match the SMTP domain of the Unity Connection site gateway. (You can check the SMTP domain on the System Settings > SMTP Configuration > Server page in Cisco Unity Connection Administration on the Unity Connection gateway.)

Preparing Cisco Unity Gateway

Do the procedures in the following sections to prepare the Cisco Unity gateway:

Configuring Primary Location Profile Page on Cisco Unity Gateway

Step 1 In the Cisco Unity Administrator on the Cisco Unity gateway, go to the **Network** > **Primary Location** > **Profile** page.

Step 2 Enter a meaningful name for the location.

Step 3 If a Dial ID has not been entered, enter one. The Dial ID identifies this location to Cisco Unity and is required to save changes to the page.

Step 4 For the Dialing Domain name:

- If your installation consists of only one Cisco Unity server, create a dialing domain name.
- If your installation consists of multiple Cisco Unity servers networked via Digital Networking, and if this server is integrated with the same phone system as other networked Cisco Unity servers, you may have already added this server to a dialing domain. If not, enter the dialing domain name, or select it from the available list. The list contains names of dialing domain names already configured on at least one other Cisco Unity server in the network.

  Note that the dialing domain name is case sensitive and must be entered exactly the same on all of the servers. To ensure that all servers are correctly added to the same dialing domain, enter the dialing domain name on one Cisco Unity server and wait for the name to replicate to the other Cisco Unity servers. By doing so, you also confirm that replication is working correctly among the servers. The time that it takes for the primary location data from other Cisco Unity servers to be reflected on the local server depends on your network configuration and replication schedule.

Step 5 In the SMTP Domain Name field, enter the interoperability domain name that you previously select in the Determining Cisco Unity Interoperability Domain Name.

Step 6 Select the **Save** icon.

Checking Cisco Unity Permissions to Create Unity Connection Users

During Cisco Unity installation, when you run the Cisco Unity Permissions wizard to grant the necessary permissions to the installation and service accounts, if you did not check the Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM check box on the Choose Whether to Enable Voice Messaging Interoperability page, do the Setting Permissions to Create Cisco Unity Connection Users on Cisco Unity.

Tip If you do not know whether you checked the check box, run the Permissions wizard in report mode. For more information, see the Report Mode Help file, PWReportHelp_<language>.htm, in the directory in which the Permissions wizard is installed.

For more information on running the Permissions wizard, see the Permissions wizard Help file, PWHelp_<language>.htm, in the directory in which the Permissions wizard is installed.

Setting Permissions to Create Cisco Unity Connection Users on Cisco Unity

Step 1 Sign in to the gateway server using an account that:

- Is a member of the Domain Admins group in the domain that the Cisco Unity server belongs to, or that has permissions equivalent to the default permissions for the Domain Admins group.
- Is either an Exchange Full Administrator or a member of the Domain Admins group in the domain that contains all of the domains from which you want to import Cisco Unity subscribers.

Step 2 Re-run the Permissions wizard, and follow the on-screen prompts until the Choose Whether to Enable Voice Messaging Interoperability page appears.

Step 3 Check the **Set Permissions Required by AMIS, Cisco Unity Bridge, and VPIM** check box.

Step 4 Follow the on-screen prompts to complete the Permissions wizard.

Extending the Active Directory Schema

Before Cisco Unity is installed, the Active Directory schema is extended to store Cisco Unity-specific information. To support interoperability with Cisco Unity Connection, the schema must be further extended.

To see the schema changes that need to be made to support Cisco Unity Connection interoperability, browse to the directory Schema\LdifScripts on Cisco Unity Disc 1, and view the file vpimgateway.ldf. (The extensions needed for Cisco Unity Connection interoperability are the same as those needed for VPIM Networking.)

Do the following procedure only if you did not already modify the Active Directory schema to support VPIM Networking. You can verify whether the schema has already been modified by examining the log file that is generated each time the schema is updated. A shortcut to the directory where the log file is located is placed on the Windows desktop.

Extending the Active Directory Schema for Cisco Unity Connection Interoperability and VPIM Networking

Step 1 Confirm that all domain controllers are on line before making the schema updates. Schema replication occurs only when all domain controllers are on line.

Step 2 On the domain controller that is the schema master, sign in using an account that is a member of the Schema Administrators group.

Step 3 On Cisco Unity DVD 1 or CD 1, or from the location to which you saved the downloaded Cisco Unity CD 1 image files, browse to the directory **ADSchemaSetup**, and double-click **ADSchemaSetup.exe**.

Step 4 In the dialog box, double-click a row to select the language in which you view the ADSchemaSetup.

Step 5 Check the **Exchange VPIM and Connection Networking Connector** check box, uncheck the other check boxes, and then select **OK**.

Step 6 When the LDAP Data Interchange Format (LDIF) scripts have finished running, select **OK**.

Step 7 When the schema extension has finished, Ldif.log and LDif.err files are saved to the desktop. View the contents of the files to confirm that the extension completed successfully.

Step 8 Wait for the changes to the schema to replicate throughout the forest before adding information to the primary location and to delivery locations. Changes to the schema may take 15 minutes or more to replicate.

Configuring a Previously Installed Interoperability Gateway for Unity Connection Interoperability on Exchange 2010 or 2007

In order for messages to be exchanged between Cisco Unity and Cisco Unity Connection via the Interoperability Gateway for Microsoft Exchange, a valid Foreign Connector must be present on the Exchange 2010 or 2007 server to properly route messages through the Interoperability Gateway. In addition, the Exchange organization to which your Cisco Unity servers belong must be allowed to send mail to and receive mail from the SMTP bridgehead servers in the remote network. In the case where the remote network is a Cisco Unity Connection site, depending on your configuration, mail may be sent and received directly with the Unity Connection site gateway or with a smart host or other relay outside of the Exchange organization that handles SMTP connections on behalf of the Unity Connection gateway.

In this section, first do the below given procedure .

If you are already familiar with how to configure the Exchange organization to allow messages to be sent and received with the Cisco Unity Connection gateway, smart host, or relay, skip the remaining procedures and handle the message delivery configuration based on rules and practices established in your organization. Otherwise, do the remaining two procedures:

Procedures

Step 1 Open the Interoperability Gateway Administrator. (In the Windows Start Menu, browse to **Start** > **Programs** > **Cisco** > **IGE Admin**.)

If the Interoperability Gateway is installed on Exchange 2010, the Interoperability Gateway Administrator prompts you to enter account credentials. Use an account that has Full Exchange Administrator privileges.

Step 2 In the top pane of the Administrator, under **Address Spaces**, confirm whether the **UCI (Cisco Unity-Connection Interoperability)** check box is checked. If it is already checked, close the Interoperability Gateway Administrator and continue with the next task in the task list. If it is not checked, check it.

Step 3 In the tree control at left in the Interoperability Gateway Administrator, select **Foreign Connector**.

Step 4 If a Foreign Connector has not previously been created that covers the interoperability domain and the UCI feature address space that you checked in Configuring a Previously Installed Interoperability Gateway for Unity Connection Interoperability on Exchange 2010 or 2007, a warning message displays in red at the top of the Foreign Connector pane.

If you do not see this warning, and a valid Foreign Connector is displayed in the list box on the upper left side of the pane, close the Interoperability Gateway Administrator and continue with the next task in the task list.

If you do see the warning, you can modify the existing Foreign Connector that was created when the Interoperability Gateway for Microsoft Exchange was initially installed. To do so, do the following substeps:

a) In the list of Foreign Connectors that are homed on the server and contain at least one address space that pertains to Cisco Unity networking (at the upper left), select the existing Foreign Connector.
b) Select **Modify** below the list box.
c) On the Execute Shell Command screen, select **Run**.

Step 5 Close the Interoperability Gateway Administrator.

Configuring a Send Connector for a Remote Voice Messaging System (Exchange 2010 or 2007 Only)

Step 1 On the Exchange server on which the Interoperability Gateway is installed, open the Exchange Management Shell.

Step 2 In the left-hand pane, expand **Organization Configuration** and select **Hub Transport**.

Step 3 In the main Hub Transport pane, select the **Send Connectors** tab.

Step 4 In the Actions pane, under Hub Transport, select **New Send Connector**.

Step 5 In the New SMTP Send Connector wizard, on the Introduction page, enter a Name for the new connector.

Step 6 Under **Select the Intended Use for this Send Connector**, select **Custom**, then select **Next**.

Step 7 On the Address space page, select **Add**.

Step 8 For Address, enter the SMTP domain of the remote network, then select **OK**.

Step 9 Select **Next**.

Step 10 On the Network settings page, select **Route Mail through the Following Smart Hosts**.

Step 11 Select **Add**.

Step 12 For IP Address, enter the IP address of the Unity Connection gateway if messages are routed directly to the gateway, or of a smart host or other relay if one is configured to deliver messages from the Exchange organization to the Unity Connection gateway.

Step 13 Select **OK**.

Step 14 Select **Next** to continue to the next page.

Step 15 On the Configure Smart Host Authentication Settings Page, select the type of authentication to use when sending mail between the Exchange organization and the Unity Connection gateway.

Step 16 Select **Next** to continue to the next page.

Step 17 On the Source Server page, the local Exchange server should be listed by default. Select **Next** to continue.

Step 18 Confirm the settings on the New Connector page and select **New** to add the new connector.

Step 19 Select **Finish** to exit the wizard.

Step 20 On the Send Connectors tab, right-click the connector that you created and select **Properties**.

Step 21 Set the Protocol Logging Level to **Verbose**.

Step 22 Select **OK** to close the properties window.

Configuring a Receive Connector for a Remote Voice Messaging System (Exchange 2010 or 2007 Only)

Step 1 On the Exchange server on which the Interoperability Gateway is installed, open the Exchange Management Shell.

Step 2 In the left-hand pane, expand **Server Configuration** and select **Hub Transport**.

Step 3 In the upper Hub Transport pane, select the local Exchange server from the list of servers.

Step 4 In the lower pane, confirm that the title of the pane is the name of the local Exchange server, then select the **Receive Connectors** tab.

Step 5 In the Actions pane, under the local server name, select **New Receive Connector**.

Step 6 In the New SMTP Send Connector wizard, on the Introduction page, enter a name for the new connector.

Step 7 Under Select the Intended Use for this Send Connector, select **Custom**, then select **Next**.

Step 8 On the Local Network settings page enter the fully qualified domain name of the local server in the Specify the FQDN this Connector Provide in Response to HELO or EHLO: field.

Step 9 Select **Next** to continue to the next page.

Step 10 On the Remote Network settings page, in the list box, select **0.0.0.0-255.255.255.255**, then select **Edit**.

Step 11 If messages are received directly from the Unity Connection gateway, enter the IP address of the gateway as both the Start Address and End Address value. If a smart host or other relay external to the Exchange organization delivers messages on behalf of the Unity Connection gateway, enter the IP address of the smart host or relay as both the Start Address and End Address value.

Step 12 Select **OK**.

Step 13 Select **Next** to continue to the next page.

Step 14 Confirm the settings on the New Connector page, then select **New** to add the new connector.

Step 15 Select **Finish** to exit the wizard.

Step 16 On the Receive Connectors tab, right-click the connector that you created and select **Properties**.

Step 17 Set the Protocol Logging Level to **Verbose**.

Step 18 Select the **Permission Groups** tab.

Step 19 Check the **Anonymous Users** check box.

Step 20 Select **OK** to close the properties window.

Configuring SMTP Access on the Unity Connection Gateway

The Cisco Unity Connection SMTP server running on each system has an IP access list that controls which IP addresses are allowed to establish connections to it. Incoming SMTP connections are automatically accepted from some servers, such as the systemwide smart host that is defined on the System Settings > SMTP Configuration > Smart Host page, and any Unity Connection or Cisco Unity locations that are part of the same site or Cisco voicemail organization.

If messages from Cisco Unity users are delivered to the Unity Connection gateway by one or more servers that are not already defined either as the systemwide smart host or as a Cisco Unity location (this would be the case, for example, in a very simple configuration with a single Cisco Unity server that also hosts the Interoperability Gateway for Microsoft Exchange and the entire Exchange organization) or in the IP access list, do the following procedure to add the IP address of the delivery servers to the Unity Connection gateway IP access list.

Note If you are unsure whether adding the IP address of the delivery servers to the Unity Connection gateway IP access list is necessary, do the procedure. Explicitly adding the address of a server for which SMTP connections are automatically accepted does not negatively impact the SMTP server.

Do the following procedure to configure SMTP access on the Unity Connection gateway

Step 1 In Cisco Unity Connection Administration on the Cisco Unity Connection gateway, expand **System Settings** > **SMTP Configuration**, then select **Server**.

Step 2 On the Edit menu, select **Search IP Address Access List**.

Step 3 Select **Add New**.

Step 4 On the New Access IP Address page, enter the IP address of the server that delivers messages on behalf of the Cisco Unity site.

Step 5 Select **Save**.

Step 6 On the Access IP Address page, check the **Allow Unity Connection** check box.

Step 7 Select **Save**.

Step 8 Repeat Step 2 through Step 7 for each additional server that delivers messages on behalf of the Cisco Unity site.

Downloading Cisco Unity Gateway Configuration File

When linking Cisco Unity and Unity Connection gateways, you download the configuration file for each gateway and load it on the other gateway. Start by downloading the Cisco Unity configuration file to a location where you can access it from Cisco Unity Connection Administration on the Unity Connection gateway.

Do the following procedure:

Step 1 In the Cisco Unity Administrator on the Cisco Unity site gateway, browse to **Network** and select **Unity Connection Networking**.

Step 2 Select **Download** to download the local site configuration file.

Step 3 Save the file to a location on your hard drive, or on media that you can use to copy the file to the Cisco Unity gateway. Note that the file contains a public key certificate and should be treated as sensitive data.

Setting Up a Template for Unity Connection Users on the Cisco Unity Gateway

While creating an intersite link on the Cisco Unity gateway, you must select the template that the Cisco Unity gateway uses to create directory objects for Unity Connection users. You should review existing templates or create a new template specifically for Unity Connection users prior to creating the link.

The template that you select affects a number of important settings, such as:

- **Public distribution list membership**—Unity Connection users are added as list members in any Cisco Unity public distribution lists that are configured for the template.
- **Show Subscriber in Email Server Address Book**—Controls whether Unity Connection users are listed in the Outlook address book.
- **Class of Service**—Although most of the class of service settings do not affect the Unity Connection users directly, the Unity Connection users are considered members of the class of service and therefore can affect search results in cases where the class of service is used as the search scope of an object such as a directory handler.

You can review existing templates in the Cisco Unity Administrator by going to any Subscribers > Subscriber Template page and selecting the Find icon. To create a new template, do the following procedure.

Creating a New Template for Cisco Unity Connection Users on the Cisco Unity Gateway

Step 1 In the Cisco Unity Administrator, go to any **Subscribers** > **Subscriber Template** page.

Step 2 Select the **Add** icon.

Step 3 In the Add a Subscriber Template dialog box, enter a name.

Step 4 Select **New Template** or **Based on Existing Template**. If you select Based on Existing Template, select the applicable template in the Based On field.

Step 5 Select **Add**.

Step 6 On the Profile page, select a Class of Service and check or uncheck the **Show Subscriber in Email Server Address Book** check box, as applicable.

Step 7 Select the **Distribution Lists** page.

Step 8 On the Distribution Lists page, to assign all new users based on this template to a public distribution list, select the list in the Public Distribution Lists box, then select > .

To remove a distribution list from those to which new users are added, select the list, then select >>.

Step 9 Select the **Save** icon.

Creating the Intersite Link on the Unity Connection Gateway

Do the following procedure to create the intersite link on the Cisco Unity Connection gateway.

If the site gateway is a Unity Connection cluster, do the procedure only on the publisher server. The publisher server must be acting primary when you do the procedure.

Step 1 In Cisco Unity Connection Administration on the Cisco Unity Connection gateway, expand **Networking**, expand **Links**, then select **Intersite Links**.

Step 2 Select **Add**.

Step 3 On the New Intersite Link page, select **Link to Cisco Unity Site or Cisco Unity Connection Site by Manually Exchanging Configuration Files**.

Step 4 Select **Download** and save the Unity Connection site configuration file to a location on your hard drive, or on media that you can use to copy the file to the Cisco Unity gateway. Note that the file contains a public key certificate and should be treated as sensitive data.

Step 5 Select **Browse** and upload the Cisco Unity configuration file that you downloaded in the Downloading Cisco Unity Gateway Configuration File.

Step 6 For Transfer Protocol settings, decide whether you want to enable SSL to encrypt directory synchronization traffic between Cisco Unity and Cisco Unity Connection.

Caution To enable SSL, you must configure the Cisco Unity server to use SSL, which affects multiple applications that access the Cisco Unity server. See the applicable version of the *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Step 7 For Synchronization Settings, check the Include Distribution Lists When Synchronizing Directory Data check box to have system distribution lists that are created on the Cisco Unity site replicated to Unity Connection so that Unity Connection users can address messages to them. (Note that only the list name and other information used in addressing are replicated.)

Note In order for individual system distribution lists to be offered for synchronization by the Cisco Unity gateway, they must also be marked to allow synchronization. By default, individual Cisco Unity system distribution lists are not marked to allow synchronization. The task list alerts you when and how to enable individual lists for synchronization.

