CHAPTER 11

Cisco Unity Connection 9.x System Settings

See the following sections:

Edit General Configuration

Table 11-1 Edit General Configuration Page

Field	Description
Time Zone	*(Display only)* The default time zone setting determines when schedules are active. In addition, the default time zone is applied to users and call handlers that have the Use Default Time Zone check box checked. **Note** The default time zone can be changed only by using the command-line interface (CLI).
System Default Language	Select the default language in which system prompts are played to users and callers. **Note** Depending on your license settings, United States English may not be available.
System Default TTS Language	Select the Text to Speech (TTS) language that will be used if a TTS engine is not available for the phone language being used by a user or a call. For example, if a user is using the Arabic language, but no TTS engine is available for Arabic, the user will hear TTS in the language you select here. This is typically the same language that you selected in the System Default Language field. However, not all of the languages supported for system prompts are supported by the Text to Speech engine. **Note** Depending on your license settings, United States English may not be available.
Recording Format	Select the default format (or codec) for recorded messages. Default setting: G.711 Mu-Law.

Table 11-1 Edit General Configuration Page (continued)

Field	Description
Maximum Greeting Length	Enter the maximum length for system call handler greetings. The range is 1 to 1,200 seconds. Default setting: 90 seconds.
Target Decibel Level for Recordings and Messages	If audio normalization is enabled for a port group, enter the average volume, in decibels, that Cisco Unity Connection automatically maintains for recording voice messages and user greetings. Decibel levels are specified in negative numbers. For example, –26 db is louder than –45 db. Default setting: –26 decibels.
Default Partition	Select the partition that Cisco Unity Connection uses as the default partition when you create new objects that are not based on other objects, for example, when you create a new call handler template, directory handler, interview handler, or VPIM location. (This partition is selected by default in the Partition list on these pages, but you can select a different partition from the list at any time.) Note that changing the default partition does not affect any objects that have already been created.
Default Search Scope	Select the search space that Cisco Unity Connection uses as the default search scope when you create new objects that are not based on other objects, for example, when you create a new direct or forwarded routing rule. (This search space is selected by default in the Search Scope list on these pages, but you can select a different search space from the list at any time.) Note that changing the default search scope does not affect any objects that have already been created.
When a Recipient Cannot Be Found	Select the action that Cisco Unity Connection takes when receiving an SMTP message from an IMAP client where a recipient does not map to any known user or VPIM contact: • Send a Non-Deliverable Receipt—Unity Connection responds to the message sender with a non-delivery receipt (NDR). • Relay Message to Smart Host—Unity Connection relays the message to the smart host for delivery to a different server. **Note** You configure the SMTP smart host on the System Settings > SMTP Configuration > Smart Host page. Default setting: Send a Non-Deliverable Receipt.
IP Addressing Mode *(Cisco Unity Connection 8.5 and later only)*	When Cisco Unity Connection is configured for IPv6, select the option from the list to control where Unity Connection listens for incoming traffic: • IPv4 • IPv6 • IPv4 and IPv6 This setting is applicable to integrations with Cisco Unified Communications Manager phone systems via SCCP or SIP. Default Setting: IPv4 **Note** This setting is applicable to Unity Connection only. IPv6 is not supported in Cisco Unified Communications Manager Business Edition.

Table 11-1 Edit General Configuration Page (continued)

Field	Description
Authenticate Graphics for HTML Notification	Select the authentication mode that prompts users to enter their Unity Connection credentials to receive images in the HTML email notification. When the credentials get authenticated the images are displayed in the email notification. This facilitates the administrator to imply the authentication policy for displaying the status items, message status, and images within a notification. Non-authentication Mode: When you disable the authentication mode, the status items, message status, and images are displayed within a notification without prompting user for the credentials. **Note** Verify the email server and email client settings to confirm the support for display of images if used within the HTML notification template. For more information on how to configure Unity Connection to receive an HTML notification, refer to "Configuring Cisco Unity Connection 9.x for HTML-based Message Notification" section of the "Configuring an Email Account to Access Cisco Unity Connection 9.x Voice Messages" chapter of the *User Workstation Setup Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_setup/guide/9xcucuwsx.html.

Find and List Servers

Table 11-2 Find and List Servers Page

Field	Description
Delete Selected	To delete a server, check the check box to the left of the display name, and select Delete Selected. You can delete multiple servers at once.
Add New	To add a server, select the Add New button. A new page opens, on which you enter data applicable to the new server.
Host Name/IP Address	*(Display only)* The host name or IP address of the Cisco Unity Connection server in a Unity Connection cluster. If Unity Connection is not configured for a cluster, this field displays the host name or IP address of the local Unity Connection server.
Description	*(Display only)* A description of the Cisco Unity Connection server in a Unity Connection cluster.

See Also

- The "Configuring a Cisco Unity Connection 9.x Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/cluster_administration/guide/9xcuccagx.html.

Server Configuration

Table 11-3 Server Configuration Page

Field	Description
Database Replication	*(Display only)* The role of the Cisco Unity Connection server (publisher or subscriber) in a Unity Connection cluster.
Host Name/IP Address	Enter the host name or IP address of the Cisco Unity Connection server in a Unity Connection cluster.
IPv6 Name	If IPv6 is enabled, enter the host name or IPv6 address of the Cisco Unity Connection server in a Unity Connection cluster.
MAC Address	*(Optional)* Enter the MAC address of the Cisco Unity Connection server in a Unity Connection cluster.
Description	*(Optional)* Enter a description of the Cisco Unity Connection server in a Unity Connection cluster.

See Also

- The "Configuring a Cisco Unity Connection 9.x Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/cluster_administration/guide/9xcuccagx.html.

Search Authentication Rules

Table 11-4 Search Authentication Rules Page

Field	Description
Limit Search To	*(Applicable to Cisco Unity Connection configurations only.)* Select the criteria by which to limit the display of search results: • All—Display all search results, regardless of the Cisco Unity Connection location to which they belong. • Location—Display only results that belong to a particular Unity Connection location. When you select this option, choose the name of the location from the Where Name Is list.
Display Name	The name of the authentication rule. Select the Display Name to go to the specific page for the authentication rule.
Delete Selected	To delete an authentication rule, check the check box to the left of the display name, and select Delete Selected. You can delete multiple authentication rules at once.
Add New	To add an authentication rule, select the Add New button. A new page opens, on which you enter data applicable to the authentication rule.

See Also

- The "Specifying Password, PIN, Sign-In, and Lockout Policies in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

New Authentication Rule

Table 11-5 New Authentication Rule Page

Field	Description
Display Name	Enter a descriptive name for the authentication rule.
Failed Sign-In ____ Attempts	Enter the number of failed sign-in attempts after which users cannot access Cisco Unity Connection. When set to 0 (zero), there is no limit to the number of failed sign-in attempts, and the user is not locked out of the account. Default setting: 3 attempts.
No Limit for Failed Sign-Ins	Check this check box so that there is no limit to the number of failed sign-in attempts, and the user is not locked out of the account.
Reset Failed Sign-In Attempts Every ____ Minutes	Enter the number of minutes after which Cisco Unity Connection clears the count of failed sign-in attempts (unless the failed sign-in limit is already reached and the account is locked). When set to 0 (zero), Cisco Unity Connection shows the following error message: **Reset Failed Sign-In Attempts Every is not in the range 1 through 120**. Default setting: 30 minutes.
Lockout Duration ____ Minutes	Enter the number of minutes that a user account remains locked after the number of allowed Failed Sign-In attempts has been reached. While the account is locked, Cisco Unity Connection prevents the user from accessing Unity Connection by phone. If a value of 0 (zero) is entered, the account remains locked until manually unlocked by the administrator. Default setting: 30 minutes.
Administrator Must Unlock	Check this check box so that accounts remain locked until manually unlocked by the administrator.
Minimum Duration Between Credential Changes ____ Minutes	Enter the number of minutes that must elapse between password changes. This setting does not apply when administrators are changing the password in Cisco Unity Connection Administration. Default setting: 1440 minutes (1 day).
Credential Expires After ____ Days	Default setting: 180 days.
Never Expires	Check this check box so that passwords or PINs based on this authentication rule never expire. Use of this check box is most applicable for low-security users or for accounts that can be accessed by more than one person. Note that when this check box is checked, the user is still able to change passwords or PINs at any time.

