System Settings

Overview

The System Settings menu in Cisco Unity Connection Administration provides various options that helps you to manage the system wide settings for different features and parameters.

General Configuration

The General Configuration settings enables the administrator to manage various system settings and conversation settings in Unity Connection.

The system settings include the default partition, default search space, and timezone in which Unity Connection plays the system prompts to users and callers. The conversation settings include the default phone language settings, target decibel level for messages and greetings, and maximum greeting length in Unity Connection system.

Managing the General Configuration Settings

Step 1 In Cisco Unity Connection Administration, expand System Settings and select General Configuration.

Step 2 On the Edit General Configuration page, enter the values of the required settings. (For more information on each field, see Help> This Page).

Step 3 Select Save.

Cluster

The Cluster settings page enables an administrator to view and manage the Unity Connection cluster related information. To access the cluster settings, sign in to Cisco Unity Connection Administration, expand System Settings and select Cluster.

The Find and List Servers page displays the hostname or IP address and the server type of the installed Unity Connection servers. If you have installed only the publisher server, you need to add the details of the subscriber server in the Cluster settings to configure a cluster. For more information, see the "Configuring Cisco Unity Connection Cluster" chapter in *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 15* available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html.

You can manage the server details of publisher or subscriber server from the Server Configuration page in which you specify the hostname, IP address, MAC details, and local bandwidth management (LBM) information of the server. For more information on each field, see Help> This Page.

Authentication Rules

Authentication rules in Unity Connection govern the policies for user passwords, PINs, and user account lockouts. The authentication rules prevent unauthorized access to Unity Connection web applications, such as Cisco PCA and Web Inbox, by locking out users when they enter invalid PINs or passwords. The two predefined authentication rules are Recommended Voice Mail Authentication Rule and the Recommended Web Application Authentication Rule.

When you add users to Unity Connection, the phone PINs and web application passwords are determined by the user template used to create the user account. By default, user templates are assigned randomly generated strings for the phone PIN and web password. All users created from a user template are assigned the same PIN and password. A user must change the password or PIN during the next sign in to secure access to his account details.

Consider the following points when configuring PINs and passwords in Unity Connection:

- To enhance security settings, change the PINs and passwords frequently. For information on changing the web application or phone passwords, see the Users chapter.

Note Users can also change the PINs or passwords using the Messaging Assistant.

- To protect Unity Connection from unauthorized access and toll fraud, every user should be assigned a unique phone PIN and web application password.
- The PINs or passwords should be of six characters and non trivial.

The PINs and passwords used in various Unity Connection applications are:

- Voicemail password: The voicemail passwords are used to sign in to a Unity Connection conversation using phone. Users can either use the phone keypad to enter a password that entirely consists of digits or can speak out the PIN if enabled for voice recognition.
- Web Application password: The web application password is used by a user to sign in to the Unity Connection web applications, such as Messaging Assistant and Web Inbox.

Note If you are using Cisco Business Edition or LDAP authentication, users must use the Cisco Business Edition or LDAP user passwords to access the Unity Connection web applications.

Configuring Authentication Rules

The authentication rules configured in Cisco Unity Connection Administration helps determine:

- The number of failed sign in attempts to the Unity Connection phone interface, Cisco PCA, or Unity Connection Administration that are allowed before an account is locked.
- The number of minutes an account remains locked before it is reset.
- Whether a locked account must be unlocked manually by an administrator.
- The minimum length allowed for passwords and PINs.
- The number of days before a password or PIN expires.

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Authentication Rules.

The Search Authentication Rules page appears displaying the default and currently configured authentication rules.

Step 2 Configure an authentication rule (For more information on each field, see Help> This Page):

- To add an authentication rule:

  On the Search Authentication Rules page, select Add New.

  On the New Authentication Rules page, enter the values of the required fields and select Save.

- To edit an existing authentication rule:

  On the Search Authentication Rules page, select the authentication rule that you want to edit.

  On the Edit Authentication Rules page, enter the values of the required fields and select Save.

- To delete one or more authentication rules:

  On the Search Authentication Rules page, select the authentication rule that you want to delete.

  Select Delete Selected and OK to confirm deletion.

Roles

A role comprises of set of privileges that define the access level to the system. System Administrator can configure multiple roles based on the administrative needs. The role assignment for a user account can be done based on the set of operations required. Unity Connection offers two types of roles:

- System Roles - System Roles are the predefined roles that come installed with Unity Connection.
- Custom Roles - Custom Roles are the roles which can be created, updated or deleted by a System Administrator.

Note You can assign or remove any role to one or more users from the Edit Roles page of Users. For more information, see the Users chapter.

Note User with System Admin or User Admin role can only update the Pin/Password for any other user with any system roles. Also any user can update the Pin/Password for other user who is not assigned any role.

Configuring Roles

You can create, modify, or delete Custom Roles based on your requirements.

To Configure Custom Role

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Roles** and select **Custom Roles**.
The Search Custom Role page appears displaying the currently configured custom roles.

Step 2 Configure the custom role:

- To add a Custom Role (For more information on each field, see Help> This Page):

  a. Select **Add New**. The New Custom Role page appears.
  b. Enter the required information in the fields.
  c. Select a system role that you want to inherit.
  d. Select the privileges to be assigned to the custom role.