Step 8 To convert recorded names from this site to a different encoding when synchronizing them with the remote site, check the **Convert Outgoing Recorded Names To** check box, and select the codec to use.

Note Verify that the codec you select is the correct one for the Cisco Unity site gateway. If you need to change the recording format after creating the intersite link, you must clear all recorded names and then resynchronize all directory data and names using the Clear Recorded Names and Resync All buttons on the Networking > Intersite Links > Search Intersite Links page in Cisco Unity Connection Administration.This can have a heavy performance impact and should only be performed during non-business hours.

Do not select G711 a-law format when setting up an intersite link to a Cisco Unity site gateway.

Step 9 By default, two tasks that each run on their own schedule to pull directory data and recorded names from Cisco Unity to Unity Connection are enabled immediately after you create the intersite link. To disable either type of directory synchronization until you manually edit and enable the applicable synchronization task, uncheck the **Enable Task to Synchronize Directory Data After the Join** or **Enable Task to Synchronize Recorded Names After the Join** check boxes.

You should perform the initial synchronization outside of normal business hours to avoid peak traffic times. In particular, if your Cisco Unity site gateway is a Platform Overlay 1 server, the synchronization activity can cause noticeable delays in the user conversation.

Step 10 For Intersite Routing, select the appropriate option:

- **Route to this Remote Site Through**—Enter the specific IP address or fully-qualified domain name of a Microsoft Exchange server in your organization that can accept SMTP messages and route them to the Interoperability Gateway for Microsoft Exchange. The host must be able to accept SMTP messages sent from the Unity Connection gateway to addresses at the interoperability domain.
- **Route to this Remote Site Through SMTP Smart Host (If One Is Defined)**—Routes outgoing messages to the host that is defined on the System Settings > SMTP Configuration > Smart Host page. If you select this option, the smart host must be defined, and must be able to accept SMTP messages sent from the Unity Connection gateway to addresses at the interoperability domain. If the smart host is not defined, a non-delivery receipt (NDR) is sent to the message sender.
- **Route to this Remote Site Through the Remote Site Gateway**—Routes outgoing messages to the Cisco Unity gateway. Use this option only if Microsoft Exchange is installed on the Cisco Unity server and the server is able to accept SMTP messages sent from the Unity Connection gateway to addresses at the interoperability domain.

Step 11 Select **Link**.

Creating the Intersite Link on the Cisco Unity Gateway

Do the following procedure to create the intersite link on the Cisco Unity gateway.

If the site gateway is a failover pair, do the procedure only on the primary server. The primary server must be active when you do the procedure.

Caution When you do Step 12 in the following procedure, synchronization of Unity Connection objects to Cisco Unity begins automatically. You should do this step outside of normal business hours to avoid peak traffic times. In particular, if your Cisco Unity site gateway is a Platform Overlay 1 server, the synchronization activity can cause noticeable delays in the user conversation.

Step 1 In the Cisco Unity Administrator on the Cisco Unity site gateway, browse to **Network** and select **Unity Connection Networking**.

Step 2 On the Unity Connection Networking page, in the Remote Configuration File field, select **Browse** and upload the Unity Connection configuration file that you downloaded in Step 4 of the Creating the Intersite Link on the Unity Connection Gateway.

Step 3 Select **Add**.

Step 4 For Template, select the template that you selected or created in the Setting Up a Template for Unity Connection Users on the Cisco Unity Gateway. The template is used to create Cisco Unity directory objects for Unity Connection users so that Cisco Unity users can address messages to them. You must select a template before you can create the intersite link.

Step 5 Optionally, enter a Display Name Suffix. When the Cisco Unity site gateway creates directory objects for Unity Connection users and any replicated system distribution lists, this suffix is placed at the end of the display names of the objects. This can help Cisco Unity users locate the proper contact to use for addressing messages in Microsoft Outlook or other clients that access the directory, particularly if Unity Connection users already have Active Directory accounts prior to creating the intersite link.

Tip If you do not want to append a suffix to Unity Connection user and system distribution list objects, delete the default text in the Display Name Suffix field and leave the field blank.

Step 6 Check the Synchronize Distribution Lists check box to have system distribution lists that are created on the Unity Connection site replicated to Cisco Unity so that Cisco Unity users can address messages to them. (Note that only the list name and other information used in addressing are replicated.)

Note In order for individual system distribution lists to be offered for synchronization by the Unity Connection gateway, they must also be marked to allow synchronization. By default, individual Unity Connection system distribution lists are marked to allow synchronization, although this setting may have been changed. The task list alerts you when and how to enable individual lists for synchronization.

Step 7 Check the **Synchronize Voice Names** check box to have Cisco Unity synchronize voice names for Unity Connection users and system distribution lists.

Step 8 If you enabled SSL in Step 6 of the Creating the Intersite Link on the Unity Connection Gateway, check the **Use Secure Sockets Layer (SSL)** check box. If the Unity Connection site gateway is using a self-signed certificate (the default for Unity Connection), also check the **Use Self-Signed Certificates** check box.

Step 9 For Outbound Audio Conversion, if you want to convert voice names to a different format before sending them to the Unity Connection site gateway, select a codec in the Voice Names field.

Note Verify that the codec you select is the correct one for the Unity Connection site gateway. If you need to change the recording format after creating the intersite link, you must clear all recorded names and then resynchronize all directory data and names using the Clear Voice Names and Total Sync buttons on the Networking > Unity Connection Networking > Profile page in the Cisco Unity Administrator. This can have a heavy performance impact and should only be done during non-business hours.

Step 10 Review and continue entering settings, as applicable.

Step 11 When you have finished entering settings, select the **Save** icon.

Step 12 Select **Join**.

Configuring Partitions and Search Spaces for Cisco Unity and Unity Connection Interoperability

When you initially set up the intersite link between Unity Connection and Cisco Unity, Unity Connection users are not able to address messages to Cisco Unity users, because the Cisco Unity users are placed in newly-created partitions (based on their home Cisco Unity server) that are not a member of any Unity Connection search spaces.

After initial replication completes between the gateways and Cisco Unity objects are replicated throughout the Unity Connection site, you can reconfigure your search spaces to include the Cisco Unity partitions. (Note that you cannot assign Cisco Unity Connection users or other objects to a partition that was created for Cisco Unity users.)

In addition, for each Unity Connection location, you can specify the Local Partition That Cisco Unity Users Can Address To By Extension. Only extensions belonging to this partition are replicated to Cisco Unity. These extensions can be used for message addressing as well as auto-attendant dialing at the Cisco Unity site. Replicated extensions are added to the Dialing Domain of the Cisco Unity site gateway. Because extensions within a Dialing Domain must be unique, the collection of all partitions selected 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. Warnings appear in the Cisco Unity application event log indicating the owner of each omitted extension. After remedying any conflicts, you may need to do a manual resynchronization on the Cisco Unity site gateway (by selecting Total Sync on the Network > Connection Networking Profile page in Cisco Unity Administrator) in order to update the extensions.

It is possible for a Connection user to not have any extensions belonging to the Local Partition That Cisco Unity Users Can Address To By Extension configured on the server on which the user is homed. In this case, Cisco Unity users need to use dial-by-name for addressing messages to such Unity Connection users. Also, callers at the Cisco Unity site can only reach the user via dial-by-name Directory Handlers.

To configure the Local Partition That Cisco Unity Users Can Address To By Extension, do the following procedure on each Unity Connection server.

Note By default, for each Unity Connection location, the default <Server Name> Partition is used as the Local Partition That Cisco Unity Users Can Address To By Extension. Cisco Unity users cannot address messages by extension to any Unity Connection users who do not have an extension in this partition.

Do the following procedure to configure the partition that Cisco Unity users can address to for a Cisco Unity Connection location :

Step 1 In Cisco Unity Connection Administration (on any location), expand **Networking** > **and** select **Locations**.

Step 2 Expand **Local Site** and select the display name of the local location (the location on which you are accessing Unity Connection Administration).

Step 3 Under Local Partition That Cisco Unity Users Can Address To By Extension, for Partition, select the name of the partition to use.

Step 4 Select **Save**.

Step 5 Repeat Step 1 through Step 4 on each Unity Connection location in the site.

Configuring Individual System Distribution Lists for Synchronization

If you checked the Include Distribution Lists When Synchronizing Directory Data check box in Step 7 of the "Creating the Intersite Link on the Unity Connection Gateway", system distribution lists created on Cisco Unity can be replicated to Cisco Unity Connection so that Unity Connection users can address to them. However, by default, individual Cisco Unity system distribution lists are not marked for synchronization. To mark them, use the Public Distribution List Builder tool, located in the Cisco Unity Tools Depot. (The option to set or unset synchronization for lists is referred to as "Configuring distribution lists for Connection Networking.")

If you checked the Synchronize Distribution Lists check box in Step 6 of the "Creating the Intersite Link on the Cisco Unity Gateway", system distribution lists created on Unity Connection can be replicated to Cisco Unity. However, in order for information about an individual list to be offered to the Cisco Unity site, the Replicate to Remote Sites Over Intersite Links check box must be checked on the Edit Distribution List Basics page for a list. By default, Replicate to Remote Sites Over Intersite Links is checked, so individual Unity Connection system distribution lists are marked for synchronization by default. However, in order to allow contacts as members of a system distribution list, you must uncheck Replicate to Remote Sites Over Intersite Links, so if you have lists that have been configured to allow contacts as members, they are not offered for replication to the remote site.

To disable synchronization for an individual list, uncheck Replicate to Remote Sites Over Intersite Links. To enable synchronization for an individual list, remove any contacts that have been added as members and check the Replicate to Remote Sites Over Intersite Links check box. To enable or disable synchronization for multiple lists at once, you can use either Bulk Edit or the Bulk Administration Tool.

Extending Cisco Unity Identified Subscriber Messaging to Include UnityConnection Networking Subscribers

When a user on the Unity Connection site calls a Cisco Unity user and leaves a message, by default Cisco Unity do not identify the message as being from the Unity Connection user. For Cisco Unity to identify callers whose calling number matches the extension or alternate extension of a Unity Connection user, identified subscriber messaging (ISM) must be extended to networking contacts. (If you are also using other types of networking, such as VPIM, you may already have enabled ISM for networking contacts.)

Enabling ISM to include Unity Connection Networking subscribers and other networking contacts requires the following:

- The automated attendant search scope on each server must be set to the dialing domain. On each server, verify that the Set Auto Attendant Search Scope field is set to Dialing Domain on the Network > Primary Location > Profile page in Cisco Unity Administrator.
- Identified subscriber messaging must be enabled on each server. (ISM is enabled for "regular" subscribers by default.) On each server, verify that the Disable Identified Subscriber Messaging check box is unchecked on the System > Configuration > Settings page in Cisco Unity Administrator. (This setting is stored in the registry. If the system is using failover, verify the setting on both the primary and secondary servers.)

Extending Identified Messaging to Include Unity Connection Networking Subscribers

Step 1 On the Cisco Unity server desktop, double-click the Cisco Unity Tools Depot icon. (If the location is using failover, start the procedure on the primary server.)

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, click **Networking - Enable Identified Subscriber Messaging (ISM) for AMIS, Bridge, VPIM and Trusted Internet Subscribers**.

Step 4 In the New Value list, click **1**, then click **Set**.

Step 5 When prompted, click **OK**.

Step 6 Click **Exit**.

Step 7 Restart Cisco Unity for the registry setting to take effect.

Step 8 If the location is using failover, repeat Step 1 through Step 7 on the secondary server.

Step 9 Repeat Step 1 through Step 8 on each Cisco Unity location in the site.

Notable Behavior in Networking Cisco Unity and Unity Connection

This section provides information about notable expected behavior associated with Cisco Unity and Unity Connection networking.

Effects of Changing Cisco Unity Administrator Configuration Settings on the Interoperability Gateway for Microsoft Exchange

The Interoperability Gateway for Microsoft Exchange gets information about Cisco Unity networking locations by communicating with the web services resource on a server running Cisco Unity 10.x. For example, when evaluating an outgoing secure message, the Interoperability Gateway looks up the configuration for the destination to determine whether the message should be decrypted and sent or returned as undeliverable. In the Cisco Unity Administrator, you configure this and other location-specific settings on the Connection Networking profile for a Cisco Unity Connection site.

To understand how your topology dictates when changes to configuration settings made in the Cisco Unity Administrator takes effect in the Interoperability Gateway, and for information on how to expedite the process, see the "The Interoperability Gateway for Microsoft Exchange with Cisco Unity 8.x" section in the "Troubleshooting Networking in Cisco Unity 8.x" chapter of the *Troubleshooting Guide for Cisco Unity Release 8.x* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity/8x/troubleshooting/guide/8xcutsgx/8xcutsg060.html#wp1017196.

Unity Connection Users Not Listed in the Directory in Exchange 2010 or 2007 Organizations

When Cisco Unity is installed in an Active Directory forest that does not contain any servers running Exchange 2003 or earlier, public distribution lists and contact objects created by the Cisco Unity server do not have a

value written to the showInAddressBook attribute. As a result, those objects are not available in an address book that is accessed through a mail client, such as Microsoft Outlook. In a Cisco Unity Connection Networking deployment, this affects all users and distribution lists that are replicated from Unity Connection.

For instructions on how to update address lists to include Unity Connection objects, see the "Public Distribution Lists and Networking Subscribers Created by Cisco Unity Are Not Listed in the Directory" section in the applicable 12.x or later version of the *Release Notes for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Differences in User Experience Between Cisco Unity and Unity Connection

When you network Cisco Unity and Unity Connection, and particularly when you migrate users from Cisco Unity to Cisco Unity Connection, users may notice differences in behavior between the two products. Unity Connection turns on the message waiting indicator (MWI) for new receipts; Cisco Unity does not.

Display of Cisco Unity User Address Information

Unity Connection users who use applications such as Cisco Unity Connection ViewMail for IBM Lotus Notes, Cisco Unity Connection ViewMail for Microsoft Outlook, and Visual Voicemail may see system-generated SMTP addresses for Cisco Unity users. For example, when viewing a message received by a Cisco Unity user, the sender is identified by display name, and the system-generated address is displayed along with the display name.

Feature Support Limitations

The following features are not supported across intersite links between Cisco Unity and Unity Connection sites:

- License pooling
- Relay of messages to or from VPIM, AMIS, Bridge, or system contacts, including blind addressing to such contacts
- Broadcast messages
- Dispatch messages
- Message recall

Manual Resynchronization on the Unity Connection Site Gateway Runs Both Directory and Voice Name Synchronization Tasks

The Resync All button on the Search Intersite Links page in Cisco Unity Connection Administration starts the Synchronize Directory With Remote Network task. When that task completes, it automatically starts the Synchronize Voice Names With Remote Network task. These tasks normally run independently on separate schedules.

No Results Found When a Unity Connection Directory Handler Search Scope is Set to a Remote System Distribution List

If you set the Search Scope of a Unity Connection directory handler to system distribution List and select a list that is homed on the Cisco Unity site, no results are returned when callers reach the handler and attempt a search. This happens because list membership is not replicated across intersite links. (This behavior does not apply to voice-enabled directory handlers, which do not have the option to use a system distribution list as the search scope.)

Outbound SMTP Authentication

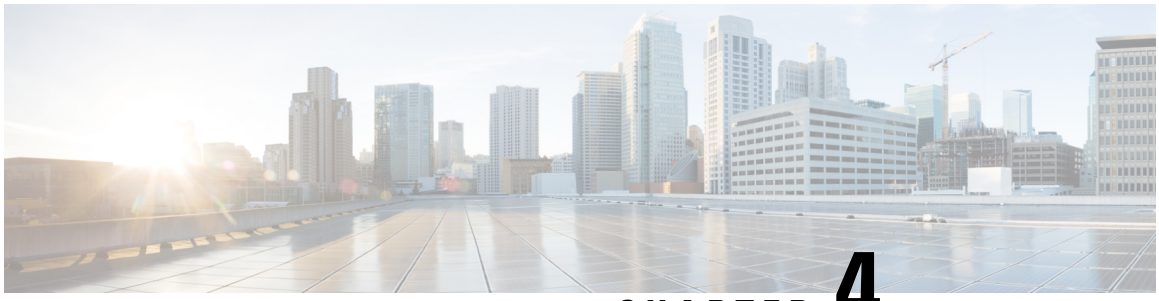
Unity Connection does not support outbound SMTP authentication. If the Exchange environment in use by Cisco Unity requires authentication, you must configure the Unity Connection site gateway to route messages.

Users May Receive Multiple Copies of a Message Sent to Multiple Distribution Lists

When a message is sent to multiple distribution lists, under some circumstances, when the message traverses an intersite link, users who are members of more than one of the lists may receive multiple copies of the message.

ViewMail for Microsoft Outlook and Body Text in Voice Messages

When Cisco Unity ViewMail for Microsoft Outlook users type text in the body of a voice message, the text is not received by Unity Connection users. Likewise, when Cisco Unity Connection ViewMail for Microsoft Outlook users type text in the body of a message, the text is not received by Cisco Unity users. However, recipients on the same type of system do receive the text (Cisco Unity users receive text sent by other Cisco Unity users, and Unity Connection users receive text sent by other Unity Connection users).



