CHAPTER 10

# System Settings

See the following sections:

# Edit General Configuration

*Table 10-1 Edit General Configuration Page*

| Field | Description |
|---|---|
| Time Zone | Select the default time zone for the server. The default time zone setting is used to determine 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. |
| System Default Language | Select the default language in which system prompts are played to users and callers.<br>**Note** Depending on your license settings, United States English may not be available. |
| System Default TTS Language | Select the default language that users hear when having their email read to them by phone. 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.<br>**Note** Depending on your license settings, United States English may not be available. |
| Recording Format | Click the default format (or codec) for recorded messages.<br>Default setting: G.711 Mu-Law. |

*Table 10-1 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.<br>Default setting: 90 seconds. |
| Automatic Gain Control (AGC) Target Decibels | If automatic gain control (AGC) is enabled, enter the average volume, in decibels, that Cisco Unity Connection automatically maintains for recording voice messages and user greetings.<br>The AGC decibel levels are set in negative numbers. For example, –26 db is louder than –45 db.<br>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.)<br>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.)<br>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:<br>• Send a Non-Deliverable Receipt—Connection responds to the message sender with a non-delivery receipt (NDR).<br>• Relay Message to Smart Host—Connection relays the message to the smart host for delivery to a different server.<br>**Note** You configure the SMTP smart host on the System Settings > SMTP Configuration > Smart Host page.<br>Default setting: Send a Non-Deliverable Receipt. |

# Find and List Servers

*Table 10-2 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 click Delete Selected. You can delete multiple servers at once. |
| Add New | To add a server, click 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 Connection cluster. If Connection is not configured for a cluster, this field displays the host name or IP address of the local Connection server. |
| Description | *(Display only)* A description of the Cisco Unity Connection server in a Connection cluster. |

### See Also

- The "Configuring a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*.

# Server Configuration

**Revised May 2009**

***Table 10-3 Server Configuration Page***

| Field | Description |
|---|---|
| Database Replication | *(Display only)* The role of the Cisco Unity Connection server (publisher or subscriber) in a Connection cluster. |
| Host Name/IP Address | Enter the host name or IP address of the Cisco Unity Connection server in a Connection cluster. |
| IPv6 Name | *(Cisco Unity Connection 7.1 or later)* If IPv6 is enabled, enter the host name or IPv6 address of the Cisco Unity Connection server in a Connection cluster. |
| MAC Address | *(Optional)* Enter the MAC address of the Cisco Unity Connection server in a Connection cluster. |
| Description | *(Optional)* Enter a description of the Cisco Unity Connection server in a Connection cluster. |

### See Also

- The "Configuring a Cisco Unity Connection Cluster" chapter of the *Cluster Configuration and Administration Guide for Cisco Unity Connection*.

# Search External Services

***Table 10-4 Search External Services Page***

| Field | Description |
|---|---|
| Delete Selected | To delete an external service, check the check box to the left of the display name, and click Delete Selected. You can delete multiple external services at once. |
| Add New | To add an external service, click the Add New button. A new page opens, on which you enter data applicable to the new external service. |
| Display Name | *(Display only)* The name of the external service. |
| Server Type | *(Display only)* The type of server to which the external service connects. |

### See Also

- The "Configuring Access to Emails in an External Message Store" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Creating Calendar Integrations" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New External Service

**Revised May 2009**

***Table 10-5 New External Service Page***

| Field | Description |
|---|---|
| Type | Click the type of server to which the external service connects. |
| Enabled | When the Enabled check box is checked, this external service can be used to do the following:<br>• Access messages from an Exchange message store.<br>• Access data from a conferencing server such as Cisco Unified MeetingPlace.<br>When the check box is not checked, access to the Exchange message store or the conferencing server fails. In Cisco Personal Communications Assistant, when the user tries to import contacts from Exchange, the error message "Import Contacts from Exchange Server Failed" appears. Attempts to access Exchange or a conferencing server by other methods fail without an error message. |
| Display Name | Enter a descriptive name for the external service.<br>You select this descriptive name when configuring users for external services. |
| Server | Enter the server name or the fully qualified domain name of the server to which the external service connects.<br>If you select SSL for Security Transport, the value of this field must match the server name as it appears in the SSL certificate. |
| Authentication Mode | *(Exchange only)* Click the applicable setting to match the authentication mode that is used by the Exchange server. |
| Transfer Extension Dial String | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* Enter the digits that Cisco Unity Connection must dial to transfer users on the phone to the opening greeting of the Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express server. |
| Security Transport Type | Select one of the following:<br>• None—Select this option only when you are not configuring SSL to secure network traffic between Cisco Unity Connection and an external service such as Exchange or Cisco Unified MeetingPlace.<br>• SSL—Select this option when you are configuring SSL to secure network traffic between Cisco Unity Connection and an external service such as Exchange or Cisco Unified MeetingPlace. We recommend using this setting. |