Note *(Applicable only for Unity Connection12.0 and 11.5)* Make sure to select the "**Read Access To System Configuration Data - Read Access** " privilege.

e. Select **Save**.

- To update a Custom Role:

a. Select the Custom Role that you want to edit. The Edit Custom Role page appears displaying the current settings of the custom role.
b. Edit the Custom Role settings as applicable..
c. Select **Save**.

- To delete a Custom Role:

a. Check the check box next to the custom role that you want to delete.
b. Select **Delete Selected**.

Note A dialog box with the "After role deletion, it's association with the users will be removed" message appears.

c. Select **OK** to confirm the deletion.

Note You can delete multiple roles by selecting more than one checkbox at a time.

Assigning or Removing Roles to a User

To Assign or Remove a Role to a User from System Settings

Step 1 In Cisco Unity Connection Administration, expand **System Settings > Roles** and select either of the following: .

- **System Roles**: The Search Roles page appears displaying already configured system roles.
- **Custom Roles**: The Search Custom Roles page appears displaying already configured custom roles.

Step 2 Assign a role to one or more users (For more information on each field, see Help> This Page):

a) Select the role that you want to assign to one or more users.
b) Select **Role Assignments** on the Edit page of the selected role.

Note Make sure to select **not in** from the **Find Users** dropdown list for the specific role that you want to assign.

c) Check the check boxes next to the users to whom you want to assign the role and select **Assign Selected**.

Step 3 Remove a role from one or more users (For more information on each field, see Help> This Page):

a) Select the role that you want to remove from one or more users.
b) Select **Role Assignments** on the Edit page of the selected role..
c) Check the check boxes next to the users for whom you want to remove the role and select **Remove Selected**.

Restriction Tables

The restriction tables allow you to control which phone numbers or URIs the users and administrators can use for transferring calls, dialing out message notifications and faxes, and to restrict specific extensions from being added as alternate extensions. For more information, see the Restriction Tables section.

Licenses

The License settings page displays the license information in a Unity Connection server. In Unity Connection, the licenses are managed by **Cisco Smart Software Licensing**. This licensing model adds flexibility to your licensing and simplifies it across the enterprise. Unity Connection must be registered with the Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite to use various licensed feature.

Unity Connection remains in the Evaluation Mode until it registers with the Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite. For information on Unity Connection licenses, see the "Managing Licenses" chapter of the *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection, Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html.

Schedules

The Schedule settings page helps to manage the various schedules in Unity Connection. An administrator can control greetings, transfer types, and access rights based on the schedules applied to a user or call handler.

Holiday Schedules

Holiday schedules work together with active schedules to control greetings, transfer types, and access rights. For more information see the Holiday Schedules section.

Global Nicknames

The Global Nickname list is a comprehensive list of common nicknames that Unity Connection considers when a caller uses voice recognition to place a call or to address messages. For example, Unity Connection considers "Bill," "Billy," and "Will" to be nicknames for the name "William."

If a user has an uncommon name or if others know the user by a different name (for example, a maiden name) consider adding these alternate names for the user. Alternate names improve the likelihood of Unity Connection placing a call when callers ask for the user by name.

Configuring a Global Nickname in Unity Connection

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Global Nicknames.

The Search Global Nicknames page appears displaying the currently configured global nicknames.

Step 2 Configure a nickname (For more information on each field, see Help> This Page)

- To add a nickname:

  On the Search Global Nicknames page, select Add New.

  On the New Global Nicknames page, enter the values of the required fields and select Save.

- To edit a nickname:

  On the Search Global Nicknames page, select the nickname that you want to edit.

  On the Edit Global Nicknames page, enter the values of the required fields and select Save.

- To delete a nickname:

  On the Search Global Nicknames page, select the nickname that you want to delete.

  Select Delete Selected and OK to confirm deletion.

Subject Line Formats

The message subject lines are visible when users view and listen to messages in Web Inbox, Messaging Inbox, an IMAP client, an RSS client, or any other visual client that displays the message subject. Subject lines are not presented to users when they listen to voice messages over phone.

You can configure both the wording and the information that is included in the subject line of voice messages, including localizing the subject line according to the language of the recipient.

The subject line format is defined for the following types of messages:

1.For Voice Messages:

- Outside caller messages: The unidentified voice messages or messages from callers who are not Unity Connection users. This also includes the messages left for a system call handler.
- User to user messages: The identified voice messages or messages from Unity Connection users.
- Interview handler messages: The messages left for interview handlers.
- Live record messages: The messages containing conversation recorded during the communication between users and callers.

2.For Notifications:

- Message Notifications: This includes Email notifications that are sent to the Unity Connection users for new voice messages.
- Missed Call Notifications: This includes the Email notifications for missed calls.
- Scheduled Summary Notifications: This includes the Email notifications sent at scheduled time(s).

For more information on Notifications Subject Line Format, see Notifications Subject Line Format section.

Subject Line Parameters for Voice Messages

Following table describes the parameters that can be used to define message subject lines.