CHAPTER 4

VPIM Networking

Introduction

Cisco Unity Connection supports the Voice Profile for Internet Mail (VPIM), an industry standard protocol 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.

VPIM Networking can be used for messaging between Unity Connection 2.x and later servers, or between Unity Connection 2.x and later servers and other VPIM-compatible voice messaging systems such as Cisco Unity 4.0 and later.

Note Additional server discovery and directory synchronization functionality is available when you use Digital Networking rather than VPIM to connect multiple Unity Connection 2.x and later servers.

Setting Up VPIM Networking

This section describes the prerequisites for setting up VPIM Networking, and provides a task list containing a high-level view of all of the tasks you need to complete for the setup, and the order in which they should be completed. If you are unfamiliar with VPIM Networking, you should first read the VPIM Messages and then review the task list and procedures before beginning the setup.

Prerequisites

Before starting the setup, verify that the following prerequisites have been met:

- Cisco Unity Connection is already installed and connected to the network.
- The remote voice messaging system that Unity Connection is networked with is listed in the "Requirements for VPIM Networking" section of the applicable system requirements document: *System Requirements for Cisco Unity Connection Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.

Task List: Setting Up Cisco Unity Connection to Use VPIM Networking

Use the task list that follows to set up VPIM Networking in Cisco Unity Connection. The links take you to detailed procedures for the setup.

1. Make decisions about your numbering plan and gather information needed to configure VPIM Networking. See the Making Design Decisions and Gathering Needed Information.
2. Determine the domain name that is used for messaging between the remote voice messaging system and Unity Connection. See the Determining the Domain Name.
3. As applicable, configure DNS files. See the Resolving Names with IP Addresses.
4. Verify network and SMTP connectivity with the remote voice messaging system. See the Verifying Connectivity with the Remote Voice Messaging System.
5. Create the VPIM locations for each remote voice messaging system. See the Creating VPIM Locations.
6. Create VPIM contacts for each VPIM location. See the Creating VPIM Contacts.
7. Optionally, customize the contact creation settings for each VPIM location. See the Customizing VPIM Contact Directory Update Settings.
8. Optionally, add an alternate name for each VPIM location. See the Adding Alternate Names for Each VPIM Location.
9. Set up the remote voice messaging system for VPIM. Precisely how this is done depends on the voice messaging system. However, you need to provide the remote system with information about Unity Connection. See the Gathering Information to Configure Another Voice Messaging System for VPIM.
10. Test the setup to verify that Unity Connection can exchange messages with the remote voice messaging system.

Procedures for Setting Up Unity Connection to Use VPIM Networking

This section contains all of the procedures necessary to set up Unity Connection for VPIM Networking.

For detailed explanations of VPIM Networking concepts, see the VPIM Messages.

Making Design Decisions and Gathering Needed Information

Before you begin setting up Unity Connection for VPIM Networking, be sure to plan for the following, and gather the applicable information:

- Review your numbering plan strategy to determine whether you need to enter prefixes on the VPIM location and to determine which numbers to assign as Dial IDs for the VPIM locations. Following are requirements that must be considered:
  - Assign unique Dial IDs. Dial IDs should not be the same as other Dial IDs or extensions.
  - If you use variable-length Dial IDs, the first digits of each ID should be unique with respect to other Dial IDs.

    Follow the given policies:
  - Establish a fixed length for Dial IDs and, if possible, a fixed length for extensions.
  - Assign Dial IDs that have at least three digits.
  - Use a different number range for Dial IDs than for extensions. Do not use Dial IDs that conflict with extensions, such as 001 or 002.
- Review your partition and search space configuration to determine the partition and search scope you use for each VPIM location. For more information, see the "Dial Plan" section of the "Call Management" chapter of the System Administration Guide for Cisco Unity Connection *Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.
- Decide for each remote voice messaging system whether to allow Unity Connection to automatically create, modify, and delete VPIM contact records for users on that system, based on information received from incoming VPIM messages. Also decide how to map the source information to VPIM contact display names and extensions.
- Decide for each remote voice messaging system whether to allow Unity Connection users to blind address messages to recipients at the location.
- Make note of the following information about the remote voice messaging system: the mailbox range, the server name, the domain name, and the IP address.

Determining the Domain Name

VPIM messages are addressed in the format <Mailbox Number>@<Domain Name>. In order for messages to be exchanged between the remote voice messaging system and Unity Connection, you need to decide on the domain name that the remote voice messaging system uses when addressing messages to Unity Connection users. The domain name is configured as follows:

- On the remote voice messaging system, the domain name is configured on the location or node profile that corresponds to Unity Connection. (For additional information, see the documentation for the remote voice messaging system.)
- In the SMTP Domain field, on the System Settings > SMTP Configuration > SMTP Server Configuration page in Cisco Unity Connection Administration.

If the remote voice messaging system location or node profile that corresponds to Unity Connection has already been configured with a domain name, use that domain name in the procedures in this section.

Domain Name Requirements

The domain name uniquely identifies the voice messaging system. When choosing domain names used by Unity Connection and the remote voice messaging system, keep the following in mind:

- Unity Connection and the remote voice messaging system cannot use the same domain name. Each system must use a unique domain name.
- The complete domain name used by Unity Connection cannot be a subset of the domain name used by the remote voice messaging system. For example, if Unity Connection is using the domain name cisco.com, the remote voice messaging system cannot use names like london.cisco.com, paris-cisco.com, or romecisco.com. However, you could use europe.cisco.com for Unity Connection, and then use the names london.cisco.com, paris-cisco.com, and romecisco.com for the remote voice messaging systems.

Caution Choosing a domain name that does not meet these requirements result in message delivery failure.

Resolving Names with IP Addresses

VPIM messages are sent over the Internet or any TCP/IP network via SMTP. Therefore, a mechanism for name resolution is required for the remote voice messaging server. The supported method for name resolution is through a Domain Name System (DNS).

You need to know the fully qualified domain name (FQDN) and IP address of the remote voice messaging server. The FQDN is displayed on the System Settings > SMTP Configuration > Server page.

Add a host address resource (A) record and a mail exchange (MX) record in DNS for the remote voice messaging server, if they do not already exist.

For more information about adding A and MX records in DNS, see the documentation for the DNS server.

Verifying Connectivity with the Remote Voice Messaging System

Verify that the servers that handle outgoing and incoming SMTP messages have network connectivity and SMTPwith the remote voice messaging server, and vice versa.

For networking with another voice messaging server, you may need to install and configure an SMTP service or gateway on that server. See the documentation of the other voice messaging system for information on installing the SMTP service or gateway. Before proceeding, verify that the SMTP service or gateway has been installed on the other voice messaging server.

Do the following procedure to verify network connectivity with the remote voice messaging server:

Step 1 Using a computer on the same local network segment as the Unity Connection server, open a command prompt window.

Step 2 Enter **ping <IP address**, where <IP address> is the IP address of the remote voice messaging server, then press **Enter**.

If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with Step 3.

Step 3 Enter **ping <Domain name** where <Domain name> is the domain name that is used to address messages to the remote voice messaging server. The domain name in this step is the domain name that is entered for the VPIM location in Cisco Unity Connection Administration when setting up VPIM Networking.

Step 4 If you received a reply when pinging the IP address in Step 2, but no replies when pinging the domain name in Step 3, see the Resolving Names with IP Addresses. When the problem is resolved, continue with Step 5.

Step 5 Test network connectivity in the opposite direction. For systems other than Unity Connection, see the documentation for information on how to conduct the test, and continue with Step 6. Note that the remaining steps in this procedure may not exactly match the steps necessary for your system, so you may need to make adjustments.

Step 6 On the remote server, ping the IP address of the local server that handles incoming SMTP messages.

If you receive no reply, troubleshoot the network connectivity problem until the problem is resolved. Then continue with Step 7.

Step 7 On the remote server, ping the domain name, where the domain name is the one that is discussed in the Determining the Domain Name.

Step 8 If pinging by domain name fails, see the Resolving Names with IP Addresses.

Note Optionally, you can verify network connectivity using the “utils network ping” CLI command.

Verifying SMTP Connectivity with the Remote Voice Messaging Server

Step 1 Using a computer on the same local network segment as the Unity Connection server, open a command prompt window

Step 2 Enter telnet <servername> 25, where <servername> is the IP address or the FQDN of the SMTP server using TCP port 25.

Step 3 Press ENTER after each command.

Step 4 If remote messaging server is connected to SMTP, you receive 220 response with the FQDN of the server and the version of SMTP.

Step 5 If the telnet test was successful, enter quit to end the telnet session.

Creating VPIM Locations

Create a VPIM location on Unity Connection for each remote voice messaging system to which users send messages. If Unity Connection sends message with a large number of voice messaging systems, you may prefer to configure only a few VPIM locations at this time and proceed with the rest of the setup. After verifying that messaging works correctly between Unity Connection and the voice messaging systems for which VPIM locations have been configured, you can create the rest of the VPIM locations.

Do the following procedure to create VPIM locations:

Step 1 In Cisco Unity Connection Administration, expand **Networking** and select **VPIM**.

Step 2 On the Search VPIM Locations page, select **Add New**.

Step 3 On the New VPIM Location page, enter basic settings, as applicable. (For more information, see Help > **This Page**)

Note Fields marked with * (an asterisk) are required.

Step 4 Select **Save**.

Step 5 On the Edit VPIM Location page, continue entering applicable settings.

Step 6 When you have finished entering settings on the Edit VPIM Location page, select **Save**.

Customizing VPIM Locations

You can customize a VPIM location using Cisco Unity Connection Administration for each remote voice messaging system to which users send messages.

Do the following procedure to customize VPIM locations:

Step 1 In Cisco Unity Connection Administration, expand **Networking** and select **VPIM**.

Step 2 On the Search VPIM Locations page, select the display name for the VPIM location that you want to customize.

Step 3 On the Edit VPIM Location page, change settings, as applicable. (For more information, see Help> **This Page**).

Step 4 When you have finished changing settings on the Edit VPIM Location page, select **Save**.

Creating VPIM Contacts

Initially, you should create only a few VPIM contacts to verify that Unity Connection and the remote voice messaging system can successfully exchange messages. After you have confirmed that messaging between Unity Connection and the remote voice messaging system is working correctly, you can finish creating the VPIM contacts.

Note You must first create VPIM locations before creating VPIM contacts, and the VPIM contacts must be created on the same Unity Connection server on which you created the VPIM locations.

You can create VPIM contacts using the Bulk Administration Tool or using Cisco Unity Connection Administration. Using the Bulk Administration Tool to Create Multiple VPIM Contacts

The Bulk Administration Tool (BAT) allows you to create multiple VPIM contacts at the same time by importing contact data from a comma-separated value (CSV) file. CSV is a common text file format for moving data from one data store to another.

Use the following procedure to prepare your CSV file.

Preparing a CSV File for Creating VPIM Contacts

Step 1 Save the data that you use to create VPIM Contacts as a CSV file.

As a best practice, do not include more than 7,500 records in a single CSV file, as you may encounter unexpected results when the Bulk Administration Tool imports the data.

Step 2 Copy the CSV file to the applicable directory.

Step 3 Open the CSV file in a spreadsheet application or another application with which you can edit and reorganize the data. Do the following:

- Confirm that the data is separated by commas, and that no tabs, spaces, or semicolons separate the data in the file.
- If any data includes a space, quotation marks, or commas, contain the characters within quotation marks.

Step 4 Rearrange the data so that the columns are in the same order as the column headers that you add in Step 5. The order of the column headers does not matter, though it is good practice to set up your CSV file as indicated here. For example, the columns of data in this sample are sorted so that the alias of the contact is followed by the last name, the first name, the extension, the remote mailbox ID (RemoteMailAddress), and then by VPIM location (DeliveryLocationDisplayName):

aabade,Abade,Alex,2001,3000,Chicago VMS VPIM Location

kbader,Bader,Kelly,2002,3100,Chicago VMS VPIM Location

tcampbell,Campbell,Terry,2003,3200,Chicago VMS VPIM Location

lcho,Cho,Li,2004,3300,Chicago VMS VPIM Location

Note The only required column headers for creating contacts are Alias and Extension. However, in order to create VPIM contacts you must also include columns for the remote mailbox ID and the VPIM location.

Step 5 Enter the column headers above the first row of data. Column headers must be separated by commas, and spelled as indicated below:

Alias,LastName,FirstName,Extension,RemoteMailAddress,DeliveryLocationDisplayName

Step 6 If applicable, add optional column headers to the first row, and the corresponding data that you want to import in the subsequent rows below. As you do so, confirm the following:

- Column headers and data are separated by commas. Note that every row does not have to contain data for optional column headers.
- Any data that includes a space, quotation marks, or commas is contained within quotation marks.

Tip Include a column with the ListInDirectory header and a value of 1 for each contact if you would like users to be able to address messages to VPIM contacts the same way that they address messages to regular Unity Connection users—by extension or by spelling the name of the recipient. For a list of optional column headers, see the "Required and Optional CSV Fields in BAT" section of the "Bulk Administration Tool" appendix of the *System Administration Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Step 7 If your CSV file contains columns of data that you do not want to import, delete the columns. Alternatively, you can title one column NOTES. The BAT ignores data beneath any NOTES column header, but it does not support more than one NOTES column in a CSV file.

Step 8 Confirm that each row contains the appropriate data corresponding to each column header.

Step 9 Save the file as a CSV file.

Step 10 Continue with the following Creating VPIM Contacts Using the Bulk Administration Tool procedure.

Creating VPIM Contacts Using the Bulk Administration Tool

Step 1 In Cisco Unity Connection Administration, expand **Tools** and select **Bulk Administration Tool**.

Step 2 On the Bulk Administration Tool page, under Select Operation, select **Create**.

Step 3 Under Select Object Type, select **System Contacts**.

Step 4 Under Select File, select **Browse**.

Step 5 In the Choose File dialog box, browse to the directory where you saved the CSV file that you created in the Preparing a CSV File for Creating VPIM Contacts and select **Open**.

Step 6 In the Failed Objects File Name field, enter the path and the name of the file in which you want errors recorded.

Step 7 Select **Submit**.

Correcting CSV Errors

The failed objects file contains data that failed to create a VPIM contact. The Bulk Administration Tool reports the first error it detects in a row in a CSV file. When you have corrected that error, the BAT may detect additional errors in the same row when the data is imported again. Thus, you may need to repeat the correction process—running the BAT and correcting an error—several times to find and correct all errors.

The failed objects file contains all the records that failed to create a VPIM contact. You can save the file as a CSV file, and use it when you run the BAT again. Note that each time you run the BAT, the failed objects file is overwritten.

Do the following procedure to correct CSV errors:

Step 1 If the Bulk Administration Tool operation results in any failures, you can immediately inspect the failed objects report file by selecting **Download the Failed Objects File**.

Step 2 Open the file and correct all problems with the data, as indicated by the information in the FailureReason column for each record.

Step 3 Remove the FailureReason column or change the heading to **JUNK**.

Step 4 When you have finished modifying the data, save the file as a CSV file with a new name.

Step 5 Run the BAT again with the CSV file that you saved in Step 4 as the input file.

Note that each time that you run BAT, the failed objects file is overwritten (unless you specify a new name for the file each time you run the tool).

Step 6 Repeat this procedure until all VPIM contact accounts are created without error, and then proceed to the After Creating VPIM Contacts.

Using Cisco Unity Connection Administration to Create VPIM Contacts

You can create VPIM contacts one at a time using Cisco Unity Connection Administration.

Do the following procedure to create VPIM contacts:

Step 1 In Cisco Unity Connection Administration, expand **Contacts** and select **Contacts**.

Step 2 On the Search Contacts page, in the Contact menu, select **New Contact**. Alternatively, select Add New on the Search Contacts page to add a new contact.

Step 3 On the New Contact page, enter the following settings and select **Save**.

Table 5: Settings for the New Contact Page

Field	Setting
Alias	Enter the alias of the VPIM contact.
First Name	Enter the first name of the VPIM contact.

Field	Setting
Last Name	Enter the last name of the VPIM contact.
Display Name	Enter the display name of the VPIM contact.
Contact Template	Select the template on which to base the VPIM contact.

Step 4 On the Edit Contact Basics page, enter the following settings and select **Save**.

Table 6: Settings for the Edit Contact Basics Page

Field	Setting
Voice Name	Select **Play/Record** to record a name for the VPIM contact.
List in Directory	Check this check box to list the VPIM contact in the Unity Connection directory.
Partition	Select the partition to which the VPIM contact belongs. Partitions are grouped together into search spaces, which are used to define the scope of objects (for example, users and distribution lists) that a user or outside caller can reach while interacting with Unity Connection. A VPIM contact can belong to only one partition. A partition can belong to more than one search space.
Transfer Enabled	*(Optional)* Check this check box if you want Unity Connection to transfer incoming calls to a phone number that is associated with the VPIM contact instead of sending a message to the remote mailbox for the VPIM contact.
Transfer Extension or URI	*(Optional)* Enter the phone number or URI that the phone system uses to transfer calls to the VPIM contact, including any outdial access codes, if necessary. This field works together with the Transfer Enabled field.
Delivery Location	Select the VPIM location for the VPIM contact.
VPIM Remote Mailbox Number	Enter the mailbox number for the VPIM contact on the remote voice messaging system.
Local Extension	*(Optional)* For VPIM contacts, you can assign a local extension that fits into the Unity Connection extension numbering scheme. A local extension allows callers to address messages to the VPIM contact using an extension, rather than knowing the location ID and the remote mailbox number of the contact. In addition, if you set the Transfer Enabled and Transfer Extension fields, callers are able to identify and be transferred to the VPIM contact.

