User Attributes

- User Attributes, on page 1

User Attributes

Overview

Cisco Unity Connection users are created to administer or provide access to the voice messaging system. The user attributes are the objects that enable you to control which users can connect to the system, and determine the system features and resources they can access.

Preparing to Add User Accounts

You need to select and define user attributes before adding user accounts in Unity Connection. The settings defined by each attribute helps determine which features are available to the users and callers, define limits, and permissions for using Unity Connection resources.

Following are the user attributes that should be configured before adding user accounts individually or in bulk:

- Class of Service: The class of service enables you to define the control access to critical features on Unity Connection. The class of service membership enables applies the class of service settings to all the member users. See the Class of Service, on page 2 section.
- User Templates: The user template settings are applied to the newly created user accounts and enables you to create predefined configurations for the majority of user settings. Any changes made to the user template settings do not affect the existing user accounts associated with that template. See the User Templates, on page 6 section.
- Mailbox Stores: Unity Connection allows you to create multiple mailbox stores that can be useful for customers with large installations, where the time required to complete a backup is an issue. Before you add user accounts, review the mailbox store that is specified in the user template that you plan to use. You may need to edit the template to specify a different mail store, or create a new template. If you change the mailbox store specified in a user template, any already-created user accounts that were based on that template are not re-assigned to the new mailbox store. However, you can reassign a user to a different mailbox store at any time. To configure the mailbox stores, see the Message Storage chapter.

- Dial Plan: The dial plan in Unity Connection includes partitions and search spaces. Partitions and search spaces provide a way to segregate the global dial and message addressing space within Unity Connection. A partition comprises a logical grouping of objects, such as users and call handlers. The objects are identified by extension, name or SMTP address. A search space contains an ordered list of partitions. See the Dial Plan section.
- Schedules: Unity Connection uses schedules to determine which user transfer rule to apply and which user greeting to play. Before you add user accounts, review the active schedule that is specified for the template that you plan to use. You may need to edit the template to specify a different schedule or create a new template. If you change the active schedule specified on a user template page, any already-created user accounts that were based on that template are not reassigned to the new schedule. In contrast, when you edit a schedule, the changes affect both new and existing users of that schedule. This means that you can update schedule settings before and after you create user accounts. You can also reassign a user to a different schedule at any time. For more information on managing holiday and schedules, see the Schedules and Holiday Schedules sections.
- Roles: Unity Connection offers levels of privileges for administrator accounts, set according to a list of predefined roles. Roles specify which tasks administrators can do. Before you add administrator accounts, select the roles that are assigned to each account. You can change which roles are assigned to the accounts at any time. For more information, see the Roles section.

Class of Service

A class of service (COS) defines limits and permissions for accounts with voice mailboxes. For example, a COS:

- Controls user access to licensed features, such as Web Inbox or Messaging Inbox (When a COS includes access to a feature that requires individual licenses, you can assign groups of users to the COS only if enough licenses are available.)
- Controls user access to non licensed features, such as Personal Call Transfer Rules and digital networking.
- Controls how users interact with Unity Connection. For example, a COS dictates the maximum length of user messages and greetings, and whether users can choose to be listed in the corporate directory.
- Controls call transfer options.
- Specifies the number of private distribution lists allowed to users, and the number of members allowed on each list.
- Specifies the restriction tables used to control the phone numbers that users can use for transfers and when placing calls.

A COS is not specified for the individual accounts or templates that are associated with users without voice mailboxes or the administrator accounts.

Remember that if you change the COS that is specified on a user template page, any user accounts that have already been created based on that template are not reassigned to the new COS. In contrast, when you edit the settings in a COS, the changes affect both new and existing members, so you can edit COS settings before and after you create user accounts. You can also reassign a user to a different COS at any time.

Default Class of Service

Unity Connection creates two predefined classes of service that you use when setting up the system.

- System: The system class of service is assigned to the administrator (users without voicemail box accounts). This class of service cannot be deleted.
- Voice Mail User COS: The voicemail user class of service is assigned to the user accounts with voicemail boxes. This class of service cannot be deleted.