Table 1: Parameters Used to Define Message Subject Lines

Parameter	Description
%CALLERID%	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 entered in the %CALLERID% (When Unknown) field is inserted into the subject line instead.
%CALLEDID%	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 Called ID is not available, the text entered in the %CALLEDID% (When Unknown) field is inserted into the subject line instead. You might find this field useful in cases where more than one organization shares a single Cisco Unity Connection system, and there are multiple inbound numbers defined so that callers can be routed to different opening greetings. In this case it might be helpful if messages left in a general help voice mailbox include the number that the sender of the message used when calling the system.
%NAME%	When the %NAME% parameter is used in the subject line format of an outside caller message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Cisco Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When the %NAME% parameter is used in the subject line format of a user to user message, it is automatically replaced with the display name of the sender of the message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When the %NAME% parameter is used in the subject line format of an interview handler message, it is automatically replaced with the ANI Caller Name of the sender of the message. If the ANI Caller Name is not available, Unity Connection inserts the display name of the interview handler. If the display name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field. When %NAME% is used in the Live Record Messages field, it is automatically replaced with the display name of the user who initiated the live record message. If the display name is not available, Unity Connection inserts the ANI Caller Name. If the ANI Caller Name is not available, Unity Connection inserts the value specified in the %NAME% (When Unknown) field.

Parameter	Description
%EXTENSION%	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 value entered in the %EXTENSION% (When Unknown) field is inserted into the subject line instead. **Note** When %EXTENSION% is used in the Live Record Messages field, it is replaced with the extension of the user who initiated the live record message
%U%	When the %U% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %U% field if the message is flagged as urgent. If the message is not urgent, this parameter is omitted.
%P%	When the %P% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %P% field if the message is flagged as private. If the message is not private, this parameter is omitted.
%S%	When the %S% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %S% field if the message is flagged as a secure message. If the message is not a secure message, this parameter is omitted.
%D%	When the %D% parameter is used in a subject line format, it is automatically replaced with the text that you enter in the %D% field if the message is flagged as a dispatch message. If the message is not a dispatch message, this parameter is omitted.

Subject Line Format Examples for Voice Messages

Table 2: Subject Line Format Example

Type of Message	Subject Line Format	Message Details	Subject Line of the Message Received
Outside caller message	%U% %D% Voice message from %CALLERID%	An outside caller with the ANI Caller ID 2065551212	"Voice message from 2065551212"
User to user message	%U% %P% %S% Message from %NAME% [%CALLERID%]	John Jones, at extension 4133-an urgent message	"Urgent Message from John Jones [4133]"
Interview handler message	Message from %NAME% [%CALLERID%]	"Sales Survey" interview handler, no ANI caller ID available	"Message from Sales Survey [Unknown caller ID]"
Live Record message	Live Record message from %CALLERID%	User recording of a phone call from a caller with the ANI caller ID 4085551212	"Live Record message from 4085551212"

When a System Call Handler or Interview Handler is configured to receive the voice messages that are forwarded to the user with mailbox assigned to the Call handler, by default the information of call handler is appeared in the **From** field of Subject Line for the messages. If you want to get the sender's original information in the **From** field of subject line of the message, do the following:

1. Execute

   ```
   run cuc dbquery unitydirdb update tbl_configuration set valuebool ='1' where
   fullname='System.Conversations.ConfigParamForSenderInfo'
   ```

   CLI command.

2. Restart the Connection Conversation Manager on the Unity Connection server to reflect the changes
3. In case of a cluster, run the CLI command on publisher server and restart the Connection Conversation Manager on both the nodes of Unity Connection.

Subject Line Format Configuration

You should consider the following when defining the subject line formats:

- You must include a % before and after the parameter.
- You can define a separate subject line format for each language that is installed on the system.
- When a subject line format is not defined for the preferred language of the user, the subject line format definition for the system default language is used instead.
- When a message is sent to a distribution list, the subject line format for the system default language is used for all recipients in the distribution list. This means that the subject line is not necessarily in the preferred language of each recipient.
- Subject line formats are applied to voice messages when the messages are saved to the database. Messages that are already in user mailboxes are not altered if the subject line format definitions are subsequently changed. Only voice messages that are recorded after the changes have been saved reflect the new subject line definition.

Configuring Subject Line Formats in Unity Connection

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Subject Line Formats.

Step 2 On the Edit Subject Line Formats page, enter the values of the required fields or parameters. (For more information on each field, see Help> This Page).

Step 3 Select Save.

Attachment Descriptions

When Unity Connection is integrated with a third party message store, it uses Text to Speech (TTS) descriptions of message attachments for the users who check the messages on phone. For example, an attachment with the extension .jpg is described as “an image.”

Configuring Description of a Message Attachment

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Attachment Descriptions.

The Search TTS Descriptions of Message Attachments page appears displaying the currently configured message attachment descriptions.

Step 2 Configure description of a message attachment (For more information on each field, see Help> This Page):

- To add description of a message attachment:

  On the Search TTS Descriptions of Message Attachments page, select Add New.

  On the New TTS Description of Message Attachment page, enter the values of the required fields and select Save.

- To edit an existing description of a message attachment:

  On the Search TTS Descriptions of Message Attachments page, select the attachment that you want to edit.

  On the Edit TTS Descriptions of Message Attachments page, enter the values of the required fields and select Save.

- To delete description of a message attachment:

  On the Search TTS Descriptions of Message Attachments page, select the attachment that you want to delete.