Field	Setting
Phone Numbers to Call Contact with Voice Commands	*(Optional)* Use the Dialed Work Phone, Dialed Home Phone, and Dialed Mobile Phone fields when you want voice recognition users to be able to call the VPIM contact by specifying a specific phone type for the contact. For dialed phone numbers, include any additional numbers necessary to dial outside calls (for example 9) and for long-distance dialing (for example, 1).
Phone Numbers or URIs to Identify Contact for Personal Call Transfer Rules	*(Optional)* Use the Work Phone, Home Phone, Mobile Phone, Other Number 1, and Other Number 2 fields to enter phone numbers or URIs that Unity Connection uses when matching the personal call transfer rules of a user against incoming phone calls from system contacts.

Step 5 Repeat Step 2 through Step 4 for all remaining VPIM contacts that you want to create.

After Creating VPIM Contacts

After creating VPIM contacts, consider the following:

- It takes a few minutes for the newly-created VPIM contact to be available to receive messages.
- You can make changes to settings for individual VPIM contacts in Cisco Unity Connection Administration.
- When you want to modify unique VPIM contact settings—such as the extension—for multiple contacts at once, you can rerun the Bulk Administration Tool.
- When a VPIM contact no longer needs a Unity Connection account, you can delete the VPIM contact. For details, see the Deleting VPIM Contacts.

Customizing VPIM Contact Directory Update Settings

In addition to manually creating, modifying, and deleting VPIM contacts, you can configure Unity Connection to automatically update records in the VPIM contact directory based on information that is contained in incoming VPIM messages. The settings that control whether the creation, modification, and deletion actions occur automatically, and how the incoming information is used to create or modify a record, can be individually configured for each VPIM location. By default, no automatic directory updates occur for any VPIM locations.

Depending on the Contact Creation settings that you select for each VPIM location, Unity Connection uses information from the header of an incoming VPIM message. If a VPIM message is received from a sender on a VPIM location that is configured to allow automatic VPIM contact creation, and no existing VPIM contact matches the information of the sender, a new VPIM contact record is created, provided that the VPIM message contains:

- A phone number
- A text name
- A domain name

- A recorded name (when required, based on the VPIM location configuration)

Additional Contact Creation settings allow you to specify how to map the parsed text name of the VPIM contact to a first name, last name, and display name, and how to map the phone number to an extension.

Note Changes to the Map VPIM Contact Extensions setting on the Contact Creation page for a VPIM location affect only VPIM contacts that are created after the setting is saved. VPIM contacts that already existed before the Map VPIM Contact Extensions setting is changed are not automatically updated. You must manually change the extension for each previously existing VPIM contact for that VPIM location.

If a VPIM message is received from a sender on a VPIM location that is configured to allow automatic VPIM contact modification, and an existing VPIM contact matches the sender information, the VPIM contact can be updated. You can select whether VPIM contact information is updated each time a message is received from a VPIM contact, or only when a message is received from a VPIM contact whose text name has changed since the directory entry was created. You can also decide whether or not to allow an update to the display name when a modification is made.

If a message from a Unity Connection user to a VPIM contact results in a non-delivery receipt (NDR), indicating that the message was undeliverable because the intended recipient does not exist (SMTP 5.1.1), and if the VPIM location is configured to allow automatic VPIM contact deletion, the VPIM contact is deleted.

You can update the VPIM location contact creation settings using Cisco Unity Connection Administration.

Before Configuring VPIM Contact Creation Settings

Before configuring the VPIM location contact creation settings, consider the following:

- If you have pre-populated VPIM contacts with specific display names that should not be changed, but want to allow automatic modification of other fields in the contact record, you can select to keep the Allow VPIM Contact Display Name Updates check box unchecked. In this case, the first name, last name, and spoken name of a contact may be modified during an automatic update. This may result in a mismatch if the spoken name is updated and the display name is not.
- When the Allow VPIM Contacts Without Recorded Voice Names check box is not checked, new VPIM contacts are not created for incoming messages that do not contain an Originator-Spoken-Name attachment. In addition, if automatic modification of VPIM contacts is enabled, and if the sender of an incoming message matches an existing VPIM contact, the VPIM contact is deleted if the attachment is not present in the message.
- When the Allow VPIM Contacts Without Recorded Voice Names check box is checked, and automatic modification of VPIM contacts is enabled, if the sender of an incoming message that does not include an Originator-Spoken-Name attachment matches an existing VPIM contact, the existing recorded name is deleted.
- If the phone number in an incoming message cannot be successfully mapped to an extension using the option selected for the Map VPIM Contact Extensions To field, a VPIM contact is not created for the sender.

Using Cisco Unity Connection Administration to Configure VPIM Contact Creation Settings

After you create a VPIM location, you can configure the settings that control automatic directory updates for that specific VPIM location using Cisco Unity Connection Administration.

Configuring VPIM Contact Creation Settings Using Cisco Unity Connection Administration

Step 1 In Cisco Unity Connection Administration, expand **Networking** and select **VPIM Locations**.

Step 2 On the Search VPIM Locations page, select the name of the VPIM location for which you want to configure contact creation settings.

Step 3 On the Edit VPIM Location page, in the Edit menu, select **Contact Creation**.

Step 4 On the Contact Creation page, check the **Automatically Create VPIM Contacts** check box to enable automatic creation of a VPIM contact record for this location when a VPIM message arrives and the sender does not already have a corresponding VPIM contact record.

Step 5 If you checked the Automatically Create VPIM Contacts check box in Step 4, in the Contact Template list, select the template on which to base the automatically created contacts.

Step 6 In the Automatically Modify VPIM Contact field, select one of the following to apply to VPIM contacts for this location:

- **No Automatic Update of Contacts**—The VPIM contact record is not updated with the sender information in a VPIM message when an incoming message has changed sender information.
- **Only When the Text Name Changes**—The VPIM contact record is updated only when the text name received in the VPIM message does not match the name of the VPIM contact.
- **With Each VPIM Message**—Every incoming VPIM message from a VPIM contact at this location results in an update to the corresponding VPIM contact record.

Step 7 Check the **Automatically Delete VPIM Contact** check box to enable automatic deletion of a VPIM contact for this location when a VPIM message is returned as undeliverable.

Step 8 Check the **Allow VPIM Contact Display Name Updates** check box to enable automatic updates to the VPIM contact display name when an incoming message from this location has a changed display name for the sender.

Step 9 Check the **Allow VPIM Contacts Without Recorded Voice Names** check box to enable automatic updates for this location to records for VPIM contacts that do not have a recorded name.

Step 10 In the Mapping Text Names field, select one of the following options to indicate how text names in incoming messages from this location are mapped to the display names for automatically created VPIM contact records:

- **Directly to VPIM Contact Display Names**—The display names for VPIM contacts match the corresponding text names.
- **Custom**—Enter the rule that defines how text names are mapped to display names for VPIM contacts. You can enter the tokens <FN>, <LN>, or <TN> (respectively first name, last name, or text name) in any combination, along with any additional text. Always precede <FN>, <LN>, or <TN> with a space, comma, or semicolon unless it appears at the beginning of the rule. In addition, always follow one of these tokens with a space, comma or semicolon unless it appears at the end of the rule. No additional characters are required at the beginning or end of a rule.

Step 11 In the Map VPIM Contact Extensions To field, select one of the following settings to indicate how the phone number on incoming messages from this location is mapped to the extension for automatically created VPIM contact records:

- **Phone Number**—Extensions are the same as the phone numbers that are parsed from incoming VPIM messages.
- **Phone Number - Remote Phone Prefix**—Extensions are formed by removing the remote phone prefix from the beginning of the phone numbers.
- **Location Dial ID + Phone Number**—Extensions are formed by adding the location Dial ID in front of the phone numbers.

- **Location Dial ID + Phone Number - Remote Phone Prefix**—Extensions are formed by removing the remote phone prefix from the beginning of the phone number, and adding the location Dial ID in front of the resulting number.

Step 12 Select **Save.**

Step 13 On the VPIM Location menu, select **Search VPIM Locations**.

Step 14 Repeat Step 2 through Step 13 for all remaining VPIM locations.

Adding Alternate Names for Each VPIM Location

When the Unity Connection system uses the voice-recognition option, you can also specify alternate names for the display name that you give a VPIM location. Users say the display name when they use voice commands to blind address to a mailbox number at a VPIM location (for example, to address to extension 55 at a VPIM location named Seattle, a user would say “five five at Seattle”) or to address a message to a VPIM contact name at a VPIM location (for example, “Robin Smith in Chicago”). Consider specifying alternate names if the VPIM location display name contains administrative information that users are not likely to know, or if it is not pronounced the way it would be read, as may be the case with acronyms and abbreviations. Also consider adding alternate names if users tend to refer to a location in multiple ways. For example, if users at one site refer to a location as “Seattle branch” and users at another site refer to the same location as “Seattle office,” you could add both “Seattle branch” and “Seattle office” as alternate names.

Do the following procedure to add an alternate name:

Step 1 In Cisco Unity Connection Administration, expand **Networking** and select **VPIM Locations**.

Step 2 On the Search VPIM Locations page, select the name of the VPIM location for which you want to add an alternate name.

Step 3 On the Edit VPIM Location page, in the Edit menu, select **Alternate Names**.

Step 4 On the Edit Alternate Names page, in the Display Name field, enter the alternate name you want for the VPIM location, then select **Add New**.

Step 5 On the VPIM Location menu, select **Search VPIM Locations**.

Step 6 Repeat Step 2 through Step 5 for all remaining VPIM locations for which you want to add alternate names.

Gathering Information to Configure Another Voice Messaging System for VPIM

Configuring another voice messaging system to exchange VPIM messages with Unity Connection may require the following information:

- The server name and domain name of the SMTP server that handles incoming SMTP messages.
- The Unity Connection phone prefix (if any) and Remote phone prefix (if any) entered on the corresponding VPIM location page.
- The mailbox number range for Unity Connection users.

Incoming VPIM messages must be routed to the SMTP server. When defining a location for Unity Connection on the remote voice messaging system, use the domain name that you entered for the SMTP server.

Unity Connection expects incoming VPIM messages to be formatted as follows:

<ConnectionPhonePrefix+ConnectionUserExtension@PrimaryLocationSMTPDomainName>

These specific properties are configured in Unity Connection, but similar information needs to be configured in the other voice messaging system.

Deleting VPIM Contacts

Step 1 In Cisco Unity Connection Administration, expand **Contacts** and select **Contacts**.

Step 2 On the Search Contacts page, check the check boxes next to the VPIM contacts that you want to delete.

Step 3 Select **Delete Selected**.

Step 4 When prompted to confirm the deletion, select **OK**.

Removing a VPIM Location

When you remove a VPIM location, you must remove (or reassign) any contacts and contact templates that use the location before deleting the VPIM location object. Use the following task list to remove a VPIM location.

1. Use the Bulk Administration Tool to export a list of all administrator-defined contacts. See the "Bulk Administration Tool"
2. Download the export file, and use a text editor to modify it to contain only the rows in which the DeliveryLocationDisplayName matches the display name of the VPIM location that you are removing. (If you plan to reassign the contacts to a different VPIM location, update the value in the DeliveryLocationDisplayName column.)
3. Use the Bulk Administration Tool to delete the list of contacts you generated in Task 2. Alternatively, to reassign the contacts to a different VPIM location, use the Update option.
4. In Cisco Unity Connection Administration, expand Templates and select Contact Templates. If a contact template is configured to use the VPIM location as the delivery location, change the delivery location, or delete the template. (You may need to select the display name of each template on the Search Contact Templates page to verify or change the delivery location.)
5. To delete the location, in Unity Connection Administration, expand Networking and select VPIM Locations. On the Search VPIM Locations page, check the check box next to the display name of the location that you want to delete, then select Delete Selected.

   For more information on Bulk Administration Tool, appendix of *System Administration Guide for Cisco Unity Connection, Release 12.x,* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Note If the Unity Connection is in HTTPS network, make sure to run the Network Remover task to completely remove the location from the network. The VPIM contacts get automatically deleted on deleting a VPIM location.

VPIM Messages

VPIM messages are made up of one or more MIME-encoded parts. The VPIM specification allows for optional MIME parts for spoken name and for forwarded and text messages. Unity Connection does not, however, support sending or receiving a vCard (an electronic business card that includes phone number, text name, and email address). If a vCard is attached to an outgoing or incoming message, Unity Connection removes the vCard data. In addition, any attachments to messages other than the voice message and embedded messages are removed from outgoing and incoming messages.

Unity Connection allows you to specify whether the recorded name of the sender is sent with outgoing messages. If incoming messages include a recorded name, it is played as part of the message. Unity Connection can also be configured to update the directory with information from the header from incoming messages.

Outgoing messages to a VPIM location do not include any recipients other than those at the VPIM location. Therefore, when a VPIM recipient replies to all addressees on a message, the reply go only to the sender and to any other recipients at the same VPIM location.

Figure 1 shows a sample VPIM message. Only a portion of the MIME encoding of the spoken name and voice message parts are shown because they are very long.

Figure 4: Sample VPIM Message

VPIM Addresses

A VPIM address is in the same format as a typical SMTP email address: localpart@hostpart. The right-hand side of the address is the domain name of the system on the TCP/IP network that handles messages. The left-hand side of the address is a unique identifier for the user. Typically, the left-hand side is the user mailbox number or the mailbox number with a prefix.

For example, an outgoing VPIM message to Terry Campbell with the remote mailbox ID 2233 could be addressed:

To: 2233@remotevoicemailsystem.com

If it is necessary to accommodate the numbering plan for your organization, the address can also contain a prefix:

To: 8882233@remotevoicemailsystem.com

VPIM addresses are created by Unity Connection when sending VPIM messages; they are not entered by users when addressing messages.

Message Addressing Options

Unity Connection provides the following ways to address messages to individuals on a remote voice messaging system:

- Unity Connection directory—When the List in Directory check box is checked for VPIM contacts, the Unity Connection directory has the names and extensions for the VPIM contacts. Users can address

messages to VPIM contacts the same way that they address messages to regular Unity Connection users—by extension or by spelling the name of the recipient. Note that spoken name confirmation is available when a recorded name exists for the VPIM contact; if the contact does not have a recorded name, Unity Connection uses Text to Speech to play the display name of the contact.

- Blind addressing—Blind addressing allows users to send messages to recipients at the VPIM location even if the recipients are not defined as contacts in the Unity Connection directory. If the Allow Blind Addressing check box is checked on the VPIM Location page, users can address messages to recipients at this location by entering a number that is made up of the VPIM location Dial ID and the mailbox number of the recipient, or by saying the digits of the mailbox number and the display name of the VPIM location (for example, “five five at Seattle office”).
- Distribution lists—Users can address messages to a private or system distribution list that includes VPIM contacts so that the VPIM contact receives the message.

Messaging Similarities and Limitations

For the most part, messaging between Unity Connection users and individuals on a remote voice messaging system is the same as messaging among Unity Connection users. For example:

- Messages marked urgent when they are sent are marked urgent when they are retrieved by the recipient.
- Messages marked private when they are sent are marked private when they are retrieved by the recipient.
- Users can send messages to Unity Connection distribution lists that include VPIM contacts.

Note the following exceptions:

- Requests for read receipts and delivery receipts are both returned as delivery receipts.
- In order for users on the remote voice messaging system to send messages to Unity Connection distribution lists, the Accept Messages From Foreign System check box must be checked on the Edit Distribution List Basics page in Unity Connection Administration. This check box is not checked by default.

Audio Format Considerations

The Audio Format Conversion settings for the VPIM location (on the Networking > Edit VPIM Location page in Cisco Unity Connection Administration) allow you to control the audio format of outgoing and incoming VPIM messages, as follows:

- Incoming Messages—You can set whether incoming VPIM messages are stored in the format in which they were sent, or converted to the audio format that Unity Connection uses for recording messages.
- Outbound Messages—You can set whether outbound VPIM messages are sent in the format in which they were recorded, or converted to the G.726 codec.

To make decisions about these settings, consider the following:

- The audio format that the local Unity Connection server uses for recording and playing voice messages.
- The audio format in which the remote voice messaging system can send and receive VPIM messages. Some voice messaging systems support only the G.726 format for VPIM messages, but you must consult the documentation of the remote voice messaging server to be sure.

- The network bandwidth.

The incoming VPIM messages be stored in the same audio format that the local Unity Connection server uses for recording and playing messages.