Table 11-5 New Authentication Rule Page (continued)

Field	Description
Expiration Warning Days	Enter the number of days before passwords or PINs expire that Cisco Unity Connection will warn users that a password or PIN is about to expire. A value of 0 (zero) means that Unity Connection will not warn users that a password or PIN is about to expire. Default setting: 15 days.
Minimum Credential Length	Enter the required number of digits for user passwords and PINs. In general, shorter passwords and PINs are easier to use, but longer passwords and PINs are more secure. We recommend requiring eight or more digits. When you change the minimum credential length, users are required to use the new length the next time that they change the password or PIN. Enter a value between 1 and 64 digits. Default setting: 8 digits.
Stored Number of Previous Credentials	Enter a value for the number of previous passwords or PINs that Cisco Unity Connection stores for a user. When a user enters a new password or PIN, Unity Connection compares it to the stored passwords or PINs, and rejects it if it matches a password or PIN in the history. A value of 0 (zero) means that Unity Connection does not store any previous passwords or PINs for the user. Default setting: 5 passwords or PINs.
Check for Trivial Passwords	Check this check box to have Cisco Unity Connection verify that a new password or PIN meets the following criteria when the passwords or PINs are changed by using Cisco Unity Connection Administration, the Unity Connection Messaging Assistant, or the Unity Connection conversation: • The digits are not all the same (for example, 9999). • The digits are not consecutive (for example, 1234 or 4321). • The password or PIN is not the same as the primary extension that is assigned to the user. In addition to checking this check box, consider providing users with a password or PIN policy that advises them to avoid specifying a password or PIN that: • Spells their first or last name, their organization or company name, or any other obvious words. • Contains their primary extension. • Is the reverse of their primary extension or contains the reverse of their primary extension. • Uses the same digits more than twice in a row (for example, 900012). • Is a 1-digit increment of a previous password or PIN (for example, 20185 to 20186). • Contains fewer than three different digits (for example, 18181).

See Also

Edit Authentication Rule

Table 11-6 Edit Authentication Rule Page

Field	Description
Display Name	Enter a descriptive name for the authentication rule.
Failed Sign-In ____ Attempts	Enter the number of failed sign-in attempts after which users cannot access Cisco Unity Connection. When set to 0 (zero), there is no limit to the number of failed sign-in attempts, and the user is not locked out of the account. Default setting: 3 attempts.
No Limit for Failed Sign-Ins	Check this check box so that there is no limit to the number of failed sign-in attempts, and the user is not locked out of the account.
Reset Failed Sign-In Attempts Every ____ Minutes	Enter the number of minutes after which Cisco Unity Connection clears the count of failed sign-in attempts (unless the failed sign-in limit is already reached and the account is locked). When set to 0 (zero), Cisco Unity Connection shows the following error message: **Reset Failed Sign-In Attempts Every is not in the range 1 through 120**. Default setting: 30 minutes.
Lockout Duration ____ Minutes	Enter the number of minutes that a user account remains locked after the number of allowed Failed Sign-In attempts has been reached. While the account is locked, Cisco Unity Connection prevents the user from accessing Unity Connection by phone. If a value of 0 (zero) is entered, the account remains locked until manually unlocked by the administrator. Default setting: 30 minutes.
Administrator Must Unlock	Check this check box so that accounts remain locked until manually unlocked by the administrator.
Minimum Duration Between Credential Changes ____ Minutes	Enter the number of minutes that must elapse between password changes. This setting does not apply when administrators are changing the password in Cisco Unity Connection Administration. Default setting: 1440 minutes (1 day).
Credential Expires After ____ Days	Default setting: 180 days.
Never Expires	Check this check box so that passwords or PINs based on this authentication rule never expire. Use of this check box is most applicable for low-security users or for accounts that can be accessed by more than one person. Note that when this check box is checked, the user is still able to change passwords or PINs at any time.

Table 11-6 Edit Authentication Rule Page (continued)

Field	Description
Expiration Warning Days	Enter the number of days before passwords or PINs expire that Cisco Unity Connection will warn users that a password or PIN is about to expire. A value of 0 (zero) means that Unity Connection will not warn users that a password or PIN is about to expire. Default setting: 0 days.
Minimum Credential Length	Enter the required number of digits for user passwords and PINs. In general, shorter passwords and PINs are easier to use, but longer passwords and PINs are more secure. We recommend requiring eight or more digits. When you change the minimum credential length, users are required to use the new length the next time that they change the password or PIN. Enter a value between 1 and 64 digits. Default setting: 8 digits.
Stored Number of Previous Credentials	Enter a value for the number of previous passwords or PINs that Cisco Unity Connection stores for a user. When a user enters a new password or PIN, Unity Connection compares it to the stored passwords or PINs, and rejects it if it matches a password or PIN in the history. A value of 0 (zero) means that Unity Connection does not store any previous passwords or PINs for the user. Default setting: 5 passwords or PINs.
Check for Trivial Passwords	Check this check box to have Cisco Unity Connection verify that a new password or PIN meets the following criteria when the passwords or PINs are changed by using Cisco Unity Connection Administration, the Unity Connection Messaging Assistant, or the Unity Connection conversation: • The digits are not all the same (for example, 9999). • The digits are not consecutive (for example, 1234 or 4321). • The password or PIN is not the same as the primary extension that is assigned to the user. In addition to checking this check box, consider providing users with a password or PIN policy that advises them to avoid specifying a password or PIN that: • Spells their first or last name, their organization or company name, or any other obvious words. • Contains their primary extension. • Is the reverse of their primary extension or contains the reverse of their primary extension. • Uses the same digits more than twice in a row (for example, 900012). • Is a 1-digit increment of a previous password or PIN (for example, 20185 to 20186). • Contains fewer than three different digits (for example, 18181).

See Also

Roles

Table 11-7 Roles Page

Field	Description
Name	The name of the administrative role. Select the role Name to go to the Edit Role page for the role.
Description	*(Display only)* A brief description of the role privileges.

See Also

- The "Roles in Cisco Unity Connection 9.x" section in the "Preparing to Add User Accounts in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Edit Role

Table 11-8 Edit Role Page

Field	Description
Name	The name of the administrative role.
Description	A brief description of the role privileges.
Role Assignments	Select Role Assignments to view a list of users that are assigned to the role. You can also remove users from the role, view a list of users not assigned to the role, and assign users to the role.
Role Privileges	*(Display only)* This table lists the privileges that the administrative role has rights to perform, including Create, View, Update, Delete, and Execute.

See Also

- The "Roles in Cisco Unity Connection 9.x" section in the "Preparing to Add User Accounts in Cisco Unity Connection 9.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx.html.

Search Restriction Tables

Table 11-9 Search Restriction Tables Page

Field	Description
Delete Selected	To delete a restriction table, check the check box to the left of the display name, and select Delete Selected. You can delete multiple restriction tables at once.
Display Name	*(Display only)* The name of the restriction table.

See Also

- The "Restriction Tables in Cisco Unity Connection 9.x" section in the "Call Management Overview in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The "Overview of Default Restriction Tables in Cisco Unity Connection 9.x" section in the "Managing Restriction Tables in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

New Restriction Table

Table 11-10 New Restriction Table Page

Field	Description
Display Name	Enter a descriptive name for the restriction table.
Maximum Length of Dial String	Enter the maximum number of digits—including access codes—in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits fewer than or equal to the Maximum Length of Dial String value are checked against the restriction table. Dial strings that contain more than the Maximum Length of Dial String value are not permitted. For example, if local calls in your area are seven digits long, and you want to prevent users from using long distance phone numbers, enter 8 in the Maximum Length of Dial String field. (A local number plus the access code for the phone system equals 8 digits.) Default setting: 30 digits.
Minimum Length of Dial String	Enter the minimum number of digits—including access codes—in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits greater than or equal to the Minimum Length of Dial String value are checked against the restriction table. Dial strings that contain fewer than the Minimum Length of Dial String value are not permitted. For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field. Default setting: 1 digit.

Table 11-10 New Restriction Table Page (continued)

Field	Description
New Restriction Patterns Are Blocked by Default	Indicate whether new restriction patterns should be flagged as Blocked by default. Default setting: Check box not checked.