*Table 10-5 New External Service Page (continued)*

| Field | Description |
|---|---|
| Validate Server Certificate | When this check box is checked, Cisco Unity Connection validates the server certificate for the external service.<br><br>**Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of the Server field. Otherwise, validation of the server certificate will fail.<br><br>The root certificate (or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate) must be installed as Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.<br><br>When this check box is not checked, Connection does not validate the server certificate for the external service.<br><br>This check box is enabled only when the Security Transport Type field is set to SSL. |
| Alias | Enter the following:<br>• *(Cisco Unified MeetingPlace Express)* The Windows domain alias for the API user that Cisco Unity Connection uses to log on to the Cisco Unified MeetingPlace Express server.<br>• *(Cisco Unified MeetingPlace)* The Windows domain alias for the privileged service account that Connection uses to log on to the Cisco Unified MeetingPlace server.<br>• *(Exchange 2003)* The Windows domain alias for the privileged service account that Connection uses to log on to the Exchange 2003 server.<br><br>Enter only the alias; do not prefix the alias with the Windows domain name. |
| Password | Enter the following:<br>• *(Cisco Unified MeetingPlace Express)* The password for the API user that Cisco Unity Connection uses to log on to the Cisco Unified MeetingPlace Express server.<br>• *(Cisco Unified MeetingPlace)* The password for the privileged service account that Connection uses to log on to the Cisco Unified MeetingPlace server.<br>• *(Exchange 2003)* The password for the privileged service account that Connection uses to log on to the Exchange 2003 server. |
| User Access to Calendar | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* When this check box is checked, users hear notification of upcoming meetings on the phone.<br><br>When this check box is not checked, users do not hear notification of upcoming meetings. |

*Table 10-5 New External Service Page (continued)*

| Field | Description |
|---|---|
| User Access to Calendar and Personal Contacts | *(Exchange 2007 and Exchange 2003 only)* When this check box is checked, users hear notification of upcoming meetings on the phone, and they are able to access their personal contacts for personal call transfer rules.<br>When this check box is not checked, users do not hear notification of upcoming meetings, and they are not able to access their personal contacts. |
| MeetingPlace Scheduling and Joining | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* When this check box is checked, users are able to schedule and join meetings.<br>When this check box is not checked, users are not able to schedule and join meetings. |
| User Access to Email in Third-Party Message Store | *(Exchange only)* When this check box is checked, users are able to access Exchange messages.<br>When this check box is not checked, users are not able to access Exchange messages. |
| Test | To test the configuration for the external service, click the Test button. The Task Execution Results window appears with the test results. |

**See Also**

- The "Configuring Access to Emails in an External Message Store" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Creating Calendar Integrations" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit External Service

**Revised May 2009**

*Table 10-6 Edit External Service Page*

| Field | Description |
|---|---|
| Type | *(Display only)* The type of server to which the external service connects. |
| Enabled | *(Display only)* When the Enabled check box is checked, this external service can be used to do the following:<br>• Access messages from an Exchange message store.<br>• Access data from a conferencing server such as Cisco Unified MeetingPlace.<br>When the check box is not checked, access to the Exchange message store or the conferencing server fails. In Cisco Personal Communications Assistant, when the user tries to import contacts from Exchange, the error message "Import Contacts from Exchange Server Failed" appears. Attempts to access Exchange or a conferencing server by other methods fail without an error message. |
| Display Name | Enter a descriptive name for the external service.<br>You select this descriptive name when configuring users for external services. |

*Table 10-6 Edit External Service Page (continued)*

| Field | Description |
|---|---|
| Server | Enter the server name or the fully qualified domain name of the server to which the external service connects.<br><br>If you select SSL for Security Transport, the value of this field must match the server name as it appears in the SSL certificate. |
| Authentication Mode | *(Exchange only)* Click the applicable setting to match the authentication mode that is used by the Exchange server. |
| Transfer Extension Dial String | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* Enter the digits that Cisco Unity Connection must dial to transfer users on the phone to the opening greeting of the Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express server. |
| Security Transport Type | Select one of the following:<br><br>• None—Select this option only when you are not configuring SSL to secure network traffic between Cisco Unity Connection and an external service such as Exchange or Cisco Unified MeetingPlace.<br><br>• SSL—Select this option when you are configuring SSL to secure network traffic between Cisco Unity Connection and an external service such as Exchange or Cisco Unified MeetingPlace. We recommend using this setting. |
| Validate Server Certificate | When this check box is checked, Cisco Unity Connection validates the server certificate for the external service.<br><br>⚠ **Caution** The CN value on the server certificate subject line or the subjectAltName:dnsname field of the server certificate must match the setting of the Server field. Otherwise, validation of the server certificate will fail.<br><br>The root certificate (or all certificates in a root certificate chain of the Certification Authority (CA) that signed the server certificate) must be installed as Connection-trust certificates in Cisco Unified Operating System Administration. Otherwise, validation of the server certificate will fail.<br><br>When this check box is not checked, Connection does not validate the server certificate for the external service.<br><br>This check box is enabled only when the Security Transport Type field is set to SSL. |