  Select Delete Selected and OK to confirm deletion.

Enterprise Parameters

Enterprise parameters for Unity Connection provide default settings that apply to all services in Cisco Unified Serviceability. To view and manage the enterprise parameters, sign in to Cisco Unity Connection Administration, expand System Settings and select Enterprise Parameters.

For more information about Cisco Unified Serviceability services, see the Cisco Unified Serviceability Administration Guide Release 10.0(1), available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/admin/CUCM_BK_CDDBCDEB_00_cisco-unified-serviceability-merge-100.html.

The Table 16-1 describes the enterprise parameters available in Unity Connection. The fields not described in this table are managed from Cisco Unified Communications Manager.

Enterprise Parameter Descriptions

Parameter Name	Description
Cluster ID	Specifies the parameter value for the server. The administrator cannot edit the parameter value from the Enterprise Parameters page.
Max Number of Device Level Trace	Specifies the number of devices that can be traced concurrently if you select device name based trace in the Trace Configuration in Cisco Unified Serviceability. Default setting: 12 Minimum: 0 Maximum: 256

Parameter Name	Description
Localization Parameters	
Default Network Locale	Specifies the default network locale for tones and modulations of voice. The selected network locale applies to all gateways and phones that do not have the network locale set at the device or device pool level. **Note** Make sure that the selected network locale is installed and supported for all gateways and phones. Reset all devices for the parameter change to take effect. Default setting: United States
Default User Locale	Specifies the default user locale for language selection. Not all locales are supported by all models. For models that do not support this setting, set their locale explicitly to something they support. **Note** Reset all devices for the parameter change to take effect. Default setting: English United States
Prepare Cluster for Rollback	
Prepare Cluster for Rollback to pre 8.0	If a Unity Connection cluster is upgraded to a higher version, this settings specifies the previous version of Unity Connection Default setting: False
Trace Parameters	
File Close Thread Flag	Enables the use of separate threads to close trace files. This may improve the performance of the system at the end of a trace file. Default setting: True
FileCloseThreadQueueWaterMark	Defines the high-water mark after which the separate thread used to close trace files stops accepting trace files to close; the trace file is then closed without the use of a separate thread. Default setting: 100 Minimum: 0 Maximum: 500
Clusterwide Domain Configuration Parameters	
Organization Top Level Domain	Defines the top level domain for the organization (for example, cisco.com). Maximum length: 255 Allowed values: Provide a valid domain (for example, cisco.com) with up to 255 of the following characters: any upper or lower case letter (a-z, A-Z), any number (0-9), the hyphen (-), or the dot (.) The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om is an example of an invalid domain.

Parameter Name	Description
Cluster Fully Qualified Domain Name	Defines one or more Fully Qualified Domain Names (FQDN) for the cluster. Multiple FQDNs must be separated by a space. Wildcards can be specified within an FQDN using an asterisk (*). Examples are cluster-1.rtp.cisco.com and *.cisco.com. Requests containing URLs (for example, SIP calls) whose host portion matches any of the FQDNs in this parameter are recognized as a request destined for the cluster and/or devices attached to it. Maximum length: 255 Allowed values: Provide one or more fully qualified domain names (FQDN), or partial FQDNs using the * wildcard (for example, cluster-1.cisco.com or *.cisco.com). Multiple FQDNs must be separated by a space. The following characters are allowed: • Any upper or lower case letter (a-z or A-Z) • Any number (0-9) • Hyphen (-) • Asterisk (*) • Dot (.) The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om serves as an example of an invalid domain.
Cisco Support Use	
Cisco Support Use 1	Used by Cisco Technical Support only. Maximum length: 10
Cisco Support Use 2	Used by Cisco Technical Support only. Maximum length: 10
Cisco Syslog Agent	

Parameter Name	Description
Remote Syslog Server Name 1 to Remote Syslog Server Name 5	Enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. You can configure up to five remote Syslog servers to accept Syslog messages. If a server name is not specified, Cisco Unified Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server. Maximum length: 255 Allowed values: Provide a valid remote syslog server name with the following characters: • A-Z • a-z • 0-9 • . • -
Syslog Severity for Remote Syslog Messages	Select the desired Syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to remote syslog. If a remote server name is not specified, Cisco Unified Serviceability does not send the Syslog messages. Default setting: Error
CUCReports Parameters	
Report Socket Unity Connection Timeout	Specifies the maximum number of seconds used when trying to establish a Unity Connection with another server. Increase this time if Unity Connection experiences issues on a slow network. Default setting: 10 Minimum: 5 Maximum: 120
Report Socket Read Timeout	Specifies the maximum number of seconds used when reading data from another server. Increase this time if Unity Connection experiences issues on a slow network. Default setting: 60 Minimum: 5 Maximum: 600

Service Parameters

Service parameters for Unity Connection allow you to configure different services in Cisco Unified Serviceability.You can view a list of service parameters and the descriptions by selecting the question mark button in the Service Parameter Configuration window.

If you turn off a service in Cisco Unified Serviceability, Unity Connection retains any updated service parameter values. If you start the service again, Unity Connection sets the service parameters to the changed values.

To view and manage the service parameters, sign in to Cisco Unity Connection Administration, expand System Settings and select Service Parameters.