See Also

- The "Creating Restriction Tables in Cisco Unity Connection 9.x" section in the "Managing Restriction Tables in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Edit Restriction Table Basics

Table 11-11 Edit Restriction Table Basics Page

Field	Description
Display Name	Enter a descriptive name for the restriction table.
Maximum Length of Dial String	Enter the maximum number of digits—including access codes—in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits fewer than or equal to the Maximum Length of Dial String value are checked against the restriction table. Dial strings that contain more than the Maximum Length of Dial String value are not permitted. For example, if local calls in your area are seven digits long, and you want to prevent users from using long distance phone numbers, enter 8 in the Maximum Length of Dial String field. (A local number plus the access code for the phone system equals 8 digits.) Default setting: 30 digits.
Minimum Length of Dial String	Enter the minimum number of digits—including access codes—in a call transfer, message notification, or fax delivery number. Only the dial strings that contain a number of digits greater than or equal to the Minimum Length of Dial String value are checked against the restriction table. Dial strings that contain fewer than the Minimum Length of Dial String value are not permitted. For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field. Default setting: 1 digit.
New Restriction Patterns are Blocked by Default	Indicate whether new restriction patterns should be flagged as Blocked by default. Default setting: Check box not checked.

Table 11-11 Edit Restriction Table Basics Page (continued)

Field	Description
Order	*(Display only)* Indicates the order in which the Unity Connection evaluates the pattern when applying the restriction table. Select Add New to add a new pattern, or Change Order to change the order of the patterns. Note that the order of the patterns is important. Cisco Unity Connection sequentially compares a phone number to the call patterns in the restriction table, starting with call pattern 0. If a number matches more than one call pattern, the number is permitted or restricted according to the first call pattern that it matches. The last pattern in the table always matches all numbers (*).
Blocked	Check this check box to have Cisco Unity Connection prohibit use of phone numbers that match the pattern.
Pattern	Enter specific numbers or patterns of numbers that can be permitted or restricted. Include external and long-distance access codes. Use digits 0 through 9 and the following special characters: • * to match zero or more digits. • ? to match exactly one digit. Each ? serves as a placeholder for one digit. • # to correspond to the # key on the phone. • + to call from one country to other country

See Also

- The "Modifying Restriction Tables in Cisco Unity Connection 9.x" section in the "Managing Restriction Tables in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Change Restriction Pattern Order

Table 11-12 Change Restriction Pattern Order Page

Field	Description
Change Restriction Pattern Order	To change the order of patterns in a restriction table, select the pattern in the list, then select the up or down arrow to move the pattern relative to the other patterns in the list. When you are done, select Save.

See Also

- The "Modifying Restriction Tables in Cisco Unity Connection 9.x" section in the "Managing Restriction Tables in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Licenses

Table 11-13 Licenses Page

Field	Description
License Status	(Display only) Demonstration (Demo): Unity Connection remains in the "Demo" mode until it connects to the ELM server for the first time. The "Demo" mode is available only for 60 days of grace period and then the license status changes to "Expire". Compliance: If the required number of licenses for the desired features are installed on the ELM server, the license status is "Compliance". Violation: If the required number of licenses for the desired features are not installed on the ELM server, the license status becomes "Violation". The "Violation" mode is available only for 60 days of grace period and then the license status changes to "Expire". Expire: If you do not obtain and install the required number of licenses for the desired features on the ELM server within the 60 days of grace period, the license status becomes "Expire". **Note** For more information on the ELM server and its configuration, refer to ELM user guide at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/elmuserguide/9_0_1/CUCM_BK_E596FD72_00_enterprise-license-manager-user-90.html
ELM server	(Display only) The Host name/IP address of the ELM server on which Unity Connection is configured.
Last connectivity time with ELM server	(Display only) The last time when the ELM server was synchronized with Unity Connection. Note that the value of the Last Connectivity Time with ELM Server will be in the Coordinated Universal Time (UTC) time zone.
Last compliance Time	(Display only) The last time when the Unity Connection was in Compliance mode. Note that the value of the Last Compliance Time will be in the Coordinated Universal Time (UTC) time zone.
Licensed Seats For	(Display only) The description of the Cisco Unity Connection licensed feature.
Feature Name	(Display only) The name of the Cisco Unity Connection licensed feature.
Current used	(Display only) The number of seats that are being used currently.

See Also

- The "Managing Licenses in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Search Schedules

Table 11-14 Search Schedules Page

Field	Description
Delete Selected	To delete a schedule, check the check box to the left of the display name, and select Delete Selected. You can delete multiple schedules at once.
Display Name	*(Display only)* The name of the schedule. Select the Display Name to edit the schedule.

See Also

- The "Schedules and Holidays in Cisco Unity Connection 9.x" section in the "Call Management Overview in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The "Overview of Default Schedules in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

New Schedule

Table 11-15 New Schedule Page

Field	Description
Display Name	Enter a descriptive name for the schedule.
Holiday Schedule	Select which Holiday schedule (if any) to apply to this schedule.

See Also

- The "Creating Schedules in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Edit Schedule Basics

Table 11-16 Edit Schedule Basics Page

Field	Description
Display Name	Enter a descriptive name for the schedule.
Holiday Schedule	Select which Holiday schedule (if any) to apply to this schedule.

Table 11-16 Edit Schedule Basics Page (continued)

Field	Description
Delete Selected	To delete a schedule, check the check box to the left of the display name, and select Delete Selected. You can delete multiple schedules at once.
Add New	To add a schedule, select the Add New button. A new page opens, on which you enter data applicable to the new schedule.
Name	*(Display only)* The name of the schedule detail. Select the name to go to the specific page for the schedule detail.
Start Time	*(Display only)* The time at which the schedule becomes active based on this schedule detail.
End Time	*(Display only)* The time at which the schedule becomes inactive based on this schedule detail.
Days Active	*(Display only)* The days on which the schedule is active based on this schedule detail.

See Also

- The "Modifying Schedules in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

New Schedule Detail

Table 11-17 New Schedule Detail Page

Field	Description
Name	Enter a descriptive name that other administrators will recognize when they work with this schedule.
Start Time	From the lists, select the hour, minute, and a.m. or p.m. designation at which the schedule becomes active.
End Time	From the lists, select the hour, minute, and a.m. or p.m. designation at which time the schedule becomes inactive. **Note** The end time must be later than the start time. To specify an end time of midnight (12:00 am), check the End of Day check box.
End of Day	Check this check box to specify that the schedule becomes inactive at midnight (the end of the day).
Active Every Day	Check this check box to make the schedule active every day of the week (including weekends) between the start time and end time that you specify for this schedule detail.
Active Weekdays	Check this check box to make the schedule active every week day (Monday through Friday, weekends excluded) between the start time and end time that you specify for this schedule detail.
Active Monday	Check this check box to make the schedule active each Monday between the start time and end time that you specify for this schedule detail.
Active Tuesday	Check this check box to make the schedule active each Tuesday between the start time and end time that you specify for this schedule detail.
Active Wednesday	Check this check box to make the schedule active each Wednesday between the start time and end time that you specify for this schedule detail.

Table 11-17 New Schedule Detail Page (continued)

Field	Description
Active Thursday	Check this check box to make the schedule active each Thursday between the start time and end time that you specify for this schedule detail.
Active Friday	Check this check box to make the schedule active each Friday between the start time and end time that you specify for this schedule detail.
Active Saturday	Check this check box to make the schedule active each Saturday between the start time and end time that you specify for this schedule detail.
Active Sunday	Check this check box to make the schedule active each Sunday between the start time and end time that you specify for this schedule detail.

See Also

Edit Schedule Detail

Table 11-18 Edit Schedule Detail Page

Field	Description
Name	Enter a descriptive name that other administrators will recognize when they work with this schedule.
Start Time	From the lists, select the hour, minute, and a.m. or p.m. designation at which the schedule becomes active.
End Time	From the lists, select the hour, minute, and a.m. or p.m. designation at which time the schedule becomes inactive. **Note** The end time must be later than the start time. To specify an end time of midnight (12:00 am), check the End of Day check box.
End of Day	Check this check box to specify that the schedule becomes inactive at midnight (the end of the day).
Active Every Day	Check this check box to make the schedule active every day of the week (including weekends) between the start time and end time that you specify for this schedule detail.
Active Weekdays	Check this check box to make the schedule active every week day (Monday through Friday, weekends excluded) between the start time and end time that you specify for this schedule detail.
Active Monday	Check this check box to make the schedule active each Monday between the start time and end time that you specify for this schedule detail.
Active Tuesday	Check this check box to make the schedule active each Tuesday between the start time and end time that you specify for this schedule detail.
Active Wednesday	Check this check box to make the schedule active each Wednesday between the start time and end time that you specify for this schedule detail.
Active Thursday	Check this check box to make the schedule active each Thursday between the start time and end time that you specify for this schedule detail.
Active Friday	Check this check box to make the schedule active each Friday between the start time and end time that you specify for this schedule detail.
Active Saturday	Check this check box to make the schedule active each Saturday between the start time and end time that you specify for this schedule detail.