*Table 10-6 Edit External Service Page (continued)*

| Field | Description |
|---|---|
| Alias | Enter the following:<br>• *(Cisco Unified MeetingPlace Express)* The Windows domain alias for the API user that Cisco Unity Connection uses to log on to the Cisco Unified MeetingPlace Express server.<br>• *(Cisco Unified MeetingPlace)* The Windows domain alias for the privileged service account that Connection uses to log on to the Cisco Unified MeetingPlace server.<br>• *(Exchange 2003)* The Windows domain alias for the privileged service account that Connection uses to log on to the Exchange 2003 server.<br>Enter only the alias; do not prefix the alias with the Windows domain name. |
| Password | Enter the following:<br>• *(Cisco Unified MeetingPlace Express)* The password for the API user that Cisco Unity Connection uses to log on to the Cisco Unified MeetingPlace Express server.<br>• *(Cisco Unified MeetingPlace)* The password for the privileged service account that Connection uses to log on to the Cisco Unified MeetingPlace server.<br>• *(Exchange 2003)* The password for the privileged service account that Connection uses to log on to the Exchange 2003 server. |
| User Access to Calendar | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* When this check box is checked, users hear notification of upcoming meetings on the phone.<br>When this check box is not checked, users do not hear notification of upcoming meetings. |
| User Access to Calendar and Personal Contacts | *(Exchange 2007 and Exchange 2003 only)* When this check box is checked, users hear notification of upcoming meetings on the phone, and they are able to access their personal contacts for personal call transfer rules.<br>When this check box is not checked, users do not hear notification of upcoming meetings, and they are not able to access their personal contacts. |
| MeetingPlace Scheduling and Joining | *(Cisco Unified MeetingPlace and Cisco Unified MeetingPlace Express only)* When this check box is checked, users are able to schedule and join meetings.<br>When this check box is not checked, users are not able to schedule and join meetings. |
| User Access to Email in Third-Party Message Store | *(Exchange only)* When this check box is checked, users are able to access Exchange messages.<br>When this check box is not checked, users are not able to access Exchange messages. |
| Test | To test the configuration for the external service, click the Test button. The Task Execution Results window appears with the test results. |

### See Also

- The "Configuring Access to Emails in an External Message Store" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Creating Calendar Integrations" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Authentication Rules

*Table 10-7 Search Authentication Rules Page*

| Field | Description |
|---|---|
| Limit Search To | *(Applicable to standalone configurations only.)* Select the criteria by which to limit the display of search results:<br>• All—Display all search results, regardless of the Cisco Unity Connection location to which they belong.<br>• Location—Display only results that belong to a particular 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. Click 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 click Delete Selected. You can delete multiple authentication rules at once. |
| Add New | To add an authentication rule, click the Add New button. A new page opens, on which you enter data applicable to the authentication rule. |

**See Also**

- The "Specifying Password, Logon, and Lockout Policies" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Authentication Rule

*Table 10-8 New Authentication Rule Page*

| Field | Description |
|---|---|
| Display Name | Enter a descriptive name for the authentication rule. |
| Failed Logon ____ Attempts | Enter the number of failed logon attempts after which users cannot access Cisco Unity Connection.<br>When set to 0 (zero), there is no limit to the number of failed logon attempts, and the user is not locked out of the account.<br>Default setting: 3 attempts. |
| No Limit for Failed Logons | Check this check box so that there is no limit to the number of failed logon attempts, and the user is not locked out of the account. |
| Reset Failed Logon Attempts Every ____ Minutes | Enter the number of minutes after which Cisco Unity Connection clears the count of failed logon attempts (unless the failed logon limit is already reached and the account is locked).<br>When set to 0 (zero), a failed logon attempt results in the user account being locked until manually unlocked by an administrator.<br>Default setting: 30 minutes. |

*Table 10-8 New Authentication Rule Page (continued)*

| Field | Description |
|---|---|
| Lockout Duration ____ Minutes | Enter the number of minutes that a user account remains locked after the number of allowed Failed Logon attempts has been reached. While the account is locked, Cisco Unity Connection prevents the user from accessing Connection by phone.<br>If a value of 0 (zero) is entered, the account remains locked until manually unlocked by the administrator.<br>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.<br>Default setting: 1440 minutes (1 day). |
| Credential Expires After ____ Days | Default setting: 180 days. |
| Never Expires | Check this check box so that passwords 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 at any time. |
| Expiration Warning Days | Enter the number of days before passwords expire that Cisco Unity Connection will warn users that a password is about to expire.<br>A value of 0 (zero) means that Connection will not warn users that a password is about to expire.<br>Default setting: 0 days. |
| Minimum Credential Length | Enter the required number of digits for user passwords. In general, shorter passwords are easier to use, but longer passwords are more secure. We recommend requiring eight or more digits.<br>When you change the minimum credential length, users are required to use the new length the next time that they change their passwords.<br>A value of 0 (zero) means that blank passwords are permitted.<br>Default setting: 6 digits. |
| Stored Number of Previous Credentials | Enter a value for the number of previous passwords that Cisco Unity Connection stores for a user. When a user enters a new password, Connection compares it to the stored passwords, and rejects it if it matches a password in the history.<br>A value of 0 (zero) means that Connection does not store any previous passwords for the user.<br>Default setting: 5 passwords. |