Multiple VPIM Bridgeheads

In an HTTPS network, you can designate multiple Unity Connection locations in the network as VPIM bridgeheads. The following are the ways to add multiple bridgeheads in an HTTPS network:

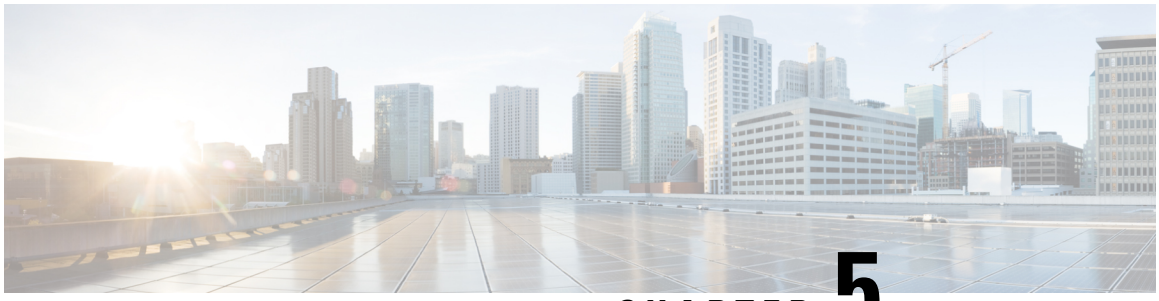
- You can add different VPIM servers on different VPIM bridgehead in an HTTPS network with unique dial id.
- You can add the same VPIM server on multiple VPIM bridgeheads with unique and not null remote phone prefix along with a unique dial id.
- You can add the same VPIM server to the same VPIM bridgehead multiple times with unique remote phone prefix. However, if a VPIM server is already added as VPIM bridgehead on Cisco Unity Connection with no remote phone prefix and you want to add the same VPIM server to same Unity Connection location or another Unity Connection location as VPIM bridgehead with some remote phone prefix (Non Null value) then you need to perform the following steps:

  Manually delete all the existing VPIM contacts that are created with no remote phone prefix.

  Change the remote phone prefix of already connected VPIM location.

  Add the same VPIM location as VPIM bridgehead with different remote phone prefix to another or the same Unity Connection location.

  Push the contacts from the VPIM server to the Unity Connection location.



CHAPTER 5

Making Changes to the Networking Configuration

Making Changes to the Networking Configuration

Removing a Location From a Unity Connection Site

When you remove a location from a Cisco Unity Connection site, it stops replicating directory information with other locations, and all objects that are homed on the server are removed from other locations. Likewise, all objects that are homed on other locations on the site are removed from the server you are removing.

You should consider the impacts of removing a location from the site prior to doing so, particularly if you plan to add the location back to the site later. Consider the following impacts:

- Users on the server are removed from distribution lists that are homed on other locations in the site, and users on other locations are removed from distribution lists that are homed on the server you remove. If you later add the server back into the site, you need to update distribution list membership on the re-added server to include any remote users, and update distribution list membership on all other locations in the site to include users on the re-added server.
- System call handlers and interview handlers on other locations that are configured to send messages to a user or distribution list that is homed on the server you remove are reconfigured to send messages to the undeliverable messages list of the location. Likewise, system call handlers and interview handlers on the server you remove that are configured to send messages to a user or distribution list that is homed on another location are reconfigured to send messages to the local undeliverable messages list. If you later add the server back into the site, you need to update the recipients for these handlers to use the correct remote object. (Even if you do not plan to add the server back into the site, you should make sure that someone is checking messages that are sent to the undeliverable messages list, or re-assign handlers that use it as a recipient.)
- Partitions that are homed on the server are removed from search spaces that are homed on other locations in the site, and partitions that are homed on other locations are removed from search spaces that are homed on the server you remove. If you later add the server back into the site, you need to review the partition membership of search spaces on the re-added server and on all other locations in the site. Depending on the version of Unity Connection on the server and the search space configuration, you may need to manually re-add remote partitions to each search space, or you may need to reorder the partitions within the search space to match the configuration that you had prior to removing the location.

- One location in the site retains a copy of search spaces that are homed on the server being removed, and the copy continues to be replicated amongst remaining locations in the site. Likewise, the server being removed makes a copy of remote search spaces that are homed on other locations. The copies replace the original search spaces on any objects that reference them. If you later add the server back into the site, Unity Connection automatically attempts to resolve the ownership of the search space copies to their original location and then deletes the copies. If you do not plan to add the server back into the site, you can reassign object references that use the search space copies to use other search spaces, and then delete the copies.
- One location in the site retains a copy of search spaces that are homed on the server being removed, and the copy continues to be replicated amongst remaining locations in the site. Likewise, the server being removed makes a copy of remote search spaces that are homed on other locations. The copies replace the original search spaces on any objects that reference them. If you later add the server back into the site, Unity Connection automatically attempts to resolve the ownership of the search space copies to their original location and then delete the copies. If you do not plan to add the server back into the site, you can reassign object references that use the search space copies to use other search spaces, and then delete the copies.
- On each location in the site, there are configuration settings specific to other locations (for example, the fields related to cross-server transfers and SMTP routing). When you remove a server from the site, the settings for all locations in the site are deleted from the server that you remove, and the settings for the server that you remove are deleted from all other locations in the site. If you later add the server back into the site, you need to update the settings for the re-added server on all other locations in the site, and configure the settings for all other locations on the re-added server.
- If the location is part of a Cisco Voicemail Organization, all of the impacts listed above also apply for those objects and object properties that are replicated to and from the remote site.

Do the following procedure to remove a location from the site. You can remove only one Unity Connection location from a site at a time.

Depending on the size of the directory, removing a Unity Connection location can take a few minutes to a few hours. Even though the operation may have completed on the local location, it may continue to be in progress on remote locations. You should wait for the removal operation to complete on all locations in the site before making additional changes to the site.

Removing a Location

Step 1 In Cisco Unity Connection Administration on any location in the site, expand **Networking> Links** and select **IntraSite Links.**

Step 2 Check the check box to the left of the **Display Name** of the location that you want to remove.

Step 3 Select **Remove Selected** and **OK** to confirm the removal.

Caution Until Unity Connection Administration returns a status message indicating that the removal is complete, avoid making other changes on the site (for example, removing another location, joining a new location to the site, creating an intersite link to another site, or initiating a directory push or pull).

Making Changes to a Unity Connection Site Gateway

The following changes are not supported on a Unity Connection site gateway unless you unlink the gateway from the remote site, remove the gateway from the local site, make the change, add the gateway back to the local site, and relink the sites:

- Replacing the site gateway server or hard disks.
- Changing the IP address of the site gateway.
- Renaming the site gateway.

To make any of these changes, do the following tasks:

1. Remove the intersite link. Depending on the type of site the gateway is linked to, see either the Removing Intersite Link Between Two Unity Connection Sites or the Removing an Intersite Link Between a Unity Connection Site and a Cisco Unity Site
2. If there are other locations in the Unity Connection site, remove the site gateway from the site. See the Removing a Location From a Unity Connection Site
3. Make the change on the site gateway server.
4. If there are other locations in the Unity Connection site, add the Unity Connection site gateway back into the site. See the Setting Up a Unity Connection Site
5. Relink the sites. Depending on the type of site the gateway was linked to, see either the Linking Two Unity Connection Sites or the Setting Up an Intersite Link Between Cisco Unity and Unity Connection Gateways

Making Changes to a Cisco Unity Site Gateway

The following changes are not supported on a Cisco Unity site gateway unless you unlink the gateway from the Unity Connection site, make the change, and relink the sites:

- Renaming the site gateway or moving it to another domain.
- Changing the IP address of the site gateway.
- Replacing the site gateway server or upgrading it to Windows 2003.
- Converting the primary or secondary server in a failover pair to a server without failover.

To make these changes, first follow the steps in the Removing an Intersite Link Between a Unity Connection Site and a Cisco Unity Site Then, relink the sites according to the instructions in the Setting Up an Intersite Link Between Cisco Unity and Unity Connection Gateways

Removing an Intersite Link Between a Unity Connection Site and a Cisco Unity Site

The process of removing an intersite link between a Unity Connection site and a Cisco Unity site involves the following general steps:

- On the Cisco Unity site gateway, unjoin the link. This stops synchronization with the Unity Connection site and removes all Unity Connection objects from the Cisco Unity directory.

- On the Cisco Unity site gateway, remove the intersite link. This removes all configuration information about the Unity Connection site gateway from the Cisco Unity site gateway.
- On the Unity Connection site gateway, remove the intersite link. This stops synchronization with the Cisco Unity site, removes all Cisco Unity objects from the Unity Connection directory, and removes all configuration information about the Cisco Unity site gateway from the Unity Connection site gateway.

  On the Cisco Unity site gateway, the deletion of remote site objects begins as soon as you unjoin the link. On the Unity Connection site gateway, the deletion of objects begins when the **Remove Objects Associated With Deleted Remote Sites** task runs (by default, the operation runs at 10:00 p.m. daily).

  You should consider the impacts of removing an intersite link prior to doing so, particularly if you plan to relink the sites later. Consider the following impacts:

- Users and system distribution lists on each site are removed from distribution lists that are homed on the other site. If you later relink the sites, you need to update distribution list membership to include any remote users and distribution lists.
- System call handlers and interview handlers that are configured to send messages to a remote site user or distribution list are reconfigured according to the user deletion rules of the server. (Cisco Unity locations do the replacement based on the Substitute Objects configuration on the System > Configuration > Settings page in the Cisco Unity Administrator. Unity Connection locations replace the object with the local undeliverable messages list.) If you later relink the sites, you need to update the recipients for these handlers to use the correct remote object. (Even if you do not plan to relink the sites, you should make sure that someone is checking messages that are sent to a Unity Connection undeliverable messages list, or reassign handlers that use it as a recipient.)
- Partitions that were created for Cisco Unity locations are removed from search spaces in the Unity Connection site. If you later relink the sites, you need to review the partition membership of the search spaces that are owned on each Unity Connection location. Depending on the version of Unity Connection on the server and the search space configuration, you may need to manually re-add the Cisco Unity partitions to each search space, or you may need to reorder the partitions within the search space to match the configuration that you had prior to removing the intersite link.
- On each location in the site, there are cross-server configuration settings specific to other locations. When you unlink the sites, these settings are removed. If you later relink the sites, you need to reconfigure all location-specific settings in both sites.
- All intersite messaging, addressing between sites, and intersite auto-attendant features are unavailable after the link is removed.

Do the following procedure to remove an intersite link between a Unity Connection 1.x site and a Cisco Unity site. If you have a Cisco Unity failover pair, do the steps applicable to Cisco Unity only on the primary server. If you have a Unity Connection cluster, do the steps applicable to Unity Connection only on the publisher server.

Caution Because server performance can be impacted by large deletion activities, you should remove the intersite link on the Cisco Unity site gateway (Step 2 in the procedure) during non-business hours, and allow the Remove Objects Associated With Deleted Remote Sites task to run on the default schedule (or at another time during non-business hours) on the Unity Connection site gateway.

Steps to Remove an Intersite Link

Step 1 On the Cisco Unity site gateway, unjoin the link. This stops synchronization with the Unity Connection site and removes all Unity Connection objects from the Cisco Unity directory.

a) In the Cisco Unity Administrator, select **Network** and select **Connection Networking**.
b) On the Unity Connection Networking Profile page, in the **Link** section, select **Unjoin**.
c) At the unjoin warning, select **OK**.
d) Select **OK** to continue.

Step 2 On the Cisco Unity site gateway, remove the intersite link. This removes all configuration information about the Unity Connection site gateway from the Cisco Unity site gateway.

a) On the Unity Connection Networking Profile page, check the **Delete** check box next to the name of the remote site gateway.

Tip If the Delete check box is not available, wait for a minute and refresh the page.

b) Select the **Save** icon.

Step 3 On the Cisco Unity Connection site gateway, remove the intersite link. This stops synchronization with the Cisco Unity site, removes all Cisco Unity objects from the Unity Connection directory, and removes all configuration information about the Cisco Unity site gateway from the Unity Connection site gateway.

a) In Cisco Unity Connection Administration, expand **Networking**> **Links** and select **Intersite Links**.
b) On the Search Intersite Links page, check the check box next to the intersite link corresponding to the Cisco Unity site.
c) Select **Remove Selected**.
d) At the warning about deleting associated objects, select **OK**.

Step 4 Optionally, on the Unity Connection site gateway, review the schedule for the **Remove Objects Associated With Deleted Remote Sites** task. By default, to avoid affecting system performance during business hours, this task runs at once a day at 10:00 p.m., and the intersite link is not fully removed until the task has run.

To review the schedule, either select the link to the task that is displayed in the Status message on the Search Intersite Links page after you have removed the selected intersite link, or expand **Tools** and select **Task Management**; on the Task Definitions page, select **Remove Objects Associated With Deleted Remote Sites**.

Step 5 Do the following procedures to verify that the link has been removed on both site gateways:

- Verifying an Intersite Link is Removed from a Cisco Unity Site Gateway
- Verifying an Intersite Link is Removed from a Unity Connection Site Gateway

Verifying an Intersite Link is Removed from a Cisco Unity Site Gateway

Step 1 In the Cisco Unity Administrator, select **Network** > **Connection Networking**

Step 2 On the Unity Connection Networking Profile page, if the link has not yet been removed, it is displayed in the table at the top of the page. If the link has been removed, no entry is displayed in the table.

Verifying an Intersite Link is Removed from a Unity Connection Site Gateway

Step 1 In Cisco Unity Connection Administration on the Unity Connection site gateway, expand **Networking**, expand **Links**, and select **Intersite Links**.

Step 2 On the Search Intersite Links page, if the link has not yet been removed, it is displayed in the **Intersite Links** table with (Link Removal Pending) listed after the **Display Name**. If the **Remove Objects Associated With Deleted Remote Sites** task has run and the link has been removed, no entry is displayed in the Intersite Links table.

Removing Intersite Link Between Two Unity Connection Sites

When you remove an intersite link between two Unity Connection sites, each site gateway stops synchronizing directory information with the other site, removes all objects that are homed on the remote site, and removes all configuration information about the remote site gateway.

You should consider the impacts of removing an intersite link prior to doing so, particularly if you plan to relink the sites later. Consider the following impacts:

- Users and system distribution lists on each site are removed from distribution lists that are homed on the other site. If you later relink the sites, you need to update distribution list membership to include any remote users and distribution lists.
- System call handlers and interview handlers that are configured to send messages to a remote site user or distribution list are reconfigured to send messages to the undeliverable messages list of the location on which the handler is configured. If you later relink the sites, you need to update the recipients for these handlers to use the correct remote object. (Even if you do not plan to relink the sites, you should make sure that someone is checking messages that are sent to the Unity Connection undeliverable messages list, or reassign handlers that use it as a recipient.)
- Partitions that were created for remote site locations are removed from search spaces in each Unity Connection site. If you later relink the sites, you need to review the partition membership of the search spaces that are owned on each location in each site. Depending on the version of Unity Connection on the server and the search space configuration, you may need to manually re-add remote partitions to each search space, or you may need to reorder the partitions within the search space to match the configuration that you had prior to removing the intersite link.
- On each location in the site, there are cross-server configuration settings specific to other locations. When you unlink the sites, these settings are removed. If you later relink the sites, you need to reconfigure all location-specific settings in both sites.
- All intersite messaging, addressing between sites, and intersite auto-attendant features are unavailable after the link is removed.

Do the following procedure to remove an intersite link between two Unity Connection 12.x sites. If either of the gateways is a Unity Connection cluster, do the steps for that gateway only on the publisher server.

Steps to Remove an Intersite Link Between Two Unity Connection Sites

Step 1 On either site gateway, remove the intersite link. This stops synchronization with the remote site and removes all remote site objects from the local site directory.

a) In Cisco Unity Connection Administration, expand **Networking**> **Links** and select **Intersite Links**.
b) On the Search Intersite Links page, check the check box next to the intersite link corresponding to the remote site.
c) Select **Remove Selected**.
d) At the warning about deleting associated objects, select **OK**.

Step 2 Optionally, review the schedule for the **Remove Objects Associated With Deleted Remote Sites** task. By default, to avoid affecting system performance during business hours, this task runs at once a day at 10:00 p.m., and the intersite link is not fully removed until the task has run.

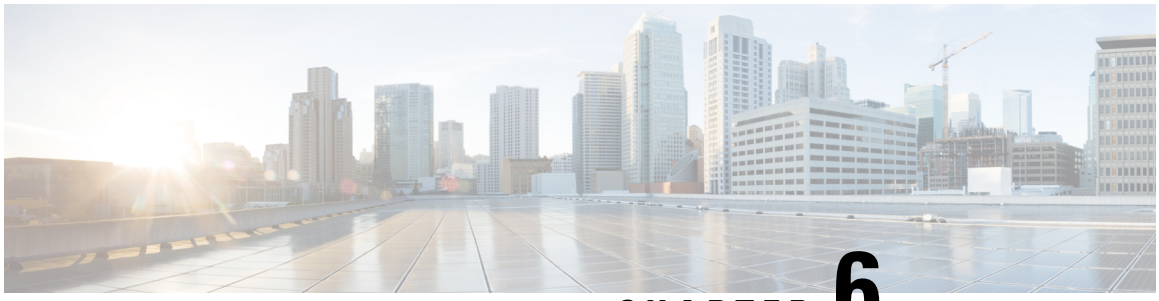
To review the schedule, either select the link to the task that is displayed in the Status message on the Search Intersite Links page after you have removed the selected intersite link, or expand **Tools** and select **Task Management**; on the Task Definitions page, select **Remove Objects Associated With Deleted Remote Sites**.