For more information about Cisco Unified Serviceability services, see the Cisco Unified Serviceability Administration Guide Release 10.0(1), available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/admin/CUCM_BK_CDDBCDEB_00_cisco-unified-serviceability-merge-100.html.

Caution Some changes to service parameters can cause system failure. You should not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (Cisco TAC) specifies the changes.

The Table 16-2 describes the service parameters that can be modified for Unity Connection. The fields not described in this table are managed from Cisco Unified Communications Manager.

Service Parameter Descriptions

Service Parameter	Description
Cisco AMC Service	
Primary Collector	Specifies the Primary AMC (AlertMgr and Collector) server that collects clusterwide real-time information. Value must match one of the configured servers and, preferably, a server with no or minimal call processing.
Failover Collector	Specifies the Failover AMC (AlertMgr and Collector) server. The server specified in this parameter is used to collect real-time data when the Primary AMC is down or unreachable. No data is collected if Failover Collector is not specified when Primary Collector is not active.
Data Collection Enabled	Determines whether collecting and alerting of real-time cluster information is enabled (True) or disabled (False). Default setting: True
Data Collection Polling Rate	Specifies the AMC collecting rate, in seconds. Default setting: 30 Minimum: 15 Maximum: 300 Unit: seconds
Server Synchronization Period	Specifies the amount of time, in seconds, that backup AMC (AlertMgr and Collector) waits at startup in order to determine if primary AMC is up and actively collecting. This parameter prevents backup AMC from assuming a collecting task prematurely. **Note** Restart the AMC service on the backup server for the parameter change to take effect. Default setting: 60 Minimum: 15 Maximum: 300 Unit: seconds
RMI Registry Port Number	Specifies the port number to turn on RMI registry. This port is used for primary or backup AMC to locate other AMC and for the RTMT servlet to find primary/backup AMC. **Note** Restart the AMC service for the parameter change to take effect. Default setting: 1099 Minimum: 1024 Maximum: 65535

Service Parameter	Description
RMI Object Port Number	Specifies the port number used for RMI remote object. This port is used for AMC to exchange data with other AMC as well as with RTMT servlet. **Note** Restart the AMC service for the parameter change to take effect. Default setting: 1090 Minimum: 1024 Maximum: 65535
AlertMgr Enabled	*(For AMC troubleshooting purpose only.)* Enables and disables the alerting (email/epage) feature. **Note** Restart the AMC service for the parameter change to take effect. Default setting: True
Logger Enabled	*(For AMC troubleshooting purpose only*.) Enables and disables the logging feature (CSV files for generating reports). **Note** Restart the AMC service for the parameter change to take effect. Default setting: True
Cisco Database Layer Monitor Service	
Maintenance Time	Specifies the hour to begin call detail recording (CDR) database maintenance. Use this parameter in combination with the Maintenance Window parameter. For example, specifying 22 in this parameter means that the CDR maintenance would begin at 10 p.m. If the Maintenance Window parameter is set to 2, it means that CDR maintenance runs every hour from 10 p.m. to midnight. If both parameters are set to 24, CDR maintenance runs every hour all day long. During CDR maintenance, the system deletes the oldest CDRs and associated call management records (CMRs). Therefore, the maximum number of records specified in the Max CDR Records parameter is maintained. Also during maintenance, the system issues an alarm if the CDR file count exceeds 200 and checks for replication links between servers that have been broken and tries to reinitialize them. Default setting: 24 Minimum: 1 Maximum: 24 Unit: hours

Service Parameter	Description
Maintenance Window	Specifies the time during which CDR maintenance is performed on an hourly basis. For example, if this parameter is set to 12, CDR maintenance runs every hour for 12 hours, starting at the time that is specified in the Maintenance Time parameter. For example, if the Maintenance Time parameter is set to 7 and this parameter is set to 12, CDR maintenance begins at 7 a.m. and run every hour until 7 p.m. If both parameters are set to 24, CDR maintenance runs every hour all day long. During CDR maintenance, the system deletes the oldest CDRs and associated CMRs. Therefore, the maximum number of records specified in the Max CDR Records parameter is maintained. Also, during maintenance, the system issues an alarm if the CDR file count exceeds 200 and checks for replication links between servers that have been broken, and tries to reinitialize them. Default setting: 2 Minimum: 1 Maximum: 24 Unit: hours
Table Out of Sync Detection	When set to On, collects Database Replication Status summary every day during the Maintenance window and compares the output of three consecutive days to determine if there are tables that have been out of sync for all three days. If that is the case, it triggers an alert. This parameter, by default, is set to Off and runs at the time specified in Maintenance Time parameter. Default: Off
MaintenanceTaskTrace	Sets the Maintenance Task trace. You must turn on this parameter to get a performance counter trace from the Maintenance Task. This is a required field. Default setting: Off
Cisco DirSync	
Maximum Number of Agreements	Specifies the maximum number of LDAP directories (also known as agreements) that can be configured in the LDAP Directory window in Cisco Unified CM Administration (System > LDAP > LDAP Directory). Creating more than one LDAP directory helps in synchronizing users from more than one search base. **Note** You must restart the Cisco DirSync service for changes to this parameter to take effect. Default setting: 5 Minimum: 1 Maximum: 5
Maximum Number of Hosts	Specifies the maximum number of LDAP host names that can be configured for failover purposes. **Note** You must restart the Cisco DirSync service for changes to this parameter to take effect. Default setting: 3 Minimum: 1 Maximum: 3