*Table 10-8 New Authentication Rule Page (continued)*

| Field | Description |
|---|---|
| Check for Trivial Passwords | Check this check box to have Cisco Unity Connection verify that a new password meets the following criteria when user phone passwords are changed by using Cisco Unity Connection Administration, the Cisco Unity Assistant, or the Connection conversation:<br>• The digits are not all the same (for example, 9999).<br>• The digits are not consecutive (for example, 1234 or 4321).<br>• The password is not the same as the primary extension that is assigned to the user.<br>In addition to checking this check box, consider providing users with a password policy that advises them to avoid specifying a password that:<br>• Spells their first or last name, their organization or company name, or any other obvious words.<br>• Contains their primary extension.<br>• Is the reverse of their primary extension or contains the reverse of their primary extension.<br>• Uses the same digits more than twice in a row (for example, 900012).<br>• Is a 1-digit increment of a previous password (for example, 20185 to 20186).<br>• Contains fewer than three different digits (for example, 18181). |

**See Also**

- The "Specifying Password, Logon, and Lockout Policies" chapter of the *System Administration Guide for Cisco Unity Connection.*

# Edit Authentication Rule

*Table 10-9 Edit Authentication Rule Page*

| Field | Description |
|---|---|
| Display Name | Enter a descriptive name for the authentication rule. |
| Failed Logon ____ Attempts | Enter the number of failed logon attempts after which users cannot access Cisco Unity Connection.<br>When set to 0 (zero), there is no limit to the number of failed logon attempts, and the user is not locked out of the account.<br>Default setting: 3 attempts. |
| No Limit for Failed Logons | Check this check box so that there is no limit to the number of failed logon attempts, and the user is not locked out of the account. |

*Table 10-9 Edit Authentication Rule Page (continued)*

| Field | Description |
|---|---|
| Reset Failed Logon Attempts Every ____ Minutes | Enter the number of minutes after which Cisco Unity Connection clears the count of failed logon attempts (unless the failed logon limit is already reached and the account is locked).<br>When set to 0 (zero), a failed logon attempt results in the user account being locked until manually unlocked by an administrator.<br>Default setting: 30 minutes. |
| Lockout Duration ____ Minutes | Enter the number of minutes that a user account remains locked after the number of allowed Failed Logon attempts has been reached. While the account is locked, Cisco Unity Connection prevents the user from accessing Connection by phone.<br>If a value of 0 (zero) is entered, the account remains locked until manually unlocked by the administrator.<br>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.<br>Default setting: 1440 minutes (1 day). |
| Credential Expires After ____ Days | Default setting: 180 days. |
| Never Expires | Check this check box so that passwords 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 at any time. |
| Expiration Warning Days | Enter the number of days before passwords expire that Cisco Unity Connection will warn users that a password is about to expire.<br>A value of 0 (zero) means that Connection will not warn users that a password is about to expire.<br>Default setting: 0 days. |
| Minimum Credential Length | Enter the required number of digits for user passwords. In general, shorter passwords are easier to use, but longer passwords are more secure. We recommend requiring eight or more digits.<br>When you change the minimum credential length, users are required to use the new length the next time that they change their passwords.<br>A value of 0 (zero) means that blank passwords are permitted.<br>Default setting: 6 digits. |

*Table 10-9 Edit Authentication Rule Page (continued)*

| Field | Description |
|---|---|
| Stored Number of Previous Credentials | Enter a value for the number of previous passwords that Cisco Unity Connection stores for a user. When a user enters a new password, Connection compares it to the stored passwords, and rejects it if it matches a password in the history.<br>A value of 0 (zero) means that Connection does not store any previous passwords for the user.<br>Default setting: 5 passwords. |
| Check for Trivial Passwords | Check this check box to have Cisco Unity Connection verify that a new password meets the following criteria when user phone passwords are changed by using Cisco Unity Connection Administration, the Cisco Unity Assistant, or the Connection conversation:<br>• The digits are not all the same (for example, 9999).<br>• The digits are not consecutive (for example, 1234 or 4321).<br>• The password is not the same as the primary extension that is assigned to the user.<br>In addition to checking this check box, consider providing users with a password policy that advises them to avoid specifying a password that:<br>• Spells their first or last name, their organization or company name, or any other obvious words.<br>• Contains their primary extension.<br>• Is the reverse of their primary extension or contains the reverse of their primary extension.<br>• Uses the same digits more than twice in a row (for example, 900012).<br>• Is a 1-digit increment of a previous password (for example, 20185 to 20186).<br>• Contains fewer than three different digits (for example, 18181). |

**See Also**

- The "Specifying Password, Logon, and Lockout Policies" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Roles

*Table 10-10 Roles Page*

| Field | Description |
|---|---|
| Name | The name of the administrative role. Click 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" section in the "Preparing to Add User Accounts" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

# Edit Role

*Table 10-11 Edit Role Page*

| Field | Description |
|---|---|
| Name | The name of the administrative role. |
| Description | A brief description of the role privileges. |
| Role Assignments | Click 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 View, Create, Update, Delete, and Execute. |

**See Also**

- The "Roles" section in the "Preparing to Add User Accounts" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

# Search Restriction Tables

*Table 10-12 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 click 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" section in the "Call Management Overview" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Overview: Default Restriction Tables" section in the "Managing Restriction Tables" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Restriction Table

*Table 10-13 New Restriction Table Page*

| Field | Description |
|---|---|
| Display Name | Enter a descriptive name for the restriction table. |