Table 11-18 Edit Schedule Detail Page (continued)

Field	Description
Active Sunday	Check this check box to make the schedule active each Sunday between the start time and end time that you specify for this schedule detail.

See Also

- The "Modifying Schedules in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Search Holiday Schedules

Table 11-19 Search Holiday Schedules Page

Field	Description
Delete Selected	To delete a holiday schedule, check the check box to the left of the display name, and select Delete Selected. You can delete multiple holiday schedules at once.
Display Name	*(Display only)* The name of the holiday schedule. Select the Display Name to edit the schedule.

See Also

New Holiday Schedule

Table 11-20 New Holiday Schedule Page

Field	Description
Display Name	Enter a descriptive name for the holiday schedule.

See Also

- The "Designating Holidays in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Edit Holiday Schedule Basics

Table 11-21 Edit Holiday Schedule Basics Page

Field	Description
Display Name	Enter a descriptive name for the holiday schedule.
Delete Selected	To delete a holiday schedule, check the check box to the left of the display name, and select Delete Selected. You can delete multiple holiday schedules at once.
Add New	To add a holiday schedule, select the Add New button. A new page opens, on which you enter data applicable to the new holiday schedule.
Holiday Name	*(Display only)* The name of the holiday. Select the Holiday Name to edit the holiday.
Start Date	*(Display only)* The start date (month, day and year) when the holiday schedule begins to take effect.
End Date	*(Display only)* The last date (month, day, and year) on which the holiday schedule is in effect.
Start Time	*(Display only)* The start time when the holiday schedule takes effect on the Start Date and on each day thereafter until the End Date. A time of 12:00 a.m. indicates the start of the day.
End Time	*(Display only)* The end time when the holiday schedule is no longer in effect on the Start Date and each day thereafter until the End Date.

See Also

New Holiday

Table 11-22 New Holiday Page

Field	Description
Holiday Name	Enter a descriptive name for the range of dates you are defining for the holiday.
Start Date	From the lists, select the month, day, and year when the holiday schedule begins to take effect. To designate an entire single day as a holiday, select the day as the value for both the Start Date and End Date, select 12:00 a.m. for the Start Time, and check the End of Day check box.
End Date	From the lists, select the last date (month, day, and year) on which the holiday schedule is in effect.
Start Time	From the lists, select the hour, minute, and time of day (a.m. or p.m.) when the holiday schedule takes effect on the Start Date and each day thereafter until the End Date. A time of 12:00 a.m. indicates the start of the day. To configure a holiday to be in effect the entire day, set the Start Time to 12:00 a.m. and check the End of Day check box.

Table 11-22 New Holiday Page (continued)

Field	Description
End Time	From the lists, select the hour, minute, and time of day (a.m. or p.m.) when the holiday schedule is no longer in effect on the Start Date and on each day thereafter until the End Date. **Note** The end time must be later than the start time. To specify an end time of midnight (12:00 a.m. or 24:00), check the End of Day check box. To specify a range of days beginning at the Start Time on the Start Date and continuing until the End Time on the End Date, split the range into multiple holiday entries. For example, to start a holiday weekend on Friday January 1st at 5 p.m. (17:00) and end it on Monday January 4th at 8 a.m. (08:00), create one new holiday and set the Start Date and End Date to January 1st, set a Start Time of 5:00 p.m. and check the End of Day check box; create a second new holiday and set the Start Date to January 2nd and the End Date to January 3rd, set a Start Time of 12:00 a.m. and check the End of Day check box; and create a third new holiday with a Start Date and End Date of January 4th, a Start Time of 12:00 a.m. and an End Time of 8:00 a.m.
End of Day	Check this check box to specify that the schedule is in effect until the end of the day (midnight or 24:00) on the Start Date and on each day thereafter until the End Date. Uncheck this check box to specify an earlier time of day in the End Time field.

See Also

Edit Holiday

Table 11-23 Edit Holiday Page

Field	Description
Holiday Name	Enter a descriptive name for the range of dates you are defining for the holiday.
Start Date	From the lists, select the month, day, and year when the holiday schedule begins to take effect. To designate an entire single day as a holiday, select the day as the value for both the Start Date and End Date, select 12:00 a.m. for the Start Time, and check the End of Day check box.
End Date	From the lists, select the last date (month, day, and year) on which the holiday schedule is in effect.
Start Time	From the lists, select the hour, minute, and time of day (a.m. or p.m.) when the holiday schedule takes effect on the Start Date and each day thereafter until the End Date. A time of 12:00 a.m. indicates the start of the day. To configure a holiday to be in effect the entire day, set the Start Time to 12:00 a.m. and check the End of Day check box.

Table 11-23 Edit Holiday Page (continued)

Field	Description
End Time	From the lists, select the hour, minute, and time of day (a.m. or p.m.) when the holiday schedule is no longer in effect on the Start Date and on each day thereafter until the End Date. **Note** The end time must be later than the start time. To specify an end time of midnight (12:00 a.m. or 24:00), check the End of Day check box. To specify a range of days beginning at the Start Time on the Start Date and continuing until the End Time on the End Date, split the range into multiple holiday entries. For example, to start a holiday weekend on Friday January 1st at 5 p.m. (17:00) and end it on Monday January 4th at 8 a.m. (08:00), create one new holiday and set the Start Date and End Date to January 1st, set a Start Time of 5:00 p.m. and check the End of Day check box; create a second new holiday and set the Start Date to January 2nd and the End Date to January 3rd, set a Start Time of 12:00 a.m. and check the End of Day check box; and create a third new holiday with a Start Date and End Date of January 4th, a Start Time of 12:00 a.m. and an End Time of 8:00 a.m.
End of Day	Check this check box to specify that the schedule is be in effect until the end of the day (midnight or 24:00) on the Start Date and on each day thereafter until the End Date. Uncheck this check box to specify an earlier time of day in the End Time field.

See Also

- The "Designating Holidays in Cisco Unity Connection 9.x" section in the "Managing Schedules and Holidays in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Search Global Nicknames

Table 11-24 Search Global Nicknames Page

Field	Description
Delete Selected	To delete a nickname, check the check box to the left of the display name, and select Delete Selected. You can delete multiple nicknames at once.
Proper Name	The name for which one or more nicknames are defined. Select Proper Name to go to the specific page for the name.

See Also

- The "Voice Recognition: Global Nickname List in Cisco Unity Connection 9.x" section in the "Changing Conversation Settings for All Users in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

New Global Nickname

Table 11-25 New Global Nickname Page

Field	Description
Proper Name	Enter a name for which you want to define nicknames. The Proper Name appears in the Global Nickname list.
Nickname	Enter variations of the Proper Name. The names you enter here are included as part of the entry for the Proper Name that is displayed in the Global Nicknames list.

See Also

Edit Global Nickname

Table 11-26 Edit Global Nickname Page

Field	Description
Delete Selected	To delete a nickname, check the check box to the left of the nickname, and select Delete Selected. You can delete multiple nicknames at once.
Add New	To add a nickname, select the Add New button. A new row is added to the table, in which you can enter a new nickname.
Nickname	Enter variations of the Proper Name. The names you enter here are included as part of the entry for the Proper Name that is displayed in the Global Nicknames list.

See Also

- The "Voice Recognition: Global Nickname List in Cisco Unity Connection 9.x" section in the "Changing Conversation Settings for All Users in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Subject Line Formats

Table 11-27 Subject Line Formats Page

Field	Description
Language	Select the applicable language. Each language that you have installed on the system has a separate subject line format.
Outside Caller Messages	Enter the format for the subject line of messages from outside callers: those who are not Cisco Unity Connection users, and also Unity Connection users who send messages without first signing in to Unity Connection or who have not been automatically identified as Unity Connection users by the Identified User Messaging feature.