Service Parameter	Description
Retry Delay on Host Failure (secs)	Specifies the number of seconds to delay before retrying the Unity Connection to the first LDAP server (hostname) that is configured in Cisco Unified CM Administration. After a Unity Connection failure, the system tries three times with reconnect to the same host. When the third attempt is also unsuccessful, the system attempts to connect to the next host name in the list in hierarchical order. Default setting: 5 Minimum: 5 Maximum: 60
Retry Delay on HostList Failure (mins)	Specifies the number of minutes to delay before retrying every LDAP server (hostnames) that is configured in Cisco Unified CM Administration. Unity Connection to LDAP servers are retried in the order they appear in Cisco Unified CM Administration and three attempts are made based on the delay interval specified in the Retry Delay On Host Failure service parameter. When all three attempts fail, the next LDAP server in the list is tried. If the system is unable to connect to any of the servers in the list, an error gets logged and the system waits until the next sync interval before retrying to connect starting with the first server in the list. Default setting: 10 Minimum: 10 Maximum: 120
LDAP Unity Connection Timeout (secs)	Specifies the number of seconds allowed for establishing the LDAP connection in Unity Connection. The LDAP service provider aborts the attempt if a connection to Unity Connection cannot be established in the specified amount of time. Default setting: 5 Minimum: 1 Maximum: 60
Delayed Sync Start Time (mins)	Specifies the delay in starting the directory synchronization process after the Cisco DirSync service starts. Directory synchronization ensures that the users in the LDAP server are copied to the Cisco Unified Communications Manager database. **Note** You must restart the Cisco Tomcat service for changes to this parameter to take effect. Default setting: 5 Minimum: 5 Maximum: 60
Cisco RIS Data Collector Parameters	
RIS Cluster TCP Port	Specifies the static TCP port that the Cisco RIS Data Collector services in the cluster use to communicate with each other. This is a required field. **Note** Restart the Cisco RIS Data Collector service on each server in the cluster for the parameter change to take effect. Default setting: 2555 Minimum: 1024 Maximum: 65535

Service Parameter	Description
RIS Client TCP Port	Specifies the static TCP port that the RIS clients use to communicate with the Cisco RIS Data Collector services in the cluster. Note: You must restart Cisco Database Layer Monitor service and the Cisco RIS Data Collector service on each server in the cluster for the parameter change to take effect. **Note** Restart Cisco Database Layer Monitor service and the Cisco RIS Data Collector services on each server in the cluster for the parameter change to take effect. Default setting: 2556 Minimum: 1024 Maximum: 65535
RIS Client Timeout	Specifies the time (in seconds) that a RIS client waits for a reply from the Cisco RIS Data Collector service. The RIS Data Collector service running on each server internally distributes 90 percent of the value specified in this parameter. To set this parameter correctly for a cluster with multiple servers, specify a value that is 4 times (or more) the number of servers that are running the RIS Data Collector service in your cluster. Choosing a higher value helps ensure that the RIS Data Collector service on one server has enough time to receive a reply from the RIS Data Collector service on another server. The time needed for a reply can vary based on factors such as the processor speed of the server, number of devices registered to the server, amount of server memory, the volume of calls, and other performance-affecting factors. Default setting: 30 Minimum: 10 Maximum: 1000 Unit: seconds
RIS Cleanup Time of the Day	Specifies the time of the day that the RIS database is cleaned up to remove any unused and old device information. During this time, the Number of Registration Attempts performance counters for all devices reset to 0. Default setting: 22:00 Maximum length: 5 Allowed values: Specify time in HH:mm format (for example 06:11). Unit: hours:minutes
RIS Unused Cisco CallManager Device Store Period	Specifies the RIS database information storage period for any unregistered or rejected device information from the Cisco CallManager service. After the time specified in this parameter expires, Cisco CallManager removes the expired entries during the next RIS database cleanup time (specified in the RIS Cleanup Time of the Day parameter). Default setting: 3 Minimum: 1 Maximum: 30 Unit: days
RIS Unused CTI Records Storage Period	Specifies the RIS database information storage period for any closed provider, device, or line information from the CTI Manager. After the time specified in this parameter expires, Cisco CTI Manager removes the expired entries during the next RIS database cleanup time (specified in the RIS Cleanup Time of the Day parameter). Default setting: 1 Minimum: 0 Maximum: 5 Unit: days