Configuring Class of Service

This section includes information on configuring a class of service for Unity Connection, define the settings for the class of service and save them.

Step 1 In Cisco Unity Connection Administration, expand Class of Service, and then select Class of Service.

The Cisco Unity Connection Administration displays the currently configured class of services.

Step 2 Configure a class of service (For information on each field, see Help> This Page):

- To add a class of service, select Add New. On the New Class of Service page, enter the applicable settings and select Save.
- To edit a single class of service, select that COS and to edit multiple class of services, check the applicable check boxes and then select Bulk Edit.
  1. On the Edit Class of Service page, edit the class of service settings.
  2. After editing the settings, select Save.
- To delete a class of service by selecting the applicable check boxes of the class of services you want to delete. Select Delete Selected.

Class of Service Membership

The class of service membership allows to add user accounts to a particular class of service containing the required features enabled in the COS.

Step 1 In Cisco Unity Connection Administration, expand Class of Services, then select Class of Service Membership.

Step 2 Select the class of service members by checking the applicable check boxes and select Move Selected.

Class of Service Settings

You can specify the settings, such as live reply and private distribution lists for the user accounts based on the selected class of service.

Live Reply

When live reply is enabled, users listening to messages over phone can reply to a message or user calls the sender. You can use COS settings to specify whether users can live reply only to messages from other users, or to messages from both users and unidentified callers (unidentified callers are outside callers or users who are forwarded to Unity Connection but who cannot be identified by the calling extension).

Users can live reply to a message using the touchstone conversation or the voice-recognition conversation. Consider informing users when you enable this feature, because even when it is enabled, the live reply option is not mentioned in the main phone menus for some phone conversation types.

The following points to be considered for live reply to users:

- Unity Connection dials the extension of the user who left the message only when the Transfer Incoming Calls to User's Phone setting for the user who left the message is set to ring an extension or another number.

Note The Transfer Incoming Calls to User's Phone field is on the Call Transfer page.

- The call transfer settings for the user who left the message dictate what Unity Connection does when the user phone is busy, and whether Unity Connection screens the call.
- If a user attempts to live reply to a message but the sender is unavailable to take the call, a reply message left for the sender is correctly identified as been sent by the user if the user called from a primary or an alternate extension. This is because Unity Connection releases the live reply call to the phone system and the user is no longer signed in to Unity Connection when leaving the reply message.

The following considerations for live reply to unidentified callers:

- Unity Connection uses the calling number provided by the phone system in the Automatic Number Identification (ANI) string. To initiate the live reply, Unity Connection checks the ANI digits against the transfer restriction table associated with the class of service of the user. If the number is allowed, Unity Connection returns the call by performing a release transfer to the phone system.
- You can configure a prefix that Unity Connection prepends to the ANI string and the minimum length of the ANI string before the prefix is applied. For example, to prepend a trunk access code to all numbers of a sufficient length, or to provide additional information that the phone system may need to process the number. Any other formatting that must be done to generate a proper dial string must be performed by the phone system.

Private Distribution Lists

COS settings allow you to specify the maximum number of lists that are available to users and the maximum number of members that users can add to each list when they use the Unity Connection conversation or the Messaging Assistant to manage the lists.

You can set the maximum number of lists, up to 99, available to each user assigned to the COS.

While both the Unity Connection conversation and the Messaging Assistant use this COS setting to determine when a user has reached the maximum number of lists, each application calculates differently the number of lists that a user owns:

- When a user uses the phone to create a new list by adding members, the Unity Connection conversation counts the number of private lists that have members and compares the total to the value in this setting to determine whether the user has reached the list limit. Lists with no members (empty lists) are not included in the total number of lists that a user owns, even if the lists have recorded names or text names.
- When a user uses the Messaging Assistant to create a new list, the Messaging Assistant counts the number of lists that have a recorded name, a text name, or members, and then compares the total to the value in

this setting to determine whether the user has reached the list limit. Lists with no members are included in the total number as long as they have recorded names or text names.

This means that if a user belongs to a COS that allows 15 lists and the user has 12 private lists with members and two lists with recorded names but no members, the user can potentially create more lists by phone than in the Messaging Assistant before reaching the list limit.