Table 11-27 Subject Line Formats Page (continued)

Field	Description
User to User Messages	Enter the format for the subject line of messages from callers who are Cisco Unity Connection users: those who have either signed in to Unity Connection, or who have been automatically identified as Unity Connection users because Identified User Messaging is enabled.
Interview Handler Messages	Enter the format for the subject line of messages from interview handlers.
Live Record Messages	Enter the format for the subject line of live record messages.
%CALLERID% (When Unknown)	Enter text to be used in subject lines when the caller ID of the sender of a message is not known. When the %CALLERID% parameter is used in a subject line format, it is automatically replaced with the ANI Caller ID of the sender of the message. If the ANI Caller ID is not available, the text that you enter in this field is inserted into the subject line instead. For example, if you enter Unknown Caller ID in this field, that text appears in the subject line. You can also leave this field blank.
%CALLEDID% (When Unknown)	Enter text to be used in subject lines when the number called by the sender of the message is not known. When the %CALLEDID% parameter is used in a subject line format, it is automatically replaced with the ID of the number called by the sender of the message. If the ID is not available, the text that you enter in this field is inserted into the subject line instead. For example, if you enter Unknown Called ID in this field, that text appears in the subject line. You can also leave this field blank.
%NAME% (When Unknown)	Enter text to be used in subject lines when both the display name and the ANI Caller Name of the sender of the message are not known. When the %NAME% parameter is used in the subject line format of an outside caller message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Cisco Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When the %NAME% parameter is used in the subject line format of a user to user message, it is automatically replaced with the display name of the sender of the message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When the %NAME% parameter is used in the subject line format of an interview handler message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Unity Connection inserts the display name of the interview handler. If the display name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When %NAME% is used in the Live Record Messages field, it is automatically replaced with the display name of the user who initiated the live record message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field.

Table 11-27 Subject Line Formats Page (continued)

Field	Description
%EXTENSION% (When Unknown)	Enter text to be used in subject lines when the extension of the sender of the message is not known. When the %EXTENSION% parameter is used in a subject line format, it is automatically replaced with the extension of the sender of the message, or for messages recorded by call handlers or interview handlers, with the extension of the handler. If the extension is not available, the text that you enter in this field is inserted into the subject line instead. For example, if you enter Unknown Extension in this field, that text appears in the subject line. You can also leave this field blank.
%U%	Enter text that is used in subject lines when a message is flagged as urgent. When the %U% parameter is used in a subject line format, it is automatically replaced with the text that you enter in this field if the message is flagged as urgent. If the message is not urgent, this parameter is omitted.
%P%	Enter text that is used in subject lines when a message is flagged as private. When the %P% parameter is used in a subject line format, it is automatically replaced with the text that you enter in this field if the message is flagged as private. If the message is not private, this parameter is omitted.
%S%	Enter text that is used in subject lines when a message is flagged as secure. When the %S% parameter is used in a subject line format, it is automatically replaced with the text that you enter in this field if the message is flagged as a secure message. If the message is not a secure message, this parameter is omitted.
%D%	Enter text that is used in subject lines when a message is flagged as a dispatch message. When the %D% parameter is used in a subject line format, it is automatically replaced with the text that you enter in this field if the message is flagged as a dispatch message. If the message is not a dispatch message, this parameter is omitted.

See Also

- The "Message Subject Line Formats in Cisco Unity Connection 9.x" and the "Types of Messages in Cisco Unity Connection 9.x" sections in the "Messaging in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Search TTS Descriptions of Message Attachments

Table 11-28 Search TTS Descriptions of Message Attachments Page

Field	Description
Language	Select the language of the descriptions that you want to see.
Delete Selected	To delete a message attachment, check the check box to the left of the display name, and select Delete Selected. You can delete multiple message attachments at once.
Add New	To add a message attachment, select the Add New button. A new page opens, on which you enter data applicable to the new message attachment.

Table 11-28 Search TTS Descriptions of Message Attachments Page (continued)

Field	Description
Extension	*(Display only)* The file extension of the message attachment for which the description applies. Select the file extension to edit the description.
Description	*(Display only)* The description that is read by Text to Speech (TTS).

See Also

New TTS Description of Message Attachments

Table 11-29 New TTS Description of Message Attachments Page

Field	Description
File Extension	Enter the file extension of the message attachment for which the description applies.
Description	Enter the description that will be read by Text to Speech (TTS).

See Also

Edit TTS Descriptions of Message Attachments

Table 11-30 TTS Descriptions of Message Attachments Page

Field	Description
File Extension	Enter the file extension of the message attachment for which the description applies.
Description	Enter the description that will be read by Text to Speech (TTS).

See Also

Enterprise Parameters

These fields do not apply to Cisco Unified Communications Manager or Cisco Unified Communications Manager Business Edition.

Table 11-31 Enterprise Parameters Page

Field	Description
Parameter Name	*(Display only)* The name of the enterprise parameter.
Parameter Value	Enter or select the value for the parameter.
Suggested Value	*(Display only)* The suggested parameter value.
Set to Default	Select the Set to Default button to set all enterprise parameters to the default values.

See Also

- The "Description of Enterprise Parameters in Cisco Unity Connection 9.x" section and the "Configuring Enterprise Parameters for Cisco Unified Serviceability Services in Cisco Unity Connection 9.x" section in the "Configuring Enterprise Parameters in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Service Parameters

These fields do not apply to Cisco Unified Communications Manager or Cisco Unified Communications Manager Business Edition.

Table 11-32 Service Parameters Page

Field	Description
Server	Select the name of the Cisco Unity Connection server.
Service	Select the service that contains the parameter that you want to update.
Parameter Name	*(Display only)* The name of the service parameter.
Parameter Value	Enter or select the value for the parameter.
Suggested Value	*(Display only)* The suggested parameter value.
Set to Default	Select the Set to Default button to set all service parameters for the service to the default values.

See Also

Search Plugins

These fields do not apply to Cisco Unified Communications Manager or Cisco Unified Communications Manager Business Edition.

Table 11-33 Search Plugins Page

Field	Description
Find	Select the Find button to display the available plugins.
Download	Select Download and follow the on-screen instructions to download and install a plugin.
Plugin Name	*(Display only)* The name of the plugin that is available to download and install.
Description	*(Display only)* The description of the plugin.

See Also

- The "Installing Plugins in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Edit Fax Server Configuration

Table 11-34 Edit Fax Server Configuration Page

Field	Description
Enabled	Check this check box to enable the connection from Cisco Unity Connection to the fax server. Uncheck this check box to disable the connection from Unity Connection to the fax server. Default setting: Check box not checked.
Fax Server Name	Enter a descriptive name for the fax server.
SMTP Address	Enter the address of the SMTP server.
IP Address	Enter the IP address of the SMTP server.
Use SMTP Smart Host	Check this check box if you are using an SMTP Smart Host. Note that you must also enter the SMTP address in the SMTP Address field. Uncheck this check box if you are not using an SMTP Smart Host.

See Also

LDAP Setup

Table 11-35 LDAP Setup Page

Field	Description
Enable Synchronizing from LDAP Server	Check this check box so that Cisco Unity Connection gets basic information on Unity Connection users from the LDAP directories that you specify on the LDAP Directory page. Data is synchronized only for the Unity Connection users that you created by importing users from the LDAP directory. Unity Connection does not automatically create new Unity Connection users when new users are added to the LDAP directory. If you want to use LDAP authentication, you must enable LDAP synchronization. When LDAP synchronization is enabled, you cannot change Unity Connection user data for the fields that were imported from the LDAP directory. You must change data in the LDAP directory and do one of the following to update the data in Unity Connection: • Manually resynchronize Unity Connection data with LDAP data by using the Perform Full Sync Now button on the LDAP Directory page. • If automatic resynchronization is configured on the LDAP Directory page, wait for the next automatic resynchronization to occur. Some LDAP directories support LDAP persistent search. When Unity Connection is integrated with an LDAP directory that supports persistent search, changes to the directory are replicated to the Unity Connection database immediately instead of being replicated when the next manual or automatic synchronization occurs.
LDAP Server Type	Select the type of LDAP server from which you want Cisco Unity Connection to get user data.

Table 11-35 LDAP Setup Page (continued)

Field	Description
LDAP Attribute for User ID	For LDAP users whose data is imported into Cisco Unity Connection, select the field in the LDAP directory that you want to appear in the Alias field in Unity Connection. Note the following considerations: • The field that you select must have a value for every user in the LDAP directory. • Every value for the field that you select must be unique. • Any LDAP user who does not have a value in the field that you select is not imported into Unity Connection. • If you are going to create new Unity Connection users by importing LDAP users, and if Unity Connection also already has users who will not be integrated with the LDAP directory, make sure that the users that you import from the directory do not have a value in the field that you select that matches the value in the Alias field for an existing Unity Connection user. • If you later need to change the field that you select now, and if you have already created LDAP configurations on the LDAP Directory page, you must delete all LDAP configurations, change the value here, and recreate all LDAP configurations. For more information, see the "Changing Which LDAP Field Is Mapped to the Alias Field in Unity Connection" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html. • You must use the same LDAP field for all LDAP directory configurations.