Service Parameter	Description
RIS Maximum Number of Unused CTI Records	Specifies the maximum number of records for closed CTI providers, devices, and lines that is kept in the RIS database. After the limit specified in this parameter reaches, Cisco CTI Manager does not save any new record for unused CTI providers, devices, or lines to the RIS database. Default setting: 3000 Minimum: 0 Maximum: 5000 Unit: records
TLC Throttling Enabled	Enables or disables Trace and Log Central throttling behavior. Default setting: True
TLC Throttling IOWait Goal	Specifies the system IOWait percentage that TLC throttles towards itself. Default setting: 10 Minimum: 10 Maximum: 40
TLC Throttling CPU Goal	Specifies the system CPU utilization percentage that TLC throttles towards itself. Default setting: 80 Minimum: 65 Maximum: 90
TLC Throttling Polling Delay	Specifies the minimum delay in milliseconds between IO wait and CPU usage polls for the purpose of trace collection throttling. Default setting: 250 Minimum: 200 Maximum: 2000
TLC Throttling SFTP Maximum Delay	Specifies the maximum time an SFTP transfer is paused in order to prevent timeouts. This is a required field. Default setting: 5000 Minimum: 1000 Maximum: 10000
Maximum Number of Processes and Threads	Specifies the maximum number of Processes and Threads running on the machine. If the total number of Processes and Threads on the machine has exceeded the maximum number, SystemAccess sends TotalProcessesThreadsExceededThresholdStart alarm and the corresponding alert is generated. Default setting: 2000 Minimum: 1000 Maximum: 3000
Enable Logging	Determines whether collecting and logging of troubleshooting perfmon data is enabled (True) or disabled (False). Default setting: True
Polling Rate	Specifies the troubleshooting perfmon data polling rate, in seconds. Default setting: 15 Minimum: 5 Maximum: 300 Unit: seconds

Service Parameter	Description
Maximum No. of Files	Specifies the maximum number of troubleshooting perfmon log files that are saved on disk. If the "Maximum No. of Files" is set to a large number, the "Maximum File Size" be reduced. **Note** If this value is reduced, excessive log files with the oldest time stamp is deleted if Troubleshooting Perfmon Data Logging is enabled and RISDC is turned on. If desired, please save these files first before changing Maximum No. of Files. Default setting: 50 Minimum: 1 Maximum: 100
Maximum File Size (MB)	Specifies the maximum file size, in megabytes, in each troubleshooting perfmon log file before the next file is started. If the "Maximum File Size" is set to a large number, the "Maximum No. of Files" should be reduced. Default setting: 5 Minimum: 1 Maximum: 500
Cisco Serviceability Reporter	
RTMT Reporter Designated Node	Specifies the designated server on which RTMTReporter runs. It is desirable that this server is a non-callprocessing server since RTMT Reporter service is CPU intensive. This field is automatically filled in with the local server IP at which Reporter is first turned on.
RTMT Report Generation Time	Specifies the number of minutes after midnight (00:00hrs) when the Real-Time Monitoring Tool, (RTMT) reports are generated. To reduce any impact to call processing, run non-real-time reports during non-production hours. Default setting: 30 Minimum: 0 Maximum: 1200
RTMT Report Deletion Age	Specifies the number of days that must elapse before reports are deleted. For example, if this parameter is set to 7, reports that were generated seven days ago get deleted on the eighth day. A value of 0 disables report generation, and any existing reports get deleted. Default setting: 7 Minimum: 0 Maximum: 30

Plugins

Application plugins extend the functionality of Unity Connection. For example, the Real-Time Monitoring Tool (RTMT) allows you to monitor the health of the system remotely through tools, such as performance-monitoring counters and the Port Monitor.

Real-Time Monitoring Tool

The Real-Time Monitoring Tool (RTMT) that runs as a client side application, uses HTTPS and TCP to monitor system performance, device status, device discovery, and CTI applications for Unity Connection. RTMT can connect directly to devices via HTTPS to troubleshoot system problems. RTMT can also monitor the voice messaging ports on Unity Connection.

RTMT allows you to do the following tasks:

- Monitor a set of predefined management objects that focus on the health of the system.
- Generate various alerts in the form of emails, for objects when values go over or below user-configured thresholds.
- Collect and view traces in various default viewers that exist in RTMT.
- View syslog messages and alarm definitions in SysLog Viewer.
- Work with performance-monitoring counters.
- Monitor the voice messaging ports on Unity Connection.

When a Unity Connection cluster is configured, you can open multiple instances of RTMT to monitor voice messaging ports on each server in the Unity Connection cluster.

For more information, see the Cisco Unified Real-Time Monitoring Tool Administration Guide for the required release, available at http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html.

Note Before you install any plugins, you must disable all intrusion detection or anti-virus services that run on the server where you want to install the plugin.

Installing a Plugin in Unity Connection

Step 1 In Cisco Unity Connection Administration, expand **System Settings** and select **Plugins**.

Step 2 On the Search Plugins page, select **Find** to select the plugin you want to install.

Step 3 Select **Download** and follow the on screen instructions for installing the plugin.

Fax Server

Fax integration in Unity Connection enables the users to receive faxes in the mailboxes and forward the received faxes to other users or fax machines for printing. Users manage faxes using phone, Messaging Inbox, or IMAP client. For more information, see the Fax Server chapter.

LDAP

The LDAP integration allows to import users from and synchronize the users with a supported corporate directory to maintain single directory information database. For more information, see the LDAP chapter.

SAML Single Sign On

Security Assertion Markup Language Single Sign On (SAML SSO) is an enhancement to the existing sign on feature. SAML SSO allows a user to gain single sign on access with Unity Connection subscriber web interfaces and across the administrative web applications on the following Unified Communications products:

- Unity Connection
- Cisco Unified Communications Manager
- Cisco Unified IM/ Presence

SAML SSO supports both LDAP and non LDAP users to gain single sign on access to web applications. For more information on SAML SSO, see the Quick Start Guide for SAML SSO in Cisco Unity Connection, Release 15, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/quick_start/guide/b_15cucqssamlsso.html.