*Table 10-13 New Restriction Table Page (continued)*

| Field | Description |
|---|---|
| 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.<br>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.)<br>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.<br>For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field.<br>Default setting: 1 digit. |
| New Restriction Patterns are Blocked by Default | Indicate whether new restriction patterns should be flagged as Blocked by default.<br>Default setting: Check box not checked. |

**See Also**

- The "Creating Restriction Tables" section in the "Managing Restriction Tables" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Restriction Table Basics

*Table 10-14 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.<br>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.)<br>Default setting: 30 digits. |

*Table 10-14 Edit Restriction Table Basics Page (continued)*

| Field | Description |
|---|---|
| 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.<br>For example, to prohibit users from using four-digit numbers, enter 5 in the Minimum Length of Dial String field.<br>Default setting: 1 digit. |
| New Restriction Patterns are Blocked by Default | Indicate whether new restriction patterns should be flagged as Blocked by default.<br>Default setting: Check box not checked. |
| Order | *(Display only)* Indicates the order in which the Connection evaluates the pattern when applying the restriction table. Click Add New to add a new pattern, or Change Order to change the order of the patterns.<br>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:<br>• * to match zero or more digits.<br>• ? to match exactly one digit. Each ? serves as a placeholder for one digit.<br>• # to correspond to the # key on the phone. |

**See Also**

- The "Modifying Restriction Tables" section in the "Managing Restriction Tables" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Change Restriction Pattern Order

*Table 10-15 Change Restriction Pattern Order Page*

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

**See Also**

- The "Modifying Restriction Tables" section in the "Managing Restriction Tables" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Licenses

*Table 10-16 Licenses Page*

| Field | Description |
|---|---|
| Install Selected | Installs a license file that you have added to the server by using the Add New button. |
| Delete Selected | To delete a license, check the check box to the left of the display name, and click Delete Selected. You can delete multiple licenses at once. |
| Add New | Click Add New to display the Add New License page, on which you specify the full path to the license file that you want to add to the server. |
| Installed | *(Display only)* Indicates whether a license file is installed. For the features in a Cisco Unity Connection license file to be available, the file must appear in the list (the file must have been added to the server), and the value of the Installed column for that license file must be Yes. |
| File Name | *(Display only)* The file names of the license files that are already installed or that have been added, so they are available to be installed. |

**See Also**

- The "Obtaining and Installing a License File" section in the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Add New License

**Revised May 2009**

*Table 10-17 Add New License Page*

| Field | Description |
|---|---|
| Select a License File to Upload | Enter the path to the Cisco Unity Connection license file that you want to install.<br>You can click Browse to locate the file.<br>**Note** The file name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores. |

**See Also**

- The "Obtaining and Installing a License File" section in the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection*.

# View License

*Table 10-18 View License Page*

| Field | Description |
|---|---|
| File Name | *(Display only)* The file name of the license file. |
| File Content | *(Display only)* The text that the license file contains. |

### See Also

- The "Obtaining and Installing a License File" section in the "Managing Licenses" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Schedules

*Table 10-19 Search Schedules Page*

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

### See Also

- The "Schedules and Holidays" section in the "Call Management Overview" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Overview: Default Schedules" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Schedule

*Table 10-20 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" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Schedule Basics

*Table 10-21 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. |
| Delete Selected | To delete a schedule, check the check box to the left of the display name, and click Delete Selected. You can delete multiple schedules at once. |

*Table 10-21 Edit Schedule Basics Page (continued)*

| Field | Description |
|---|---|
| Add New | To add a schedule, click 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. Click 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" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Schedule Detail

*Table 10-22 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.<br>**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. |

*Table 10-22 New Schedule Detail Page (continued)*

| Field | Description |
|---|---|
| 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**

- The "Creating Schedules" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Schedule Detail

*Table 10-23 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.<br>**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. |
| 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" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Holiday Schedules

*Table 10-24 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 click Delete Selected. You can delete multiple holiday schedules at once. |
| Display Name | *(Display only)* The name of the holiday schedule. Click the Display Name to edit the schedule. |

### See Also

- The "Designating Holidays" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Holiday Schedule

*Table 10-25 New Holiday Schedule Page*

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

### See Also

- The "Designating Holidays" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Holiday Schedule Basics

*Table 10-26 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 click Delete Selected. You can delete multiple holiday schedules at once. |
| Add New | To add a holiday schedule, click 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. Click 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. |

*Table 10-26 Edit Holiday Schedule Basics Page (continued)*

| Field | Description |
|---|---|
| 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**

- The "Designating Holidays" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Holiday

*Table 10-27 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.<br><br>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.<br><br>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. |
| 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.<br><br>**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.<br><br>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.<br><br>Uncheck this check box to specify an earlier time of day in the End Time field. |

### See Also

- The "Designating Holidays" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Holiday

*Table 10-28 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.<br><br>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.<br><br>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. |
| 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.<br><br>**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.<br><br>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.<br><br>Uncheck this check box to specify an earlier time of day in the End Time field. |

### See Also

- The "Designating Holidays" section in the "Managing Schedules and Holidays" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Global Nicknames

*Table 10-29 Search Global Nicknames Page*

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

**See Also**

- The "Voice Recognition: Global Nickname List" section in the "Changing Conversation Settings for All Users" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New Global Nickname