See Also

Find and List LDAP Directory Configurations

Table 11-36 Find and List LDAP Directory Configurations Page

Field	Description
Find LDAP Directory Where	To find the LDAP directories from which Cisco Unity Connection gets user data, enter the applicable specifications, and select Find.
Add New	To add an LDAP directory, select the Add New button. A new page opens, on which you enter data applicable to the new LDAP directory.

See Also

LDAP Directory Configuration

Table 11-37 LDAP Directory Configuration Page

Field	Description
LDAP Configuration Name	Enter a name for this LDAP configuration. If you are adding several LDAP configurations with different LDAP user search bases, enter a name that identifies the users in the current search base.
LDAP Manager Distinguished Name	Enter the name of an administrator account in the LDAP directory that has access to data in the LDAP user search base that you specify in the LDAP User Search Base field. Cisco Unity Connection uses this account to synchronize Unity Connection data with LDAP data. We recommend that you use an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set never to expire. (If the password for the administrator account changes, Unity Connection must be reconfigured with the new password.) If you create more than one configuration, we recommend that you create one administrator account for each configuration and give that account permission to read all user objects only within the corresponding subtree. When creating the configuration, you enter the full distinguished name for the administrator account; therefore the account can reside anywhere in the LDAP directory tree.
LDAP Password	Enter the password for the account that you specified in the LDAP Manager Distinguished Name field.
Confirm Password	Re-enter the password for the account that you specified in the LDAP Manager Distinguished Name field.

Table 11-37 LDAP Directory Configuration Page (continued)

Field	Description
LDAP User Search Base	Enter the location in the LDAP directory that contains the user data that you want to synchronize with Cisco Unity Connection user data. Unity Connection imports all users in the tree or subtree (domain or organizational unit) specified by the search base. A Unity Connection server or cluster can only import LDAP data from subtrees with the same directory root, for example, from the same Active Directory forest. **Using an LDAP Directory Other than Active Directory** If you are using an LDAP directory other than Microsoft Active Directory, and if you create a Unity Connection LDAP directory configuration that specifies the root of the directory as the user search base, Unity Connection will import data for every user in the directory. If the root of the directory contains subtrees that you do not want Unity Connection to access (for example, a subtree for service accounts), you should do one of the following: • Create two or more Unity Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Unity Connection to access. • Create one or more LDAP filters and specify them in LDAP directory configurations. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 9.x" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html. For directories other than Active Directory, we recommend that you specify user search bases that include the smallest possible number of users to speed synchronization, even when that means creating multiple configurations. **Using Active Directory** If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; Unity Connection does not follow Active Directory referrals during synchronization. The same is true for an Active Directory forest that contains multiple trees—you must create at least one configuration to access each tree. In this configuration, you must map the UserPrincipalName (UPN) attribute to the Unity Connection Alias field; the UPN is guaranteed by Active Directory to be unique across the forest. **Using Digital Networking** If you are using Digital Networking to network two or more Unity Connection servers that are each integrated with an LDAP directory, do not specify a user search base on one Unity Connection server that overlaps a user search base on another Unity Connection server, or you will have user accounts and mailboxes for the same Unity Connection user on more than one Unity Connection server. **Note** You can eliminate the potential for duplicate users by creating one or more LDAP filters on one or more Unity Connection servers. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 9.x" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Table 11-37 LDAP Directory Configuration Page (continued)

Field	Description
LDAP Custom Filter	Select one of the filters that you created on the System Settings > LDAP > LDAP Custom Filter page. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 9.x" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
Perform Sync Just Once	Check this check box to resynchronize user data in the Cisco Unity Connection database with user data in the LDAP directory one time, rather than at regular intervals. If you want to use LDAP authentication, uncheck this check box. When you check this check box, Unity Connection never resynchronizes with the LDAP directory based on values in the Perform a Re-sync Every <Interval> field or in the Next Re-sync Time field. If you have already created Unity Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Unity Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Unity Connection users. You must manually create new Unity Connection users by using either the Import Users tool or the Bulk Administration Tool.
Perform a Re-sync Every <Interval>	To resynchronize user data in the Cisco Unity Connection database with user data in the LDAP directory at regular intervals, specify the frequency with which you want the resynchronizations to occur. The minimum interval is six hours. When you specify a re-sync interval, we recommend that you: • Stagger synchronization schedules so that multiple LDAP configurations are not querying the same LDAP servers simultaneously. • Schedule synchronization to occur during nonbusiness hours. The first resynchronization occurs on the date and time specified in the Next Re-sync Time field. If you check the Perform Sync Just Once check box, these fields are unavailable, and resynchronization does not occur at the interval specified here. If you have already created Unity Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Unity Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Unity Connection users. You must manually create new Unity Connection users by using either the Import Users tool or the Bulk Administration Tool.
Next Re-sync Time (YYYY-MM-DD hh:mm)	Specify the date and time at which you next want Cisco Unity Connection to resynchronize data with the LDAP directory. After that resynchronization, Unity Connection resynchronizes at the interval specified in the Perform a Re-sync Every <Interval> field. If you check the Perform Sync Just Once check box, this field is unavailable, and resynchronization does not occur on the date and time specified here. If you have already created Unity Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Unity Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Unity Connection users. You must manually create new Unity Connection users by using either the Import Users tool or the Bulk Administration Tool.

Table 11-37 LDAP Directory Configuration Page (continued)

Field	Description
User ID	The value of the LDAP field that is listed here is stored in the Alias field in the Cisco Unity Connection database. The field that is listed here was specified on the LDAP Setup page, in the LDAP Attribute for User ID list. You can only change this value by deleting all LDAP configurations, changing the value on the LDAP Setup page, and recreating the LDAP configurations.
Middle Name	Select which value from the LDAP directory to store in the Cisco Unity Connection Middle Name field: • The value in the LDAP middleName field. • The value in the LDAP initials field.
Manager ID	The value of the manager field in the LDAP directory is always stored in the Manager ID field in the Cisco Unity Connection database.
Phone Number	Select which value from the LDAP directory to store in the Cisco Unity Connection Phone Number field: • The value in the LDAP telephoneNumber field. • The value in the LDAP ipPhone field.
First Name	The value of the givenName field in the LDAP directory is always stored in the First Name field in the Cisco Unity Connection database.
Last Name	The value of the sn field (surname) in the LDAP directory is always stored in the Last Name field in the Cisco Unity Connection database. **Caution** Every user that you want to import from the LDAP directory into Unity Connection must have a value in the LDAP sn field. Any LDAP user for whom the value of the sn attribute is blank will not be imported into the Unity Connection database.
Department	The value of the department field in the LDAP directory is always stored in the Department field in the Cisco Unity Connection database.
Mail ID	Select which value from the LDAP directory to store in the Cisco Unity Connection Corporate Email Address field (the value is temporarily stored in the Mail ID field in the Cisco Unified Communications Manager database on the Unity Connection server, which explains why the field name is Mail ID): Mail ID field: • The value in the LDAP mail field. • The value in the LDAP sAMAccountName field. If you are also configuring unified messaging for Exchange, we recommend that you choose the LDAP mail field. Depending on how you configure unified messaging, having the values from the LDAP mail field in the Unity Connection Corporate Email Address field can simplify configuring Unity Connection to access mailboxes in Exchange.