- When the user uses the Unity Connection conversation, the user reaches the list limit either by adding members to the two empty lists and creating one new list, or by creating three new lists. If the user reaches the limit by creating three new lists, the user cannot add members to the two empty lists until two lists are deleted.
- When the user uses the Messaging Assistant, the user reaches the list limit by creating one new list. Despite reaching the list limit, the user can add members to the two empty lists.

Recorded Name and Length

For each COS, you can specify whether users are allowed to record the names and the length of the recorded name.

Hearing a name recorded in the voice of the user can help callers distinguish between users with similar names. When allowed to record the names, users can either use phone conversation or Messaging Assistant to do the recording and they are prompted to complete the task during first time enrollment.

Note Unity Connection does not prevent users from completing the enrollment process if they do not record a name.

When Unity Connection users have no recorded name, Unity Connection uses the Text to Speech feature to play the username (either the display name or the concatenated first and last name, depending on which name is entered in Unity Connection Administration). The recorded names can give callers an extra level of assurance that they are reaching the person or mailbox they intended to reach. You must record the usernames at the first time enrollment. This assists the callers in understanding names.

SpeechView Transcriptions of Voice Messages

When the SpeechView feature is enabled, Unity Connection uses a third-party external transcription service to convert voice messages into text.

To use SpeechView, users must belong to a class of service that provides transcriptions of voice messages. Members of the class of service can view the transcriptions of the messages using an IMAP client configured to access the messages. The original voice message is still attached to the transcribed text message. Users can optionally configure an SMS or SMTP notification device so that Unity Connection sends the transcription to a phone or external email address.

Video

In Unity Connection, for each COS, the administrator can specify whether the users are allowed to record and play video greetings and messages. The administrator allows to play video greetings and messages for both the identified and outside callers. Unity Connection also allows the identified callers to record video greetings and messages.

The video greeting and messages settings enable the administrators to control whether the members of a class of service can record video greetings or messages nd if the video greetings and messages can be played for outside callers.

Note Unity Connection classifies remote users connecting through an intersite, intrasite, or HTTPS link as outside callers.

To allow the outside callers to access video greetings and messages, you need to enable the enable class of service settings for video greetings and messages, navigate to **Cisco Unity Connection Administration> Class of Service> Edit Class of Service> check the Enable Video** check box.

You can enable or disable the check box to allow the users to play and record video greetings and messages.

User Templates

Each user and administrator account that you add in Unity Connection is based on a user template. The user template settings include authentication rules and schedules. The authentication rules dictate the password or PIN and account lockout policy for the users that you create.

You must review the settings in the user templates that you plan to use before creating a user account. This helps you to determine whether you need to make changes to an existing user template or create new user templates. For each template, consider the features that you want to enable, specify a class of service, set a schedule and time zone for the accounts you want to create.

To minimize the number of modifications that you need to make to user accounts later, use a separate user template to specify settings applicable for each group of users that you plan to create. For example, if you plan to create accounts for the members of a sales department, create or edit an existing template to set up message notifications. Specify that messages left for the sales employees are encrypted for extra security, increase the length of messages that callers can leave, and make similar appropriate changes to settings that control the conversation heard by the sales employees.

If a particular setting must be unique for each user account, leave that setting blank on the user template, and then you can edit the setting for each user account after they are created.

Default User Templates

Unity Connection has two predefined user templates that you can edit but cannot delete.

Voicemail User Template	The settings on this template are suitable for most users.
Administrator Template	The settings on this template are suitable for users who administer Unity Connection. User accounts that are based on this template do not have voice mailboxes. By default, the template specifies the System Administrator role, which is the administrator role with the highest privileges.

Configuring User Templates

This section includes information on configuring a user template for Unity Connection, defining the settings for the user template, and saving them.

Note You can manage the user templates using the Bulk Administration Tool. For more information, see the Bulk Administration Tool section.

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

The Search User Templates page displays the default and currently configured user templates.