*Table 10-30 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**

- The "Voice Recognition: Global Nickname List" section in the "Changing Conversation Settings for All Users" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Global Nickname

*Table 10-31 Edit Global Nickname Page*

| Field | Description |
|---|---|
| Delete Selected | To delete a nickname, check the check box to the left of the nickname, and click Delete Selected. You can delete multiple nicknames at once. |
| Add New | To add a nickname, click 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" section in the "Changing Conversation Settings for All Users" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Subject Line Formats

**Revised May 2009**

*Table 10-32 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 Connection users who send messages without first logging on to Connection or who have not been automatically identified as Connection users by the Identified User Messaging feature. |
| 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 logged on to Connection, or who have been automatically identified as 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.<br>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.<br>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.<br>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.<br>You can also leave this field blank. |

*Table 10-32 Subject Line Formats Page (continued)*

| Field | Description |
|---|---|
| %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.<br><br>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.<br><br>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, Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field.<br><br>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, Connection inserts the display name of the interview handler. If the display name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field.<br><br>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, Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Connection inserts the value specified in the %NAME% (When Unknown) field. |
| %EXTENSION% (When Unknown) | Enter text to be used in subject lines when the extension of the sender of the message is not known.<br><br>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.<br><br>You can also leave this field blank. |
| %U% | Enter text that is used in subject lines when a message is flagged as urgent.<br><br>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.<br><br>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.<br><br>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.<br><br>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" and the "Types of Messages" sections in the "Messaging" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search TTS Descriptions of Message Attachments

**Revised May 2009**

***Table 10-33 Search TTS Descriptions of Message Attachments Page***

| Field | Description |
|---|---|
| Language | Click 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 click Delete Selected. You can delete multiple message attachments at once. |
| Add New | To add a message attachment, click the Add New button. A new page opens, on which you enter data applicable to the new message attachment. |
| Extension | *(Display only)* The file extension of the message attachment for which the description applies.<br>Click the file extension to edit the description. |
| Description | *(Display only)* The description that is read by Text to Speech (TTS). |

### See Also

- The "Managing Descriptions of Message Attachments" chapter of the *System Administration Guide for Cisco Unity Connection*.

# New TTS Description of Message Attachments

**Revised May 2009**

***Table 10-34 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

- The "Managing Descriptions of Message Attachments" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit TTS Descriptions of Message Attachments

**Revised May 2009**

*Table 10-35 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**

- The "Managing Descriptions of Message Attachments" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Enterprise Parameters

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

*Table 10-36 Enterprise Parameters Page*

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

**See Also**

- The "Description of Enterprise Parameters" section in the "Configuring Enterprise Parameters" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Configuring Enterprise Parameters for Cisco Unified Serviceability Services" section in the "Configuring Enterprise Parameters" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Service Parameters

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

*Table 10-37 Service Parameters Page*

| Field | Description |
|---|---|
| Server | Click the name of the Cisco Unity Connection server. |
| Service | Click 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 click the value for the parameter. |
| Suggested Value | *(Display only)* The suggested parameter value. |

*Table 10-37 Service Parameters Page (continued)*

| Field | Description |
|---|---|
| Set to Default | Click the Set to Default button to set all service parameters for the service to the default values. |

**See Also**

- The "Description of Service Parameters" section in the "Configuring Service Parameters" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Configuring Service Parameters for Cisco Unified Serviceability Services" section in the "Configuring Service Parameters" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search Plugins

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

*Table 10-38 Search Plugins Page*

| Field | Description |
|---|---|
| Find | Click the Find button to display the available plugins. |
| Download | Click 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" section in the "Installing Plugins" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Edit Fax Server Configuration

*Table 10-39 Edit Fax Server Configuration Page*

| Field | Description |
|---|---|
| Enabled | Check this check box to enable the connection from Cisco Unity Connection to the fax server.<br>Uncheck this check box to disable the connection from Connection to the fax server.<br>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. |

*Table 10-39 Edit Fax Server Configuration Page (continued)*

| Field | Description |
|---|---|
| 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.<br>Uncheck this check box if you are not using an SMTP Smart Host. |

**See Also**

- The "Creating a Cisco Fax Server Integration" chapter of the *System Administration Guide for Cisco Unity Connection*.

# LDAP Setup

**Revised May 2009**

*Table 10-40 LDAP Setup Page*

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

*Table 10-40 LDAP Setup Page (continued)*

| Field | Description |
|---|---|
| LDAP Attribute for User ID | For LDAP users whose data is imported into Cisco Unity Connection, choose the field in the LDAP directory that you want to appear in the Alias field in Connection. Note the following considerations:<br>• The field that you choose must have a value for every user in the LDAP directory.<br>• Every value for the field that you choose must be unique.<br>• Any LDAP user who does not have a value in the field that you choose is not imported into Connection.<br>• If you are going to create new Connection users by importing LDAP users, and if 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 choose that matches the value in the Alias field for an existing Connection user.<br>• If you later need to change the field that you choose 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.<br>• You must use the same LDAP field for all LDAP directory configurations. |

**See Also**

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users" section in the "Integrating Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Find and List LDAP Directory Configurations

*Table 10-41 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 click Find. |
| Add New | To add an LDAP directory, click the Add New button. A new page opens, on which you enter data applicable to the new LDAP directory. |

**See Also**

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users" section in the "Integrating Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.