Table 11-37 LDAP Directory Configuration Page (continued)

Field	Description
Custom User Field Name	Cisco Unity Connection allows you to synchronize LDAP directory attributes that are not included among the defaults for the Standard User Fields to be Synchronized. Using Custom User Fields, you can synchronize LDAP attributes to a customized field that gets saved in the Unity Connection database. In the Custom User Field Name text box, enter a name for the customized field that you want to create. The custom user field can contain up to 64 alphanumeric characters, including spaces. Unity Connection saves the new customized field in the database. You can create up to five custom user fields. Click the (+) button to add additional rows on which you can create new fields.
LDAP Attribute	In the LDAP attribute field, enter a valid LDAP attribute that exists in your LDAP directory. The maximum field length is 128 characters.
Host Name or IP Address for Server	Enter the server name or the IP address of the LDAP server that you want Cisco Unity Connection to access when updating the Unity Connection database with changes to the LDAP directory. If you check the Use SSL check box, specify a host name in this field, or synchronization may fail.
LDAP Port	Enter the port on the LDAP server that Cisco Unity Connection should use to access the LDAP directory.
Use SSL	Check this check box to use SSL to encrypt data that is transmitted between the LDAP server and the Cisco Unity Connection server during synchronization. If you check this check box, specify a host name in the Host Name or IP Address for Server field, or synchronization may fail. To enable SSL encryption, you must also export SSL certificates from the applicable LDAP directory servers and upload the certificates on all Unity Connection servers. For more information, see the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
Add Another Redundant LDAP Server	Select this button and enter the applicable values to add one or more additional LDAP servers that contain the same data and that Cisco Unity Connection can access for resynchonization if the first specified LDAP server fails or is taken out of service for maintenance. This feature only works when you are using Active Directory for your LDAP directory.
Save	Select Save to save this configuration. After the first time you select Save, the Delete, Copy, Perform Full Sync Now, and Add New buttons appear.
Delete	Select to delete this configuration. This button is not available until after the first time you save this configuration.
Copy	Select to copy this configuration. This button is not available until after the first time you save this configuration.
Perform Full Sync Now	Select to resynchronize Cisco Unity Connection user data with user data in the LDAP directory. This button is not available until after the first time you save this configuration.
Add New	Select to add a new configuration, which allows you to synchronize Cisco Unity Connection data from additional LDAP user search bases. This button is not available until after the first time you save this configuration.

See Also

LDAP Authentication

Table 11-38 LDAP Authentication Page

Field	Description
Use LDAP Authentication for End Users	Check this check box so that Cisco Unity Connection web applications authenticate user names and passwords against the LDAP directory. When this check box is not checked, Unity Connection web applications authenticate user names and passwords against the user name and web application password in the Unity Connection database. When users sign in to Unity Connection by phone, Unity Connection always authenticates based on the voicemail password in the Unity Connection database, never based on any value in the LDAP directory.
LDAP Manager Distinguished Name	Enter the name of an administrator account in the LDAP directory that has access to data in the LDAP user search base that you specify in the LDAP User Search Base field. Cisco Unity Connection uses this account to authenticate user names and passwords that are entered in Unity Connection web applications against user data in the LDAP directory.
LDAP Password	Enter the password for the account that you specified in the LDAP Manager Distinguished Name field.
Confirm Password	Re-enter the password for the account that you specified in the LDAP Manager Distinguished Name field.
LDAP User Search Base	Enter the location in the LDAP directory that contains the user data that you want to use to authenticate user names and passwords that are entered in Cisco Unity Connection web applications. If you created more than one LDAP configuration, the user search base that you specify here must contain all of the user search bases that you specified in your LDAP configurations.
Host Name or IP Address for Server	Enter the server name or the IP address of the LDAP server that you want to use to authenticate user names and passwords that are entered in Cisco Unity Connection web applications. If you are configuring SSL, specify a host name in this field, or authentication will probably fail for IMAP clients. If you specify an IP address and the SSL certificate identifies the LDAP server only by host name (which is common; certificates rarely include the IP address of a server), Unity Connection cannot verify the identity of the LDAP server. When you are using Active Directory for your LDAP directory, we highly recommend that you specify an Active Directory global catalog server for much faster response times and for greater reliability. If you change this value, and if IMAP clients are accessing Unity Connection, restart the Unity Connection IMAP Server service. If other web applications are accessing Unity Connection (for example, Cisco Personal Communications Assistant), restart the server.
LDAP Port	Enter the port on the LDAP server that Cisco Unity Connection should use to access the LDAP directory. If you are using Active Directory for your LDAP directory and if you specified an Active Directory global catalog server in the Host Name or IP Address for Server, specify: • 3268 if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server. • 3269 if you are using SSL.

Table 11-38 LDAP Authentication Page (continued)

Field	Description
Use SSL	Check this check box to use SSL to encrypt the user name and password that are transmitted between the Cisco Unity Connection server and the LDAP server during authentication. If you check this check box, specify a host name in the Host Name or IP Address for Server field, or authentication will probably fail for IMAP clients. If you specify an IP address and the SSL certificate identifies the LDAP server only by host name (which is common; certificates rarely include the IP address of a server), Unity Connection cannot verify the identity of the LDAP server. To enable SSL encryption, you must also export SSL certificates from the applicable LDAP directory servers and upload the certificates on all Unity Connection servers. For more information, see the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
Add Another Redundant LDAP Server	Select this button and enter the applicable values to add one or more additional LDAP servers that contain the same data and that Cisco Unity Connection can access for authentication if the first specified LDAP server fails or is taken out of service for maintenance. This feature only works when you are using Active Directory for your LDAP directory.

See Also

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 9.x Users with LDAP Users" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Phone Number Conversion

Table 11-39 Phone Number Conversion Page (Cisco Unity Connection 8.5 and Later Only)

Field	Description
Regular Expression for LDAP Phone Number Pattern	Enter a regular expression to specify which phone numbers to operate on (for example, phone numbers that are 10 digits long) and the portion of the phone numbers to use as a basis for the extensions (for example, the last four digits).
Replacement Pattern	Enter a replacement pattern that specifies whether to use the values selected by the regular expression, or to perform additional operations (for example, to prepend an 8). ⚠ **Caution** Unity Connection validates the syntax of the regular expression but does not validate the replacement pattern, and also cannot validate the result of the regular expression and the replacement pattern. We recommend that you verify the results on the Import Users page of Connection Administration before you create Unity Connection subscribers.

See Also

Find and List LDAP Filters

Table 11-40 Find and List LDAP Filters Page (Cisco Unity Connection 8.5 and Later Only)

Field	Description
Find LDAP Custom Filter Where	To find LDAP filters, enter the applicable specifications, and select Find. To add a search criterion, select +. Multiple search criteria are Anded together; a filter must match all criteria to be displayed when you select Find. To remove the last search criterion, select –. To remove all search criteria except the first, select Clear Filter. To create a new filter by copying an existing filter, select the icon in the Copy column for the filter that you want to copy. This causes the LDAP Filter Configuration page to appear with the name and text of the selected filter. You must change the name of the new filter before you can save it.
Add New	To add an LDAP custom filter, select the Add New button. A new page opens, on which you enter data applicable to the new LDAP filter.

See Also

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 9.x Users with LDAP Users" section in the "Integrating Cisco Unity Connection 9.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

SMTP Server Configuration

Table 11-41 SMTP Server Configuration Page

Field	Description
SMTP Port #	*(Display only)* The port that Cisco Unity Connection uses for incoming and outgoing SMTP connections. Unity Connection uses SMTP for sending text message notifications; communicating with clients that send or receive voice, fax and text messages from Unity Connection; and communicating with VPIM locations and other digitally networked Unity Connection servers.

Table 11-41 SMTP Server Configuration Page (continued)

Field	Description
SMTP Domain	The domain name that Cisco Unity Connection uses to route messages between digitally networked Unity Connection servers and to construct the SMTP address of the sender on outgoing SMTP messages. For each user, Unity Connection creates an SMTP address of <Alias>@<SMTP Domain>. This SMTP address is displayed on the Edit User Basics page for the user. Examples of outgoing SMTP messages that use this address format include messages sent by users on this server to recipients on other digitally networked Unity Connection servers and messages that are sent from the Unity Connection phone interface or Messaging Inbox and relayed to an external server based on the Message Actions setting of the recipient. Unity Connection also uses the SMTP Domain to create sender VPIM addresses on outgoing VPIM messages, and to construct the From address for notifications that are sent to SMTP notification devices. When Unity Connection is first installed, the SMTP Domain is automatically set to the fully qualified host name of the server. Make sure that the SMTP domain of Cisco Unity Connection is different from the Corporate Email domain to avoid issues in message routing for Cisco Unity Connection. Some scenarios in which you may encounter issues with the same domain are listed below: • Routing of the voice messages between digitally networked Connection servers • Relaying of the messages • Replying and Forwarding of the voice messages using ViewMail for Outlook • Routing of the SpeechView messages to Cisco Unity Connection server • Sending the SMTP message Notifications • Routing of the VPIM messages **Note** Cisco Unity Connection requires a unique SMTP domain for every user, which is different from the corporate email domain.Due to same domain name configuration on Microsoft Exchange and Cisco Unity Connection, the users who are configured for Unified Messaging may face issues in adding recipient while composing, replying and forwarding of messages. For more information on resolving domain name configuration issues, see “Resolving SMTP Domain Name Configuration Issues” section of "Configuring Cisco Unity Connection 8.5 and Later and Microsoft Exchange for Unified Messaging" chapter in the Unified Messaging Guide for Cisco Unity Connection at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/unified_messaging/guide/9xcucumgx.html