Step 2 Configure a user template (For information on each field, see Help> This Page):

- To add a user template, select Add New. The New User Template page appears. Enter the applicable settings and select Save.
- To edit a user template, select the user template that you want to edit. On the Edit User Template Basics page, select the applicable settings from the Edit menu:
  - User Template Basics
  - Password Settings
  - Change Password
  - Roles
  - Transfer Rules
  - Message Settings
  - Message Actions
  - Caller Input
  - Mailbox
  - Phone Menu
  - Playback Message Settings
  - Send Message Settings
  - Greetings
  - Post Greeting Recording
  - Notification Devices
  - Unified Messaging Accounts
  - Video Services Accounts

  Note For more information on each user template setting, see the Settings for User Accounts and User Templates section.

- To delete a user template, select the user template 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 predefined roles that come installed with Unity Connection. You cannot create, modify or delete these roles. System roles can only be assigned or unassigned to users by System Administrator.
- **Custom Roles**: Custom roles are the roles that you create with a list of privileges based on your organizational requirements. Custom roles can be assigned or unassigned to users by System Administrator or a custom role user with role assignment privilege.

Note Only a user with System Administrator role can create, update or delete custom roles.

System Roles

At the time of Unity Connection installation, default system roles are created for various administrative functions, as mentioned in below table.

Read Only Administrator System Role

With Unity Connection 12.5(1) and later, a new system role **Read Only Administrator** is introduced that provides the read only access of Unity Connection functions to the administrator.

System Role	Description
Audio Text Administrator	This role allows an administrator to manage call handlers, directory handlers, and interview handlers.
Audit Administrator	This role allows an administrator to enable or disable Unity Connection application and database auditing, to configure audit settings, and to view or delete audit logs.
Greeting Administrator	This role allows an administrator to manage call handler recorded greetings for the Unity Connection users via TUI. **Note** You need to assign this role to a User with Voice Mailbox account because the administrator must be able to access Unity Connection by phone.

Help Desk Administrator	This role allows an administrator to reset user passwords and PINs, unlock user accounts, and view user setting pages. **Note** The "Manage Call Handlers Belonging To Users Only - View Only" privilege refers to the primary call handler assigned to a user which include all greetings, transfer rules, and menu entries that you see on the User's page under the Roles section.
Mailbox Access Delegate Account	This role allows an administrator to access to all messages. Remote applications, for example, Cisco Unified Mobility Advantage use the username and password of a user with this role for the purposes of retrieving messages on behalf of other users. Typically, this role is assigned to only one user account, which does not represent a real user but exists to access mailboxes on behalf of other users.
Read Only Administrator *(applicable with Unity Connection 12.5(1) and later)*	This role allows an administrator to view all the Unity Connection administrative functions such as system settings configurations and reports. **Note** This role also provides access to view the Clusters, Enterprise Parameters, LDAP, SAML SSO, Service Parameters, Plugins pages under System Settings on Cisco Unity Connection Administration. You can view the Cisco Unified Serviceability and RTMT client also with this role.
Remote Administrator	This role allows an administrator to administer the database using remote tools.
System Administrator	This is the top-level Unity Connection administration role. This role allows access to all Unity Connection administrative functions, including users, system settings configurations, reports, along with the administration and diagnostic tools. The default administrator account that the installer specified during initial setup of Unity Connection is set to this role. A System Administrator is the only role that has permission to create administrative accounts.

Technician	This role allows an administrator to access all functions that enable management of the Unity Connection server and phone system integration settings; administrators with this role can also run all reports, use diagnostic tools, and view all system and user settings pages.
User Administrator	This role allows an administrator to manage user accounts, access all user administration functions and user administration tools.

You can assign the above mentioned roles to the users with mailboxes except the Greeting Administrator role. As a best practice, make sure that administrators have two accounts: one without a voice mailbox for administering Unity Connection and another with a voice mailbox that they can use to access the personal mailbox.

To see the specific privileges for each administrator role, in Cisco Unity Connection Administration, expand **System Settings > Roles > System Roles** and select the name of each role. You cannot make changes to the permissions that are associated with each predefined role.

Custom Roles

Unity Connection allows the system administrator to create, update, or delete custom roles with different privileges as per the requirements, where each privilege is associated with an operation or a set of operations. Custom role can be assigned to a user having no role as well as to the user who already has a system or a custom role.