# LDAP Directory Configuration

**Revised May 2009**

*Table 10-42 LDAP Directory 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 Connection data with LDAP data.<br><br>We recommend that you use an account dedicated to 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, Connection must be reconfigured with the new password.)<br><br>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 10-42 LDAP Directory 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. Connection imports all users in the tree or subtree (domain or organizational unit) specified by the search base. A Connection server or cluster can only import LDAP data from subtrees with the same directory root, for example, from the same Active Directory forest.<br><br>**Using an LDAP Directory Other than Active Directory**<br>If you are using an LDAP directory other than Microsoft Active Directory, and if you create a Connection LDAP directory configuration that specifies the root of the directory as the user search base, Connection will import data for every user in the directory. If the root of the directory contains subtrees that you do not want Connection to access (for example, a subtree for service accounts), you should do one of the following:<br>• Create two or more Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Connection to access.<br>• Create an LDAP search filter. For more information, see the "Filtering LDAP Users" section in the "Integrating Cisco Unity Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.<br>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.<br><br>**Using Active Directory**<br>If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; 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 Connection Alias field; the UPN is guaranteed by Active Directory to be unique across the forest.<br><br>**Using Digital Networking**<br>If you are using Digital Networking to network two or more Connection servers that are each integrated with an LDAP directory, do not specify a user search base on one Connection server that overlaps a user search base on another Connection server, or you will have user accounts and mailboxes for the same Connection user on more than one Connection server.<br><br>**Note** You can eliminate the potential for duplicate users by creating an LDAP filter on one or both Connection servers. For more information, see the "Filtering LDAP Users" section in the "Integrating Cisco Unity Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*. |

*Table 10-42 LDAP Directory Page (continued)*

| Field | Description |
|---|---|
| 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.<br><br>If you want to use LDAP authentication, uncheck this check box.<br><br>When you check this check box, 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.<br><br>If you have already created Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Connection users. You must manually create new 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.<br><br>When you specify a re-sync interval, we recommend that you:<br><br>• Stagger synchronization schedules so that multiple LDAP configurations are not querying the same LDAP servers simultaneously.<br><br>• Schedule synchronization to occur during nonbusiness hours.<br><br>The first resynchronization occurs on the date and time specified in the Next Re-sync Time field.<br><br>If you check the Perform Sync Just Once check box, these fields are unavailable, and resynchronization does not occur at the interval specified here.<br><br>If you have already created Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Connection users. You must manually create new 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, Connection resynchronizes at the interval specified in the Perform a Re-sync Every <Interval> field.<br><br>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.<br><br>If you have already created Connection users from LDAP data, this resynchronization imports updated LDAP data for the existing Connection users. However, if new users have been added to the LDAP directory, this resynchronization does not create new Connection users. You must manually create new Connection users by using either the Import Users tool or the Bulk Administration Tool. |
| User ID | The value of the LDAP field that is listed here is stored in the Alias field in the Cisco Unity Connection database.<br><br>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 | Choose which value from the LDAP directory to store in the Cisco Unity Connection Middle Name field:<br><br>• The value in the LDAP middleName field.<br><br>• The value in the LDAP initials field. |

*Table 10-42 LDAP Directory Page (continued)*

| Field | Description |
|---|---|
| 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 | Choose which value from the LDAP directory to store in the Cisco Unity Connection Phone Number field:<br>• The value in the LDAP telephoneNumber field.<br>• 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.<br>**Caution** Every user that you want to import from the LDAP directory into 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 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 | Choose which value from the LDAP directory to store in the Cisco Unity Connection Mail ID field:<br>• The value in the LDAP mail field.<br>• The value in the LDAP sAMAccountName field. |
| 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 Connection database with changes to the LDAP directory.<br>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.<br>If you check this check box, specify a host name in the Host Name or IP Address for Server field, or synchronization may fail.<br>To enable SSL encryption, you must also export SSL certificates from the applicable LDAP directory servers and upload the certificates on all Connection servers. For more information, see the "Integrating Cisco Unity Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*. |
| Add Another Redundant LDAP Server | Click 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.<br>This feature only works when you are using Active Directory for your LDAP directory. |
| Save | Click Save to save this configuration. After the first time you click Save, the Delete, Copy, Perform Full Sync Now, and Add New buttons appear. |
| Delete | Click to delete this configuration.<br>This button is not available until after the first time you save this configuration. |

*Table 10-42 LDAP Directory Page (continued)*

| Field | Description |
|---|---|
| Copy | Click to copy this configuration.<br>This button is not available until after the first time you save this configuration. |
| Perform Full Sync Now | Click to resynchronize Cisco Unity Connection user data with user data in the LDAP directory.<br>This button is not available until after the first time you save this configuration. |
| Add New | Click to add a new configuration, which allows you to synchronize Cisco Unity Connection data from additional LDAP user search bases.<br>This button is not available until after the first time you save this configuration. |

**See Also**

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users" section in the "Integrating Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.