Caution Because server performance can be impacted by large deletion activities, you should allow the **Remove Objects Associated With Deleted Remote Sites** task to run on the default schedule (or at another time during non-business hours).

Step 3 To verify that the link has been removed, expand **Networking**> **Links** and select **Intersite Links**.

On the Search Intersite Links page, if the link has not yet been removed, it is displayed in the **Intersite Links** table with (Link Removal Pending) listed after the **Display Name**. If the **Remove Objects Associated With Deleted Remote Sites** task has run and the link has been removed, no entry is displayed in the I**ntersite Links** table.

Step 4 Repeat Step 1 through Step 3on the other site gateway.



CHAPTER 6

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

Introduction

This chapter describes the cross-server sign-in, transfer, and live reply features available between Cisco Unity Connection locations in a site, between Unity Connection locations in different sites linked by an intersite link, and between Cisco Unity and Unity Connection locations in sites linked by an intersite link. The chapter also covers the procedure to configure the cross-server feature.

Overview of Cross-Server Sign-In, Transfer, 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 networked locations. For this reason, only the home location of the user has information about call transfer settings, greetings, and other specific details for the user. In order for the location to properly handle calls destined for a user on a different location, it must hand off the call to the home location of the user. The purpose of the cross-server feature is to make the user experience in a networked environment almost the same as in a single server environment, as shown in Table 7: Cross-Server Features.

Table 7: 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 call the same number, regardless of which is the home server, and are transferred to the applicable home server to sign in.

Feature	Description
Cross-server transfer	Cross-server transfer enables calls from the automated attendant or from a directory handler of one location to be transferred to a user on another location, 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 location by transferring to the user (according to the call transfer and screening settings of the called user).

Although the cross-server features are distinct features, they all use the same underlying functionality—an enhanced supervised call transfer:

1. The location on which a sign-in, transfer, or live reply originates puts the caller on hold and calls the receiving location by dialing a phone number designated as the cross-server dial string for the receiving location.
2. When the receiving location answers, the originating location sends a sequence of DTMF tones that identify the call as a handoff request.
3. The receiving location responds with a sequence of DTMF tones, and the originating location hands off the call to the receiving location for processing.

At this point the functionality is the same as if the call had originated on the receiving location.

In this chapter, an originating location is defined as a server (or cluster) that calls other locations. A receiving location is defined as a server (or cluster) that answers a cross-server call.

Cross-server dial strings are not synchronized between locations. Each originating location can be configured with a dial string for each receiving location. Note that if an originating location is configured for multiple phone system integrations, you must select a dial string that all phone system integrations can use to reach the receiving location.

Search Space Considerations for Cross-Server Sign-In, Transfers, and Live Reply

When a user dials the pilot number of a Unity Connection location that is not his or her home server, the answering location processes the call according to its call management plan. A search space is assigned to the call by the first call routing rule that the call matches. At each subsequent processing step, the search scope of the call may change. Unity Connection uses the search space that is assigned to the call at the point that the call reaches the Attempt Sign-In conversation to identify which user is trying to sign in. If a user calls from an extension that is in a partition that is not a member of this search space, 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 in which they appear in the search space. Check the direct routing rules on each Unity Connection location that handles incoming sign-in calls from remote users to determine the search space that is set by the rule or other call management object that sends calls to the Attempt Sign-In

conversation. If the partitions that contain remote users are not a part of this search space, cross-server sign-in does not work, even if it is enabled.

Also note that for cross-server calls from one Unity Connection location to another Unity Connection location (either in the same site or in a remote site), a mismatch between the search space that is applied to the call on the originating location and the search space that is applied on the receiving location can cause problems for cross-server sign-ins and cross-server transfers. A match could be made on the search scope on the originating location that cannot be made on a different search scope on the receiving location. For this reason, you should verify that the same search scope is configured on both originating and receiving locations. For example, call routing rules can be used to direct cross-server calls on the receiving location to the appropriate search space based on the cross-server dial string that is used to reach that location.

For cross-server live reply, as with any live reply attempt, a Unity Connection user can only call the sender if the sender is in a partition that is a member of the search space configured for the user.

Cross-Server Sign-In

The cross-server sign-in feature enables users who are calling from outside the organization to call the same number regardless of which server they are homed on, and they are transferred to the applicable home server to sign in. If you do not enable cross-server sign-in, users need to call the phone number of their home server to sign in.

The process for a cross-server sign-in call is as follows:

1. A user calls the server configured for cross-server sign-in. The user is identified by the calling number or is asked to enter his or her ID.
2. The server looks up the caller ID in the database to determine whether the account is homed on the local server or on a networked server.
    - If the user account is homed on the local server, the sign-in proceeds as usual.
    - If the user account is homed on another server, the conversation plays a “One moment please” prompt (if configured to do so), puts the user on hold, and calls the user home server using the same port that the user called in on. Note that if the user is calling from his or her primary or alternate extension, the “One moment please” prompt is typically the first prompt that the user hears.

      When the receiving server answers, the originating server sends a sequence of DTMF tones that identifies the call as a cross-server sign-in.
3. The receiving location responds with a sequence of DTMF tones.
4. The originating location hands off the call to the receiving server for processing. The conversation on the receiving server prompts for the user password. At this point, the behavior is as though the user had called the receiving server directly.

The intended use of this feature is limited to users calling in from outside your organization. Although cross-server sign-in transfers internal calls to the home server, doing so for a large number of users increase the load on the servers. Therefore, user phones should always be configured so that the “Messages” or voicemail speed-dial button calls the home server of the user directly. When moving a user account from one server to another, update the phone system configuration for the user accordingly.

In case of a video call, when two Unity Connection locations are linked by an intersite, intrasite link, or HTTPS network, then if a user from one Unity Connection location attempts to sign-in to another Unity Connection location, the call is downgraded to audio.

Prerequisites for Enabling Cross-Server Sign-In

If your Cisco Voicemail Organization includes Cisco Unity servers, all of the networked Cisco Unity servers that you configure as originating locations for cross-server sign-in must be configured to be in the same dialing domain as the Cisco Unity site gateway. The dialing domain is configured on the Network > Primary Location > Profile page in the Cisco Unity Administrator.

Task List for Enabling Cross-Server Sign-In

Whether you are configuring a single Unity Connection site, an organization that contains two Unity Connection sites, or an organization that contains a Unity Connection site and a Cisco Unity site, the same basic set of tasks applies. Use the following task list to enable cross-server sign-in. The cross references take you to detailed procedures.

1. Determine which locations are originating locations and which are the receiving locations for cross-server sign-in. Often a single location is designated as the originating location that all users call into from outside the organization, and all other location are designated as receiving locations; however, this does not have to be the case. A single location also may be both an originating location and a receiving location.
2. For each originating location, make a list of the phone numbers that the location must dial to reach the receiving location servers.

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, you need a dial string that all phone system integrations can use to reach the receiving location.

3. Configure each receiving location so that it can handle incoming cross-server handoff requests.
   - If the receiving location is a Cisco Unity Connection server, see the Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests.
   - If the receiving location is a Cisco Unity server, see the Verifying a Receiving Cisco Unity Location Routes Calls to the Opening Greeting.
4. If Cisco Unity Connection locations receive cross-server handoff requests from Cisco Unity servers, configure the Unity Connection locations to allow cross-server DTMF sequences that begin with #. See the Configuring a Unity Connection Receiving Location to Allow Cross-Server DTMF Sequences from Cisco Unity Locations.
5. For each originating location, enable the cross-server sign-in feature and enter the pilot numbers of the receiving locations from the list that you created in Task 2.
   - If the location is a Cisco Unity Connection server, see the Configuring a Unity Connection Originating Location to Perform Cross-Server Sign-In Requests.
   - If the location is a Cisco Unity server, see the Configuring a Cisco Unity Originating Location to Perform Cross-Server Sign-In Requests.

6. Test the cross-server sign-in functionality. See the Testing Cross-Server Sign-In.

Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests

By default, each Unity Connection server is configured to ignore cross-server handoff requests. To enable cross-server features, you must configure the receiving location to accept requests and also verify that the location routes incoming cross-server calls to a call handler. Do the following two procedures toconfigure each receiving Unity Connection location to accept handoffs. (Doing so allows the location toreceive handoffs of all types-sign-in, transfer, and live reply.)

Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests

Step 1 In Cisco Unity Connection Administration, on a location that accepts cross-server handoffs for users who are homed on that location (the receiving location), expand **System Settings** > **Advanced** and select **Conversations**.

Step 2 Check the **Respond to Cross-Server Handoff Requests** check box.

Step 3 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying Call Routing Rules are Set to Route Calls to a Call Handler Greeting

Step 1 In Cisco Unity Connection Administration, on a location that accepts cross-server handoffs, expand **Call Management** > **Call Routing** and select **Direct Routing Rules**.

Step 2 Select the display name of the routing rule that applies to incoming cross-server calls from originating locations.

Step 3 Verify that calls that match the rule are routed to a call handler.

Step 4 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying a Receiving Cisco Unity Location Routes Calls to the Opening Greeting

In order to accept cross-server handoff requests, each Cisco Unity server must be configured to route calls to the Opening Greeting call handler. (This is the default when Cisco Unity is initially installed.)

Note For failover systems, do the procedure on both the primary and secondary servers.

Do the following procedure to verify that call routing rules are set to route calls to the Opening Greeting

Step 1 In the Cisco Unity Administrator, on a location that accepts cross-server sign-in handoffs, expand **Call Routing** > **and select** > **Direct Calls**.

Step 2 Verify that incoming cross-server calls from originating locations are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Step 3 Repeat the procedure on all remaining Cisco Unity receiving locations.

Configuring a Unity Connection Receiving Location to Allow Cross-Server DTMF Sequences from Cisco Unity Locations

The sequence of DTMF tones that an originating Cisco Unity location sends to the receiving location begins with # (pound). By default, the Unity Connection opening greeting and other call handlers are configured to ignore any additional caller input following a # key. In such a configuration, all cross-server handoffs fail.

You have a couple of options for changing the behavior on a Unity Connection receiving location so that cross-server handoffs are performed successfully:

- Change the opening greeting (or other existing call handler that receives the cross-server handoff calls based on your routing rule configuration) to allow additional input following a # key.
- Create a new call handler and direct-call routing rule specifically to handle cross-server calls. The new call handler must allow additional input after the # key. The direct call routing rule should route calls to the new call handler based on criteria that apply to cross-server calls—the calling number of any originating Cisco Unity location, for example, or the cross-server dial string that the originating locations dial to reach the receiving location. (If you do not want other calls to match the routing rule, select criteria that are unique to cross-server calls.)

Do the following procedure on each Unity Connection receiving location to configure the opening greeting or other call handler to allow additional input after the # key, and, optionally, to create a new direct-call routing rule.

Procedure

Step 1 Sign in to Cisco Unity Connection Administration for a location that accept across-server sign-in handoffs. Expand **Call Management** and select **System Call Handlers**.

Step 2 On the Search Call Handlers page, you can do either of the following:

- Select the display name of the opening greeting or other call handler that you want to modify. Skip to Step 6.
- Select **Add New** to create a new call handler specifically for cross-server calls. See the Step 3.

Step 3 On the New Call Handler page, enter basic settings, as applicable. (For more information on each field, see Help> **This Page**).

Step 4 To configure the call handler to accept the cross-server DTMF sequence:

1. In the Edit menu, select **Caller Input**.
2. On the Caller Input page, select **#** and uncheck the **Ignore Additional Input** check box.
3. Select **Save**.

Step 5 Create a new Direct Call Routing Rule to send calls from the Cisco Unity servers to the call handler:

1. Expand **Call Management > Call Routing** and select **Direct Routing Rules**.
2. On the Direct Routing Rules page, select **Add New**.
3. On the New Direct Rule page, enter the name of the new rule in the Display Name field and select **Save**.

4. On the Edit Direct Rule page, for the Send Call To field, select **Call Handler** and the name of the call handler you added in Step 2.
5. Select **Save**.
6. Under Routing Rule Conditions, select **Add New**.
7. Configure the routing rule condition to match cross-server calls from Cisco Unity servers. For example, use the Calling Number field to match the phone numbers of the Cisco Unity ports that answer user calls.
8. Select **Save**.
9. On the Edit menu, select **Edit Direct Routing Rule**.
10. Repeat f. through i. for each additional number or number pattern that you need to match cross-server calls.

Step 6 Repeat the procedure on all remaining Unity Connection receiving locations.

Configuring a Unity Connection Originating Location to Perform Cross-Server Sign-In Requests

By default, a Unity Connection location does not attempt to perform a cross-server sign-in for users homed on any other locations.

Step 1 In Cisco Unity Connection Administration, on a location that handles sign-in calls from remote users (the originating location), expand **Networking** and select **Locations**.

Step 2 On the Search Locations page, select the Display Name of a remote location that accepts cross-server sign-in requests for users homed on this location (or the receiving location).

Step 3 On the Edit Location page for the receiving location, initiate cross-server features to the receiving location:

a) To enable cross-server sign-in to the remote location, check the **Allow Cross-Server Sign-In to this Remote Location** check box.

b) Enter the dial string that this location uses to call the receiving location when performing the handoff (for example, the pilot number of the home server).

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, enter a dial string that all phone system integrations can use to reach the receiving location.

Step 4 Repeat Step 2 and Step 3 to configure each receiving location that accepts cross-server sign-in handoffs from this location.

Tip After you have saved the changes on a page, use the **Next** and **Previous** buttons to quickly navigate through each location in the organization.

Step 5 Repeat the procedure on all remaining Unity Connection originating locations.

Configuring a Cisco Unity Originating Location to Perform Cross-Server Sign-In Requests

By default, a Cisco Unity originating location do not attempt to perform a cross-server sign-in for users homed on any other locations. Do the following procedure to enable cross-server sign-in on any Cisco Unity originating locations.

Note If the system is using failover, do the procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

Step 1 In the Cisco Unity Administrator, expand **Network** > **and select** > **Dialing Domain Options**.

Note If the Dialing Domain Options link is unavailable on the system, you must first configure the dialing domain on the Primary Location Settings page in the Cisco Unity Administrator.

Step 2 In the Cross Server Logon section, select the **Subscribers Dial the Same Number to Log On to Cisco Unity** check box.

Step 3 In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each server that is displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers are replicated to the secondary server.)

Step 4 Check the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "One moment please" prompt is optional, you must check the check box because the cross-server process can take several seconds before the receiving server prompts users to enter their passwords.

Step 5 Select **Save**.

Step 6 Repeat the procedure on all remaining Cisco Unity originating locations.

Testing Cross-Server Sign-In

You must test cross-server sign-in before allowing users to use the feature. For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

Do the following procedure to test cross-server sign-in:

Step 1 Create a new user account (or use an existing account) on each of the destination servers for testing purposes. Be sure to verify that the user account information has replicated to all of the servers that you are testing. The time that it takes for the user data to replicate depends on your network configuration and replication schedule.

Step 2 For each user account, call the pilot number for the server configured for cross-server sign-in, and attempt to sign in. Verify that:

- The "One moment please" prompt is played (if configured to do so).
- You successfully sign in.

Cross-Server Transfers

A cross-server transfer is a special kind of supervised transfer that passes control of a call from the automated attendant or a directory handler to the home server of the called user.

1. A caller calls a Cisco Unity or Unity Connection server on which an audio text application has been configured.
2. The caller does either of the following:
   - In a call handler (such as the opening greeting), enters the extension of a user on another server.
   - In a directory handler, spells the name of a user on another server.
1. The server that is handling the call puts the caller on hold, and calls the home server of the user.
2. When the receiving server answers, the originating server sends a sequence of DTMF tones that identify the call as a cross-server transfer.
3. The receiving server responds with a sequence of DTMF tones.
4. The originating server hands off the call to the receiving server for processing. At this point, the behavior is as though the caller had directly called the automated attendant or directory handler on the receiving server.
5. In case of a video call, when two Unity Connection locations are linked by an intersite, intrasite link, or HTTPS network, then if a user from one Unity Connection location attempts to cross-server transfer, the call is downgraded to audio with respect to supervise transfer.
6. In case of a video call, when two Unity Connection locations are linked by an intersite, intrasite link, or HTTPS network, then if a user from one Unity Connection location attempts to cross-server transfer, the call gets established video only with respect to release to switch.

When cross-server transfers have been configured, user call transfer, call screening, call holding, and announce features are available.

Prerequisites for Enabling Cross-Server Transfers

If your Cisco voicemail organization includes networked Cisco Unity servers:

- All of the Cisco Unity servers that you configure as originating locations for cross-server transfers must be configured to be in the same dialing domain as the Cisco Unity site gateway. The dialing domain is configured on the Network > Primary Location > Profile page in the Cisco Unity Administrator.
- The addressing, directory handler, and automated attendant search scopes for each Cisco Unity server must be set to the dialing domain or global directory. For details, see the “Setting the Addressing, Directory Handler, and Automated Attendant Search Scopes” section in the “Digital Networking” chapter of the applicable *Networking Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Task List for Enabling Cross-Server Transfers

Whether you are configuring a single Unity Connection site, an organization that contains two Unity Connection sites, or an organization that contains a Unity Connection site and a Cisco Unity site, the same basic set of tasks applies. Use the following task list to enable cross-server transfers. The cross references take you to detailed procedures.