Table 11-41 SMTP Server Configuration Page (continued)

Field	Description
Change SMTP Domain	Select this button to change the value of the SMTP Domain field. When changing the value, note the following considerations: • Confirm that the new SMTP Domain is entered in a valid domain format and can be resolved to the Cisco Unity Connection server by any SMTP servers that validate the sending domain or by an SMTP smart host if you use one to route messages to the Unity Connection server. • Each Unity Connection server in a Digital Network must have a unique SMTP Domain. • After you change the SMTP domain, you must restart the Unity Connection Conversation Manager, Unity Connection Message Transfer Agent, and Unity Connection SMTP Server services in Cisco Unity Connection Serviceability. If this server is in a Unity Connection cluster, you must restart all three services on both servers. To change the SMTP domain, do the following: 1. Navigate to System Settings> SMTP Configuration> Server> Change SMTP domain. 2. On the Cisco Unified Serviceability page, first stop and then start the following services: – Conversation manger STOP/START – Message transfer agent STOP/START – SMTP Server STOP/START
Limit Number of Simultaneous Incoming Connections	*(Cisco Unity Connection 8.5 and later)* Enter the maximum number of SMTP clients that can be connected to the Cisco Unity Connection SMTP server at one time for sending messages. Default setting: 20 connections.
Limit Number of Simultaneous Outgoing Connections *(Cisco Unity Connection 8.5 and later only)*	Enter the maximum number of outgoing connections that the Cisco Unity Connection SMTP server can have open with other SMTP servers at one time. Default setting: 2 connections.
Limit Size of Message	Enter the maximum size of message that clients can send to Cisco Unity Connection by using SMTP. Default setting: 10,000 kilobytes (approximately 10 megabytes).
Limit Messages Accepted per SMTP Session	Enter the maximum number of messages that a client can send to Cisco Unity Connection in a single SMTP session. Default setting: 10 messages.
Limit Number of Recipients per Message	Enter the maximum number of recipients allowed for a single message that is sent by a client to Cisco Unity Connection by using SMTP. Default setting: 15,000 recipients.

Table 11-41 SMTP Server Configuration Page (continued)

Field	Description
Delivery Retry Timeout	Check the Override Default check box and enter a value between 0 and 10800 in the Minutes field to have Cisco Unity Connection periodically retry the delivery of SMTP messages that have failed because of issues that may be temporary (for example, the remote SMTP server is not responding). When this check box is checked and a value greater than 0 is entered, Unity Connection retries once a minute until the message is successfully sent or the timeout interval specified in the Minutes field has passed. If the timeout has passed without success, Unity Connection sends a non-delivery receipt to the sender. Default setting: 0 minutes (Unity Connection immediately sends a non-delivery receipt to the sender and does not retry delivery of failed SMTP messages). **Note** The system default Delivery Retry Timeout value may be subject to change in later releases. If you override the default value with a custom Minutes value, the custom value will be retained in any upgrades.
Allow Connections from Untrusted IP Addresses	When this check box is checked, Cisco Unity Connection allows SMTP connections from clients or servers whose IP addresses do not match any address pattern that is configured on the IP Address Access List. When this check box is not checked, Unity Connection denies SMTP connection requests from clients or servers whose IP addresses do not match any address pattern that is configured on the IP Address Access List. Default setting: Check box not checked.
Require Authentication from Untrusted IP Addresses	When this check box is checked, Cisco Unity Connection requires authentication for SMTP connections from clients or servers whose IP addresses do not match any address pattern that is configured on the IP Address Access List. When this check box is not checked, Unity Connection allows these types of clients to connect without authenticating. This option is unavailable when the Allow Connections from Untrusted IP Addresses check box is not checked.
Transport Layer Security from Untrusted IP Addresses Is	Select how Cisco Unity Connection handles Transport Layer Security (TLS) with a client or server that attempts to connect from an IP address that does not match any address pattern configured on the IP Address Access List. • Disabled—Unity Connection does not offer TLS as an option for SMTP sessions initiated by clients or servers with untrusted IP addresses. In most cases, if the client is configured to use TLS, but Unity Connection does not offer it, the connection fails and the client notifies the user. • Required—Clients or servers connecting from untrusted IP addresses must use TLS to initiate SMTP sessions with the Unity Connection server. • Optional—Clients or servers connecting from untrusted IP addresses can use TLS to initiate SMTP sessions with the Unity Connection server, but are not required to do so. This option is unavailable when the Allow Connections from Untrusted IP Addresses check box is not checked.

See Also

- The "Setting Up SMTP Message Notifications in Cisco Unity Connection 9.x" section in the "Setting Up SMTP and SMS (SMPP) Message Notifications in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The "Configuring IMAP Settings in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

Search IP Address Access List

Table 11-42 Search IP Address Access List Page

Field	Description
Delete Selected	To delete an IP address, check the check box to the left of the IP address, and select Delete Selected. You can delete multiple IP addresses at once.
Add New	To add an IP address, select the Add New button. A new page opens, on which you enter data applicable to the new IP address.
IP Address	*(Display only)* A unique IP address or an IP address pattern that Cisco Unity Connection uses to allow or deny SMTP connections from SMTP clients or servers.
Allow Connection	When this check box is checked, Cisco Unity Connection allows SMTP connections from any client or server whose IP address matches this address pattern. When this check box is not checked, Cisco Unity Connection denies SMTP connections from any client or server whose IP address matches this address pattern.

See Also

- The "Configuring IMAP Settings in Cisco Unity Connection 9.x" chapter and the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The "Setting Up a Cisco Unity Connection 9.x Site" section in the "Setting Up Networking Between Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.
- The "Setting Up Networking Between Cisco Unity and Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.

New Access IP Address

Table 11-43 New Access IP Address Page

Field	Description
IP Address	Enter the IP address of a client or server that should be specifically allowed or denied access to the Cisco Unity Connection SMTP server. **Note** You can enter a single * (asterisk) to match all possible IP addresses.

See Also

- The "Configuring IMAP Settings in Cisco Unity Connection 9.x" chapter and the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.
- The "Setting Up a Cisco Unity Connection 9.x Site" section in the "Setting Up Networking Between Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.
- The "Setting Up Networking Between Cisco Unity and Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.

Access IP Address

Table 11-44 Edit Access IP Address Page

Field	Description
IP Address	Enter the IP address of a client or server that should be specifically allowed or denied access to the Cisco Unity Connection SMTP server. **Note** You can enter a single * (asterisk) to match all possible IP addresses.
Allow Connection	When this check box is checked, Cisco Unity Connection allows SMTP connections from any client or server whose IP address matches this address pattern. When this check box is not checked, Cisco Unity Connection denies SMTP connections from any client or server whose IP address matches this address pattern.

See Also

- The "Configuring IMAP Settings in Cisco Unity Connection 9.x" chapter and the "Configuring Transcription (SpeechView) in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.

- The "Setting Up a Cisco Unity Connection 9.x Site" section in the "Setting Up Networking Between Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.
- The "Setting Up Networking Between Cisco Unity and Cisco Unity Connection 9.x Servers" chapter of the *Networking Guide for Cisco Unity Connection Release 9x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/networking/guide/9xcucnetx.html.

Smart Host

Table 11-45 Smart Host Page

Field	Description
Smart Host	Enter the IP address or fully qualified domain name of the SMTP smart host through which Cisco Unity Connection relays SMTP messages. (Enter the fully qualified domain name of the server only if DNS is configured.) Unity Connection relays all SMTP notifications through the smart host. You can configure Unity Connection to relay voicemail, email, fax, or delivery receipt messages that it receives for a particular user to an SMTP address through the smart host. You can also configure Unity Connection to route SMTP messages for VPIM locations or for other digitally networked Unity Connection servers through the smart host; you may need to do this if, for example, a firewall prevents direct SMTP communication with the remote voice messaging system.

See Also

- The "Setting Up SMTP Message Notifications in Cisco Unity Connection 9.x" section in the "Setting Up SMTP and SMS (SMPP) Message Notifications in Cisco Unity Connection 9.x" chapter of the *System Administration Guide for Cisco Unity Connection Release 9.x*, available at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/administration/guide/9xcucsagx.html.