# LDAP Authentication

**Revised May 2009**

*Table 10-43 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.<br>When this check box is not checked, Connection web applications authenticate user names and passwords against the user name and web application password in the Connection database.<br>When users log on to Connection by phone, Connection always authenticates based on the voice mail password in the 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 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.<br>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. |

*Table 10-43 LDAP Authentication Page (continued)*

| Field | Description |
|---|---|
| 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.<br><br>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), Connection cannot verify the identity of the LDAP server.<br><br>When you are using Active Directory for your LDAP directory, we recommend that you specify an Active Directory global catalog server for faster response times. |
| LDAP Port | Enter the port on the LDAP server that Cisco Unity Connection should use to access the LDAP directory.<br><br>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:<br><br>• 3268 if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Connection server.<br><br>• 3269 if you are using SSL. |
| 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.<br><br>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), Connection cannot verify the identity of the LDAP server.<br><br>To enable SSL encryption, you must also export SSL certificates from the applicable LDAP directory servers and upload the certificates on all Connection servers. For more information, see the "Integrating Cisco Unity Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*. |
| Add Another Redundant LDAP Server | Click 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.<br><br>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 Connection Users with LDAP Users" section in the "Integrating Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Advanced LDAP Settings

*Table 10-44 Advanced LDAP Settings Page*

| Field | Description |
|---|---|
| User Extension Regular Expression | Enter a regular expression to convert the phone number that is imported from the LDAP directory into an extension for use in Cisco Unity Connection. For example:<br>• To use the phone number as the extension, without punctuation, if any, enter:<br>[0-9]+<br>• To use the last four digits of the phone number as the extension, enter:<br>[0-9][0-9][0-9][0-9]$<br>• To use the first four digits of the phone number as the extension, enter:<br>^[0-9][0-9][0-9][0-9] |

**See Also**

- The "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users" section in the "Integrating Connection with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection*.

# SMTP Server Configuration

**Revised May 2009**

*Table 10-45 SMTP Server Configuration Page*

| Field | Description |
|---|---|
| SMTP Port # | *(Display only)* The port that Cisco Unity Connection uses for incoming and outgoing SMTP connections. Connection uses SMTP for sending text message notifications; communicating with clients that send or receive voice, fax and text messages from Connection; and communicating with VPIM locations and other digitally networked Connection servers. |
| SMTP Domain | *(Display only)* The domain name that Cisco Unity Connection uses to route messages between digitally networked Connection servers and to construct the SMTP address of the sender on outgoing SMTP messages.<br>For each user, 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 Connection servers and messages that are sent from the Connection phone interface or Cisco Unity Inbox and relayed to an external server based on the Message Actions setting of the recipient.<br>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.<br>When Connection is first installed, the SMTP Domain is automatically set to the fully qualified host name of the server. |

*Table 10-45 SMTP Server Configuration Page (continued)*

| Field | Description |
|---|---|
| Change SMTP Domain | Click this button to change the value of the SMTP Domain field. When changing the value, note the following considerations:<br>• 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 Connection server.<br>• Each Connection server in a Digital Network must have a unique SMTP Domain. |
| Limit Number of Simultaneous Client Connections | Enter the maximum number of clients that can simultaneously connect to the Cisco Unity Connection SMTP server for sending or receiving messages.<br>Default setting: 5 connections. |
| Limit Size of Message | Enter the maximum size of message that clients can send to Cisco Unity Connection by using SMTP.<br>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.<br>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.<br>Default setting: 15,000 recipients. |
| Retry Delivery Timeout | *(Cisco Unity Connection 7.1 or later)* 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, 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, Connection sends a non-delivery receipt to the sender.<br>Default setting: 0 minutes (Connection immediately sends a non-delivery receipt to the sender and does not retry delivery of failed SMTP messages).<br>**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.<br>When this check box is not checked, 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.<br>Default setting: Check box not checked. |

*Table 10-45 SMTP Server Configuration Page (continued)*

| Field | Description |
|---|---|
| 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.<br>When this check box is not checked, Connection allows these types of clients to connect without authenticating.<br>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.<br>• Disabled—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 Connection does not offer it, the connection fails and the client notifies the user.<br>• Required—Clients or servers connecting from untrusted IP addresses must use TLS to initiate SMTP sessions with the Connection server.<br>• Optional—Clients or servers connecting from untrusted IP addresses can use TLS to initiate SMTP sessions with the Connection server, but are not required to do so.<br>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" section in the "Setting Up SMTP and SMS (SMPP) Message Notifications" chapter of the *System Administration Guide for Cisco Unity Connection*.
- The "Configuring IMAP Settings" chapter of the *System Administration Guide for Cisco Unity Connection*.

# Search IP Address Access List

*Table 10-46 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 click Delete Selected. You can delete multiple IP addresses at once. |
| Add New | To add an IP address, click 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.<br>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. |

# New Access IP Address

*Table 10-47 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.<br>**Note** You can enter a single * (asterisk) to match all possible IP addresses. |

# Access IP Address

*Table 10-48 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.<br>**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.<br>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. |

# Smart Host

*Table 10-49 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.)<br>Connection relays all SMTP notifications through the smart host. You can configure Connection to relay voice mail, 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 Connection to route SMTP messages for VPIM locations or for other digitally networked 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" section in the "Setting Up SMTP and SMS (SMPP) Message Notifications" chapter of the *System Administration Guide for Cisco Unity Connection*.