1. Determine whether each location is an originating location, a receiving location, or both.
2. For each originating location, make a list of the phone numbers the location must dial to reach the receiving location servers.

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, you need a dial string that all phone system integrations can use to reach the receiving location.

3. Configure each receiving location so that it can handle incoming cross-server handoff requests.
   - If the receiving location is a Unity Connection server, see the "Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests" section on page 6-11.
   - If the receiving location is a Cisco Unity server, see the Verifying a Receiving Cisco Unity Location Routes Calls to the Opening Greeting.
4. If Unity Connection locations receives cross-server handoff requests from Cisco Unity servers, configure the Unity Connection locations to allow cross-server DTMF sequences that begin with #. See the Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests.
5. For each originating location, enable the cross-server transfer feature and enter the pilot numbers of the receiving locations from the list that you created in Task 2.
   - If the location is a Unity Connection server, see the Configuring Unity Connection Originating Location to Perform Cross-Server Transfer Requests.
   - If the location is a Cisco Unity server, see the Configuring a Cisco Unity Originating Location to Perform Cross-Server Transfer Requests.
6. Test the cross-server transfer functionality. See the Testing Cross-Server Transfer.

Configuring Cross-Server Transfers during Call Forward to Cisco Unity Connection

Do the following procedure to configure cross-server transfers during call forward to Cisco Unity Connection:

Step 1 To view the configuration of cross-server transfers during call forward, execute the following command:

```
run cuc dbquery unitydirdb select fullname,name,parentid,valuebool,value from vw_Configuration where
 name like 'HandoffForwardRemoteForward'
```

If the command results a configured table entry, it means the feature is configured on Cisco Unity Connection. Otherwise, go to Step 2 to create a configuration entry.

In configured table entry, check the value of "valuebool" parameter. If valuebool is one, it means the feature is enabled for Cisco Unity Connection. Otherwise, go to Step 3 to enable the feature.

Step 2 *(Applicable for Unity Connection 11.5(1) SU5 and earlier releases)* Create the configuration entry using the following command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationCreate(pName='HandoffForwardRemoteForward'::lvarchar,
pParentFullName='System.Conversations.CrossBox'::lvarchar, pType=11, pValueBool=0, pRequiresRestart=1)
```

Step 3 Enable the cross-server transfers during call forward using the following command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pName='HandoffForwardRemoteForward'::lvarchar,
pParentFullName='System.Conversations.CrossBox'::lvarchar, pValueBool=1)
```