Authz Server

Unity Connection enhances the SAML SSO and non SSO login experience for Jabber users by providing the support of OAuth 2.0 Authorization Code Grant Flow. For faster login, Authorization Code Grant Flow requires an Authorization Server (Authz Server) to provide the access and refresh tokens to the Jabber client. In Unity Connection, the publisher server of Cisco Unified CM associated with a phone system is configured as an Authz server. After configuring an Authz server, Unity Connection uses the authorization keys provided by the Authz server to validate the token of a Jabber client. If authorization keys are changed on Cisco Unified CM, you must synchronize the keys between Unity Connection and Authz server. You can configure multiple Authz server by providing the credential of Cisco Unified CM associated with the phone system.

Note In multisite deployment where CUCM SME is installed, you can configure the publisher server (where Jabber end points are connected) of every leaf cluster as an Authz server for connecting with Unity Connection.

To configure an Authz server, see Configuring an Authz Server in Unity Connection

Consider the following points while configuring the Authz server in Unity Connection:

- Make sure that OAuth Authorization Code Grant Flow feature is enabled on both Cisco Unified CM and Cisco Unity Connection.

  By default, the OAuth flow is disabled on Cisco Unity Connection. To enable the feature, navigate to System Settings > Enterprise Parameters in Cisco Unity Connection Administration. On Enterprise Parameters page, enter the applicable settings under **SSO and OAuth Configuration** field and select the Enabled option for **OAuth with Refresh Login Flow**.

- The username and password entered for the Authz server must be same as the username and password of the system administrator of Cisco Unified CM.
- The Tomcat services of Cisco Unified CM are up and running.
- Make sure to upload the valid certificates of Cisco Unified CM to the tomcat trust of Cisco Unity Connection or check the **Ignore Certificate Errors** check box to ignore the certificate validation errors for the Authz server.

For more information on certificates, see "Security" chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html.

- The version of Jabber client must be 11.9 and later.
- The version of Cisco Unified CM must be 11.5.1 SU3 and later.

Configuring an Authz Server in Unity Connection

To configure an Authz server in Unity Connection, do the following procedure:

Step 1 In Cisco Unity Connection Administration, expand **System Setting** and select **Authz Server**. The Search Authz Server page appears displaying the currently configured Authz servers.

Step 2 Configure an Authz server (For more information on each field, see Help> This Page):

- To add an Authz server :
  1. **a.** Select **Add New**. The New Authz Server page appears.
  2. **b.** Enter the required information in the field.
  3. **c.** Select **Save**.
- To update an Authz server:
  1. **a.** Select the Authz server that you want to edit. The Edit Authz Server page appears.
  2. **b.** Edit the Authz server settings as required.
  3. **c.** Select **Save**.
- To delete an Authz server:
  1. **a.** Check the check box adjacent to the display name of the Authz server that you want to delete.
  2. **b.** Select **Delete Selected**.
  3. **c.** Select **OK** to confirm the deletion.

  You can delete multiple Authz server by selecting more than one check box at a time.

Cross-Origin Resource Sharing (CORS)

CORS is a specification that allows client applications to process cross-origin requests in a more secure way. Typically for a web application, cross-origin requests from the original domain (where the application originated) to another domain are forbidden by the web browser due to a Single Origin Policy. CORS provide a way for the web browser and server to interact and determine whether or not to allow cross-origin request. CORS standard uses HTTP headers to establish an agreement between the web browser and the Unity Connection server to provide services to permitted domains.

Unity Connection provides support to the client applications of a cross domain server to access content on a Unity Connection server directly by creating an entry for cross domain server in Unity Connection. The entry for cross domain server must pre-exist in Unity Connection to process the CORS requests.

Unity Connection has extended the Single Sign On (SAML SSO) endpoint to support CORS.

Note CORS functionality is supported by Unity Connection 10.5 and later releases using VMRest APIs.

Configuring CORS in Unity Connection

Step 1 In Cisco Unity Connection Administration, expand System Settings and select Cross-Origin Resource Sharing (CORS).

The Search Cross-Origin Resource Sharing page appears displaying the currently configured CORS.

Step 2 Configure Cross-Origin Resource Sharing (For more information on each field, see Help> This Page):

- To add a CORS:

  On the Search Cross-Origin Resource Sharing page, select Add New.

  On the New Cross-Origin Resource Sharing page, enter the values of the required fields and select Save.

- To edit an existing CORS:

  On the Search Cross-Origin Resource Sharing page, select the CORS that you want to edit.

  On the Edit Cross-Origin Resource Sharing page, enter the values of the required settings and select Save.

- To delete one or more CORS:

  On the Search Cross-Origin Resource Sharing page, select the CORS that you want to delete.

  Select Delete Selected to delete the CORS.

SMTP Configuration

The SMTP configuration is a type of messaging that allows users to send and receive Unity Connection voice messages. For more information on SMTP configuration and messaging, see the Messaging chapter.