Step 4 Disable the cross-server transfers during call forward using the following command:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pName='HandoffForwardRemoteForward'::lvarchar,
pParentFullName='System.Conversations.CrossBox'::lvarchar, pValueBool=0)
```

Note
- In case of a cluster, execute the commands only on publisher server and make sure that database replication is working fine for the cluster.
- Service restart is not required after executing the above commands.

Note With Unity Connection 11.5(1) SU6 and later, you can also enable the cross-server transfers during call forward through Cisco Unity Connection Administration. To enable the feature, navigate **System Setting** > **Advanced** > **Conversations** and check the **Cisco Unity Cross-Server Handoff During Call Forward** check box on Conversation Configuration page of Cisco Unity Connection Administration.

Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests

By default, each Unity Connection server is configured to ignore cross-server handoff requests. To enable cross-server features, you must configure the receiving location to accept requests and also verify that the location routes incoming calls to a call handler.

Do the following procedure configure a Unity Connection receiving location

Step 1 Sign in to Cisco Unity Connection Administration for a location that accepts cross-server handoffs for users homed on that location (the receiving location). Expand **System Settings** > **Advanced** and select **Conversations**.

Step 2 Check the **Respond to Cross-Server Handoff Requests** check box.

Step 3 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying Call Routing Rules are Set to Route Calls to a Call Handler Greeting

Step 1 Sign in to Cisco Unity Connection Administration for a location that accepts cross-server handoffs. Expand **Call Management** > **Call Routing** and select **Direct Routing Rules**.

Step 2 Select the display name of the routing rule that applies to incoming cross-server calls from originating locations.

Step 3 Verify that calls that match the rule are routed to a call handler.

Step 4 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying a Receiving Cisco Unity Location Routes Calls to the Opening Greeting

In order to accept cross-server handoff requests, each Cisco Unity server must be configured to route calls to the opening greeting call handler. (This is the default when Cisco Unity is initially installed.) Do the following procedure on each of the receiving Cisco Unity servers to verify that the call routing rules are set properly to accept handoffs.

Note For failover systems, do the procedure on both the primary and secondary servers.

Step 1 Sign in to Cisco Unity Administrator for a location that accepts cross-server transfer handoffs. Expand **Call Routing** > **Direct Calls**.

Step 2 Verify that incoming cross-server calls from originating locations are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Step 3 Repeat the procedure on all remaining Cisco Unity receiving locations.

Configuring a Unity Connection Receiving Location to Allow Cross-Server DTMF Sequences from Cisco Unity Locations

The sequence of DTMF tones that an originating Cisco Unity location sends to the receiving location begins with # (pound). By default, the Unity Connection opening greeting and other call handlers are configured to ignore any additional caller input following a # key. In such a configuration, all cross-server handoffs fail.

You have a couple of options for changing the behavior on a Unity Connection receiving location so that cross-server handoffs are performed successfully:

- Change the opening greeting (or other existing call handler that receives the cross-server handoff calls based on your routing rule configuration) to allow additional input.
- Create a new call handler and direct-call routing rule specifically to handle cross-server calls. The direct call routing rule should route calls to the new call handler based on criteria that apply to cross-server calls—the calling number of any originating Cisco Unity location, for example, or the cross-server dial string that the originating locations dial to reach the receiving location. (If you do not want other calls to match the routing rule, select criteria that are unique to cross-server calls.)

Do the following procedure on each Unity Connection receiving location to configure the opening greeting or other call handler to allow additional input after the # key, and, optionally, to create a new direct-call routing rule.

Step 1 Sign in to Cisco Unity Connection Administration for a location that accepts cross-server transfer handoffs. Expand **Call Management** and select **System Call Handlers**.

Step 2 On the Search Call Handlers page, select the display name of the opening greeting or other call handler that you want to modify, or select **Add New** to create a new call handler specifically for cross-server calls.

Step 3 If you did not create a new call handler in Step 2, skip to Step 6. If you created a new call handler in Step 2, on the New Call Handler page, enter basic settings, as applicable. (For field information, on the Help menu, select **This Page**.)

Step 4 To configure the call handler to accept the cross-server DTMF sequence, do the following substeps:

a) On the Edit menu, select **Caller Input**.
b) On the Caller Input page, select #.
c) Uncheck the **Ignore Additional Input** check box.
d) Select **Save**.

Step 5 If you created a new call handler in Step 2, create a new direct-call routing rule to send calls from the Cisco Unity servers to the call handler for processing:

a) Expand **Call Management > Call Routing**, then select **Direct Routing Rules**.
b) On the Direct Routing Rules page, select **Add New**.
c) On the New Direct Rule page, enter the name of the new rule in the Display Name field.
d) Select **Save**.
e) On the Edit Direct Rule page, for Send Call To, select **Call Handler**, then select the name of the call handler you added in Step 2.
f) Select **Save**.
g) Under Routing Rule Conditions, select **Add New**.
h) Configure the routing rule condition to match cross-server calls from Cisco Unity servers. For example, use the Calling Number field to match the phone numbers of the Cisco Unity ports that answer user calls.
i) Select **Save**.
j) On the Edit menu, select **Edit Direct Routing Rule**.
k) Repeat g. through j. for each additional number or number pattern that you need to match cross-server calls.

Step 6 Repeat the procedure on all remaining Unity Connection receiving locations.

Configuring Unity Connection Originating Location to Perform Cross-Server Transfer Requests

By default, a Unity Connection location do not attempt to perform a cross-server transfer. Note that when you enable cross-server transfers on Unity Connection, cross-server live reply is automatically enabled. Do the following procedure to enable cross-server transfer and live reply on any Unity Connection originating locations.

Do the following procedure to configure a Unity Connection originating location to perform cross-server transfer and live reply handoff requests:

Step 1 In Cisco Unity Connection Administration, on a location that transfers calls to remote users (the originating location), expand **Networking** and select **Locations**.

Step 2 On the Search Locations page, select the Display Name of a remote location that accepts cross-server transfer handoffs for users who are homed on this location (the receiving location).

Step 3 On the Edit Location page for the receiving location, do the following to initiate cross-server features to this receiving location:

a) To enable cross-server transfer and live reply to the remote location, check the **Allow Cross-Server Transfer to this Remote Location** check box.

b) Enter the dial string that this location uses to call the receiving location when performing the handoff (for example, the pilot number of the receiving location).

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, enter a dial string that all phone system integrations can use to reach the receiving location.

Step 4 Repeat Step 2 and Step 3 for each receiving location that accepts cross-server transfer handoffs from this location.

Tip After you have saved the changes on a page, use the **Next** and **Previous** buttons to quickly navigate through each location in the organization.

Step 5 Repeat the procedure on all remaining Unity Connection originating locations.

Configuring a Cisco Unity Originating Location to Perform Cross-Server Transfer Requests

By default, a Cisco Unity originating location do not attempt to perform cross-server transfers to any other locations. Do the following procedure to enable cross-server transfers on any Cisco Unity originating locations.

Note If the system is using failover, do the following procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

Step 1 In the Cisco Unity Administrator, go to the **Network** > **Dialing Domain Options** page.

Note If the Dialing Domain Options link is unavailable on the system, you must configure the dialing domain on the Primary Location Settings page in the Cisco Unity Administrator.

Step 2 Select the **Cross-server Transfer: Pass Control to the Called Subscriber's Cisco Unity Server** check box. (Selecting Release Calls to the Phone System disables cross-server transfers originating from this server. Instead of handing off calls to the home server of the user, Cisco Unity attempts a release transfer to the Cross-Server Transfer Extension configured for the user. This fails if a Unity Connection user does not have a Cross-Server Transfer Extension configured.)

Step 3 In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each server displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers are replicated to the secondary server.)

Step 4 Select the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "One moment please" prompt is optional, you should check the check box because the cross-server process can take several seconds before the caller is transferred.

Step 5 Select **Save**.

Step 6 Repeat the procedure on all remaining Cisco Unity originating locations.

Testing Cross-Server Transfer

You should test the cross-server transfers before allowing callers to use the feature. For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

Do the following procedure to test cross-server transfer:

Step 1 Create a new user account (or use an existing account) on each of the destination servers for testing purposes. Be sure to verify that the user account information has replicated to all of the servers that you are testing. The time that it takes for the user data to replicate depends on your network configuration and replication schedule.

Step 2 For each user account, call the pilot number for the server configured for cross-server transfer, and enter the user extension at the opening greeting. Verify that:

- The “One moment please” prompt is played (if configured to do so).
- The call is transferred to the user phone or the greeting, according to the call transfer settings of the called user.

Cross-Server Live Reply

Live reply, when enabled, allows a user who is listening to messages by phone to reply to a message from another user by transferring to the user. Note that whether users have access to live reply is controlled by the class of service.

When cross-server live reply is enabled:

1. After listening to a message from a user on another networked location, the message recipient selects to call the user who left the message.

   Note that if identified subscriber messaging (ISM) is disabled on the location that recorded the message, the cross-server live reply option is only available for messages that are sent by users who sign in and address and send the message from their mailboxes.

2. The originating location puts the user on hold and looks up the extension in the database to determine whether the user who is being replied to is on the same server or is on another networked location. If the user is on the same server, processing proceeds as usual.

   However, if the user who is being replied to is on another location, the originating location calls the applicable receiving location.

3. When the receiving location answers, the originating location sends a sequence of DTMF tones that identify the call as a cross-server live reply.

4. The receiving location responds with a sequence of DTMF tones.

5. The originating location hands off the call to the receiving location for processing.

Prerequisites: Enabling Cross-Server Live Reply

- If your Cisco Voicemail Organization includes networked Cisco Unity servers:
  - All of the Cisco Unity servers that you configure as originating locations for cross-server live reply must be configured to be in the same dialing domain as the Cisco Unity site gateway. The dialing domain is configured on the Network > Primary Location > Profile page in the Cisco Unity Administrator.
  - Users must belong to a class of service for which live reply between users is enabled. For Cisco Unity users, live reply between users is enabled on the Subscribers > Class of Service > Messages page in the Cisco Unity Administrator, by checking the Subscribers Can Reply to Messages from Other Subscribers by Calling Them check box.
  - For cross-server live reply to be available to messages that were sent when the sender called the recipient from a recognized phone number and was forwarded to Cisco Unity, identified subscriber messaging must be set up between networked Cisco Unity servers and extended to include Unity Connection Networking subscribers. For instructions, see the "Extending Cisco Unity Identified Subscriber Messaging to Include UnityConnection Networking Subscribers" section.
- Users must belong to a class of service for which live reply between users is enabled. For Cisco Unity Connection users, live reply between users is enabled on the Class of Service > Edit Class of Service page in Cisco Unity Connection Administration, by selecting the **Users Can Reply to Messages from Other Users by Calling Them** check box.

Task List for Enabling Cross-Server Live Reply

Note In Unity Connection, cross-server live reply is automatically supported (for users whose class of service allows it) when cross-server transfer is enabled. If you have previously configured a Unity Connection location as an originating or receiving location for cross-server transfers, the location also originates or receives cross-server live reply requests.

Use the following task list to enable cross-server live reply between Cisco Unity and Unity Connection sites, or to enable cross-server transfers and live reply between Unity Connection locations (either in a single site or between two Unity Connection sites). The cross references take you to detailed procedures.

1. Determine whether each location is an originating location, a receiving location, or both.
2. For each originating location, make a list of the phone numbers the location must dial to reach the receiving location servers.

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, you need a dial string that all phone system integrations can use to reach the receiving location.

3. Configure each receiving location so that it can handle incoming cross-server handoff requests.

- If the receiving location is a Cisco Unity Connection server, see the Configuring a Unity Connection Receiving Location to Allow Cross-Server DTMF Sequences from Cisco Unity Locations.
- If the receiving location is a Cisco Unity server, see the Verifying That a Receiving Cisco Unity Location Routes Calls to the Opening Greeting.

4. If Unity Connection locations receive cross-server handoff requests from Cisco Unity servers, configure the Unity Connection locations to allow cross-server DTMF sequences that begin with #. See the Configuring a Unity Connection Originating Location to Perform Cross-Server Sign-In Requests.
5. For each originating location, enable the applicable cross-server features and enter the pilot numbers of the receiving locations from the list that you created in Task 2.
   - If the location is a Cisco Unity Connection server, see the Configuring a Cisco Unity Originating Location to Perform Cross-Server Sign-In Requests.
   - If the location is a Cisco Unity server, see the Configuring a Cisco Unity Originating Location to Perform Cross-Server Live Reply Requests.
6. Test the cross-server live reply functionality. See the Testing Cross-Server Sign-In.

Procedures: Enabling Cross-Server Live Reply

Configuring a Unity Connection Receiving Location to Accept Cross-Server Handoff Requests

By default, each Unity Connection server is configured to ignore cross-server handoff requests. To enable cross-server features, you must configure the receiving location to accept requests and also verify that the location routes incoming calls to a call handler.

Step 1 In Cisco Unity Connection Administration, on a location that accepts cross-server handoffs for users who are homed on that location (the receiving location), expand **System Settings** > **Advanced** and select **Conversations**.

Step 2 Check the **Respond to Cross-Server Handoff Requests** check box.

Step 3 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying Call Routing Rules are Set to Route Calls to a Call Handler Greeting

Step 1 In Cisco Unity Connection Administration, on a location that accepts cross-server handoffs, expand **Call Management** > **Call Routing** and select **Direct Routing Rules**.

Step 2 Select the display name of the routing rule that applies to incoming cross-server calls from originating locations.

Step 3 Verify that calls that match the rule are routed to a call handler.

Step 4 Repeat the procedure on all remaining Unity Connection receiving locations.

Verifying That a Receiving Cisco Unity Location Routes Calls to the Opening Greeting

In order to accept cross-server handoff requests, each Cisco Unity server must be configured to route calls to the Opening Greeting call handler. (This is the default when Cisco Unity is initially installed.) Do the following procedure on each of the receiving Cisco Unity servers to verify that the call routing rules are set properly to accept handoffs.

Note For failover systems, do the procedure on both the primary and secondary servers.

Step 1 In the Cisco Unity Administrator, on a location that accepts cross-server live reply handoffs, go to the **Call Routing** > **Direct Calls** page.

Step 2 Verify that incoming cross-server calls from originating locations are routed to the Opening Greeting.

The Default Call Handler routing rule (which cannot be deleted or modified) sends calls to the Opening Greeting. Therefore, if you have not added any routing rules, the server is already set to correctly process cross-server calls.

Step 3 Repeat the procedure on all remaining Cisco Unity receiving locations.

Configuring a Unity Connection Receiving Location to Allow Cross-Server DTMF Sequences from Cisco Unity Locations

The sequence of DTMF tones that an originating Cisco Unity location sends to the receiving location begins with # (pound) and includes a second tone that distinguishes the type of handoff (sign-in, transfer, or live reply). By default, the Unity Connection opening greeting and other call handlers are configured to ignore any additional caller input following a # key. In such a configuration, all cross-server handoffs fail.

You have a couple of options for changing the behavior on a Unity Connection receiving location so that cross-server handoffs are performed successfully:

- Change the opening greeting (or other existing call handler that receive the cross-server handoff calls based on your routing rule configuration) to allow additional input.
- Create a new call handler and direct-call routing rule specifically to handle cross-server calls. The direct call routing rule should route calls to the new call handler based on criteria that apply to cross-server calls—the calling number of any originating Cisco Unity location, for example, or the cross-server dial string that the originating locations dial to reach the receiving location. (If you do not want other calls to match the routing rule, select criteria that are unique to cross-server calls.)

Do the following procedure on each Unity Connection receiving location to configure the opening greeting or other call handler to allow additional input after the # key, and, optionally, to create a new direct-call routing rule.

Step 1 In Cisco Unity Connection Administration, on a location that accepts cross-server sign-in handoffs, expand **Call Management** and select **System Call Handlers**.

Step 2 On the Search Call Handlers page, select the display name of the opening greeting or other call handler that you want to modify, or select **Add New** to create a new call handler specifically for cross-server calls.

Step 3 If you did not create a new call handler in Step 2, skip to Step 6. If you created a new call handler in Step 2, on the New Call Handler page, enter basic settings, as applicable. (For field information, on the Help menu, select **This Page**.)

Step 4 To configure the call handler to accept the cross-server DTMF sequence, do the following substeps:

a) In the Edit menu, select **Caller Input**.
b) On the Caller Input page, select #.
c) Uncheck the **Ignore Additional Input** check box and select **Save**.

Step 5 If you created a new call handler in Step 2, create a new direct-call routing rule to send calls from the Cisco Unity servers to the call handler for processing:

a) Expand **Call Management > Call Routing** and select **Direct Routing Rules**.
b) On the Direct Routing Rules page, select **Add New**.
c) On the New Direct Rule page, enter the name of the new rule in the Display Name field.
d) Select **Save**.
e) On the Edit Direct Rule page, for Send Call To, select **Call Handler**, then select the name of the call handler you added in Step 2.
f) Select **Save**.
g) Under Routing Rule Conditions, select **Add New**.
h) Configure the routing rule condition to match cross-server calls from Cisco Unity servers. For example, use the Calling Number field to match the phone numbers of the Cisco Unity ports that answer user calls and select **Save**.
i) On the Edit menu, select **Edit Direct Routing Rule**.
j) Repeat g. through i. for each additional number or number pattern that you need to match cross-server calls.

Step 6 Repeat the procedure on all remaining Unity Connection receiving locations.

Configuring a Unity Connection Originating Location to Perform Cross-Server Live Reply and Transfer Requests

By default, a Unity Connection location do not attempt to perform a cross-server live reply. Note that when you enable cross-server live reply on Unity Connection, cross-server transfer is automatically enabled. Do the following procedure to enable cross-server transfer and live reply in on any Unity Connection originating locations.

Step 1 In Cisco Unity Connection Administration, on a location that transfers calls to remote users (the originating location), expand **Networking** and select **Locations**.

Step 2 On the Search Locations page, select the Display Name of a remote location that accepts cross-server live reply and transfer handoffs for users who are homed on this location (the receiving location).

Step 3 On the Edit Location page for the receiving location, do the following to initiate cross-server features to this receiving location:

a) To enable cross-server transfer and live reply to the remote location, check the **Allow Cross-Server Transfer to this Remote Location** check box.
b) Enter the dial string that this location uses to call the receiving location when performing the handoff (for example, the pilot number of the receiving location).

Note You can enter only one dial string for each receiving location. If the originating location is configured for multiple phone system integrations, enter a dial string that all phone system integrations can use to reach the receiving location.

Step 4 Repeat Step 2 and Step 3 for each receiving location that accepts cross-server transfer handoffs from this location.

Tip After you have saved the changes on a page, use the **Next** and **Previous** buttons to quickly navigate through each location in the organization.

Step 5 Repeat the procedure on all remaining Unity Connection originating locations.

Configuring a Cisco Unity Originating Location to Perform Cross-Server Live Reply Requests

By default, a Cisco Unity originating location do not attempt to perform a cross-server live reply to any other locations. Do the following procedure to enable cross-server live reply on any Cisco Unity originating locations.

Note If the system is using failover, do the following procedure on both the primary and secondary server, because most of the settings on the Network > Dialing Domain Options page are stored in the registry. (Registry settings are not replicated to the secondary server.)

Step 1 In the Cisco Unity Administrator, expand **Network** > **and select** > **Dialing Domain Options** page.

Note If the Dialing Domain Options link is unavailable on the system, you must configure the dialing domain on the Primary Location Settings page in the Cisco Unity Administrator.

Step 2 In the Live Reply section, select the **Subscribers with Class of Service Rights Can Reply to Messages from Subscribers Homed on Other Cisco Unity Servers by Calling Them** check box, then select **Cross-Server Live Reply: Pass Control to the Called Subscriber's Cisco Unity Server**. (Selecting Release Calls to the Phone System disables cross-server transfers originating from this server. Instead of handing off calls to the home server of the user, Cisco Unity attempts a release transfer to the Cross-Server Transfer Extension configured for the user. This fails if a Unity Connection user does not have a Cross-Server Transfer Extension configured.)

Step 3 In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the pilot number in the Dial String field for each server displayed in the table. (Note that the pilot numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the pilot numbers are replicated to the secondary server.)

Step 4 Select the **Play Prompt During Cross-Server Logon, Transfer, and Live Reply so That Callers Know Something Is Happening** check box. Although playing the "One moment please" prompt is optional, you should check the check box because the cross-server process can take several seconds before the caller is transferred.

Step 5 Select **Save**.

Step 6 Repeat the procedure on all remaining Unity Connection originating locations.

Testing Cross-Server Live Reply

You should test the cross-server live reply before allowing callers to use the feature.

For failover systems, first test that the primary destination servers answer cross-server calls. Then manually fail over the destination servers to verify that the secondary server answers cross-server calls. If the destination servers are properly configured for failover, the secondary server should answer cross-server calls when the primary server is unavailable.

Do the following procedure to test cross-server live reply:

Step 1 Create a new user account (or use an existing account) on each location for testing purposes. Verify that users belong to a class of service in which live reply is enabled. Also verify that the user account information has replicated to all of the servers that you are testing. The time that it takes for the user data to replicate depends on your network configuration and replication schedule.

Step 2 Sign in as a user on an originating location and send a message to the test users on other locations.

Step 3 For each user that receives the test message, sign in, listen to the message, and select to call the sender. Verify that:

- The "One moment please" prompt is played (if configured to do so).
- The call is transferred to the user phone or the greeting, according to the call transfer settings of the called user.

Notable Behavior for Cross-Server Sign-In, Transfers, and Live Reply

This section provides information about notable expected behavior associated with cross server sign-in, transfers and live reply.

Cross-Server Sign-In Not Providing User Workstation Client Sign-In Access

Users must access their home server (or cluster) when using client applications such as the Cisco Personal Communications Assistant (Cisco PCA) and IMAP clients. The phone interface is the only client that provides cross-server sign-in capability.

Users Prompted for a Password During Cross-Server Sign-In Between Unity Connection and Cisco Unity

When a Unity Connection user calls a Cisco Unity location from a known extension and is transferred to the home location using cross-server sign-in, the receiving Unity Connection location can identify the user but does not recognize that the user is calling from a known extension. For this reason, the user is always prompted for a password, regardless of whether the Skip Password When Calling From a Known Extension setting is selected on the System Settings > Advanced > Conversation page in Cisco Unity Connection Administration.

Likewise, when a Cisco Unity user calls a Unity Connection location from a known extension and is transferred to the home location using cross-server sign-in, the user is always prompted for a password, regardless of whether Prompt for Phone Password is set to Only When User Calls from an Unknown Extension (on the Phone Password page for the user).

Factors Causing Delays During Cross-Server Handoff

The following factors can contribute significantly to delays in cross-server call handoff:

- Longer user extensions. A four-digit extension does not take as long to dial during the handoff as a ten-digit extension.

- Longer dialing strings to reach the receiving location. A four-digit dialing string does not take as long to dial as a ten-digit dialing string.
- Multiple elements (such as PIMG/TIMG units, voice gateways, TDM trunks, and PSTN interfaces) in the call path between the originating location and the receiving location. More elements in the call path require more processing time for handing off cross-server calls.

In your environment, these factors can create delays that may cause the cross-server features to be unusable or unfeasible for callers. You must test your cross-server configuration on a representative call path in your environment to determine whether the delays that callers experience are acceptable.

Increased Port Usage with Cross-Server Features

The cross-server features require the use of ports on both the originating and receiving locations. Depending on how busy your servers are, you may need to add more ports or an additional server before enabling these features. You may also need to adjust how ports are configured. For example, you may need to enable more ports to accept incoming calls.

After enabling the cross-server features, you should monitor activity on the servers closely until you are confident that the servers can handle the increased load. For Cisco Unity Connection servers, you can use the Port Activity report in Cisco Unity Connection Serviceability to monitor port usage. For Cisco Unity servers, you can use the Port Usage Analyzer for this task. The Port Usage Analyzer is available in the Report Tools section of Tools Depot. See Port Usage Analyzer Help for detailed instructions. Be sure to also monitor the Windows Event Viewer on any originating and receiving Cisco Unity servers for event log messages related to problems with ports.

Transfer Overrides on Cross-Server Transfers

When a caller enters an extension in the automated attendant followed by the digits “#2,” the caller is routed directly to the greeting for the extension entered without a transfer being attempted. This is known as the transfer override digit sequence.

Unity Connection automatically supports the transfer override sequence between networked locations. For Cisco Unity servers, by default the transfer override digit sequence is ignored when the user who is associated with the extension preceding the “#2” is homed on another server in the dialing domain. If you want to enable the transfer override digit sequence for users who are homed on other locations in the dialing domain, including Unity Connection locations, do the following procedure on each Cisco Unity server that originates the cross-server transfer requests.

Procedure to enable transfer override on cross-server transfers from a Cisco Unity location

Step 1 On the Cisco Unity server desktop, double-click the **Cisco Unity Tools Depot** icon.

Step 2 In the left pane, under Administrative Tools, double-click **Advanced Settings Tool**.

Step 3 In the Unity Settings pane, select **Networking—Allow Transfer Override on Cross-Server Transfer Handoff**.

Step 4 In the New Value list, select **1**, and then select **Set**.

Step 5 When prompted, select **OK**.

You do not need to restart the Cisco Unity software or server when you make a change.

Note For Cisco Unity failover, registry changes on one Cisco Unity server must be made manually on the other Cisco Unity server, because registry changes are not replicated.

Using Cross-Server Features with Display Original Calling Number on Transfer Parameter

When Cisco Unity Connection (and/or Cisco Unity) is integrated with Cisco Unified Communications Manager, the Display Original Calling Number on Transfer from Cisco Unity service parameter in Cisco Unified CM can interfere with the cross-server handoff, because the receiving location does not recognize that the incoming cross-server handoff call is from another location.

Do the following tasks so that cross-server handoffs complete properly between locations when this service parameter is set in Cisco Unified CM. In the task list, you create a special directory number for each receiving location that is used only during cross-server handoffs, so that the receiving location recognizes the call as a handoff.

Task List for Configuring a Cross-Server Directory Number for Cross-Server Features

1. In Cisco Unified Communications Manager Administration, create a new directory number (for example, on a CTI route point) for each location that receives cross-server sign-in, transfer, or live reply calls. Configure the new directory number to always forward calls to the pilot number for the location. See the "Directory Number Configuration" chapter of the applicable *Cisco Unified Communications Manager Administration Guide* for your release of Cisco Unified CM, at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
2. Configure each receiving location with a forwarded call routing rule that sends calls in which the forwarding station equals the location's new cross-server directory number to the Opening Greeting call handler. See the Adding Forwarded Call Routing Rules to Destination Locations for Cross-Server Calls.
3. Update each originating location to dial the cross-server directory number of the receiving location during cross-server calls, rather than the pilot number. See the Configuring the Cross-Server Directory Number as the Dial String on Originating Locations.

Adding Forwarded Call Routing Rules to Destination Locations for Cross-Server Calls

This section contains two procedures. Do either or both of the procedures, depending on whether you have Cisco Unity Connection and/or Cisco Unity receiving locations:

Step 1 In Cisco Unity Connection Administration on any one of the Unity Connection receiving locations, create the new forwarded routing rule:

a) Expand **Call Management** > **Call Routing** and select **Forwarded Routing Rules**.
b) On the Forwarded Routing Rules page, select **Add New**.
c) On the New Forwarded Rule page, enter the name of the new rule in the Display Name field and select **Save**.
d) On the Edit Forwarded Routing Rule page, for Send Call To, select **Call Handler**. From the call handler drop-down list, select **Opening Greeting** and select **Save**.
e) On the Edit Forwarded Routing Rule page, under Routing Rule Conditions, select **Add New**.

f) On the New Forwarded Routing Rule Condition page, select **Forwarding Station**. From the forwarding station drop-down list, select **Equals**. In the text box, enter the new cross-server directory number for this location.
g) Select **Save**.

Step 2 Return to the Forwarded Routing Rules page by selecting **Forwarded Routing Rules** > **Forwarded Routing Rules**, or by navigating to **Call Management** > **Call Routing** > **Forwarded Routing Rules**.

Step 3 Check the order of forwarded routing rules on the page. If the new routing rule that you created in Step 1 is not at the top of the table (in order of descending precedence) do the following substeps to move the new routing rule to the top of the forwarded routing rules table:

a) On the Forwarded Routing Rules page, select **Change Order**.
b) On the Edit Forwarded Routing Rule Order page, select the Display Name of the new routing rule that you created in Step 1.
c) Select the up arrow icon below the table to move the rule to the top position. (You may need to select the icon multiple times.)
d) Select **Save**.

Step 4 Repeat the procedure for each remaining Unity Connection receiving location.

Adding Forwarded Call Routing Rule to Cisco Unity Receiving Locations

Step 1 In the Cisco Unity Administrator on any one of the Cisco Unity receiving locations, create the new forwarded routing rule:

a) Navigate to **Call Management** > **Call Routing**.
b) Select **Forwarded Calls**.
c) Select the **Add** icon.
d) In the Add a Call Routing Rule dialog box, enter the name of the new rule in the Name field.
e) Select **Add**.
f) In the Forwarding Station field, enter the new cross-server directory number for this location.
g) In the Send Call To field, select **Call Handler**. Then, select **Select Call Handler**.
h) In the Call Handler Selection box, select the Opening Greeting call handler.
i) Select **Save**.

Step 2 Check the order of forwarded routing rules on the page. If the new routing rule that you created in Step 1 is not at the top of the table (in order of descending precedence) do the following substeps to move the new routing rule to the top of the forwarded routing rules table:

a) Select **Change Rule Order**.
b) On the Forwarded Calls Rules Reorganization page, select the Display Name of the new routing rule that you created in Step 1.
c) Select **Up** to move the rule to the top position and select **Close**.

Step 3 Select the **Save** icon.

Step 4 Repeat the procedure for each remaining Cisco Unity receiving location.

Configuring the Cross-Server Directory Number as the Dial String on Originating Locations

Follow either of the given procedures depending whether you have Unity Connection and/or Cisco Unity originating locations:

Step 1 In Cisco Unity Connection Administration, on any one of the Unity Connection locations that originate cross-server calls, expand **Networking** > **and** select **Locations**.

Step 2 On the Search Locations page, select the Display Name of a receiving location.

Step 3 On the Edit Location page for the receiving location, change the dial string that this location uses to call the receiving location to the new cross-server directory number of the receiving location. Select Save.

Step 4 Repeat Step 2 and Step 3 to configure each receiving location that accepts cross-server handoffs from this location.

Tip After you have saved the changes on a page, use the **Next** and **Previous** buttons to quickly navigate through each location in the organization.

Step 5 Repeat the procedure on all remaining Unity Connection originating locations.

Configuring the Cross-Server Directory Number as the Dial String on Cisco Unity Originating Locations

Step 1 In the Cisco Unity Administrator, expand **Network** > **and select** > **Dialing Domain Options**.

Step 2 In the Pilot Numbers for Cross-Server Logon, Transfer, and Live Reply section, enter the new cross-server directory number in the Dial String field for each server that is displayed in the table.

Note The numbers that you enter are stored in the SQL Server database UnityDb on the Cisco Unity server. Therefore, if the system is using failover, the numbers are replicated to the secondary server.)

Step 3 Select **Save** and repeat the procedure on all remaining Cisco Unity originating locations.

INDEX