Note A user with custom role cannot assign system role to a user and cannot modify or delete a user with system role.

Custom Roles are created by selecting a privilege or set of privileges.

Unity Connection 12.5(1) and later provides an option to inherit a system role while creating a custom role. All the privileges associated with the inherited system role are assigned to the custom role. You cannot unassign or remove the privileges of inherited system role. As per the requirement, you can assign other privileges to the custom role as well.

Note With Unity Connection 12.5(1) and later, each new custom role has read only access privilege by default.

Below table describes the Unity Connection privileges that can be selected while creating a custom role:

Privilege to Manage Users	
Manage Users - Full Access	Allows the administrator to manage users and all of their attributes.
Manage Users: Assign/Unassign Roles	Allows the administrator to assign or unassign different custom roles to users.

Manage Users: User Name Attributes - View, Update	Allows the administrator to change the user name attributes like First Name, Display Name, Voice Name etc.
Manage Users In Bulk - Full Access	Allows the administrator to perform user bulk operations.
Read Access to System Configuration Data - Read Access *(applicable only for Unity Connection 12.0(1) and 11.5(1))*	Allows the administrator to have Read Only access to the Cisco Unity Connection Administration page. **Note** It is mandatory to select this privilege while creating a custom role. Also, this privilege does not provide access to Clusters, Enterprise Parameters, LDAP, SAML SSO, Service Parameters and Plugins.
Privilege to Manage Class of Service	
Class of Service - Full Access	Allows the administrator to manage class of service and assign/unassign it to users through class of service membership page.
Privileges to Manage Templates	
Templates: User Templates - Full Access	Allows the administrator to manage user templates.
Manage Call Handlers Greetings - Full Access	Allows the administrator to manage system call handler greetings.
Manage Call Handler Templates And System Call Handlers- Full Access	Allows the administrator to manage call handler templates and system call handlers.
Manage Call Handler Templates And System Call Handlers- View, Create, Update	Allows the administrator to create and modify call handler templates and system call handlers. Delete action is not allowed with this privilege.
Templates: Notification Templates - Full Access	Allows the administrator to manage notification templates.
Privilege to Manage Distribution Lists	
Distribution Lists - Full Access	Allows the administrator to manage distribution lists.
Privileges to Manage Call Management	
Call Management: Directory Handlers - Full Access	Allows the administrator to manage directory handlers.
Call Management: Directory Handlers - View, Create, Update	Allows the administrator to create and modify directory handlers. Delete action is not allowed with this privilege.
Call Management: Interview Handlers - Full Access	Allows the administrator to manage interview handlers.
Call Management: Interview Handlers - View, Create, Update	Allows the administrator to create and modify directory handlers. Delete action is not allowed with this privilege.

Call Management: Call Routing Rules - Full Access	Allows the administrator to manage call routing rules.
Privilege to Manage Message Storage	
Message Storage - Full Access	Allows the administrator to manage mailbox stores, mailbox quota, mailbox store membership and message aging policies.
Privileges to Manage Networking	
Networking: VPIM - Full Access	Allows the administrator to create VPIM locations and manage them.
Manage Networking And Server Roles/Activation/Deactivation - Full Access	Allows the administrator to manage networking, server configurations and activation/deactivation of services.
Privileges to Manage Unified Messaging	
Unified Messaging: Configuration - Full Access	Allows the administrator to integrate Unity Connection with unified messaging servers such as Microsoft Exchange, Office 365 etc. and manage the unified messaging accounts. **Note** Select "Manage Users - Full Access" privilege to associate users with the unified messaging account.
Unified Messaging: Speechview Transcription - Full Access	Allows the administrator to manage speechview services.
Privilege to Manage Video	
Video Service - Full Access	Allows the administrator to manage video service and assign them to users.
Privilege to Manage Dial Plan	
Dial Plan: Partitions and Search Spaces - Full Access	Allows the administrator to manage partitions and searchspaces.
Privileges to Manage System Settings	
System Settings - Full Access	Allows the administrator to manage all the System Settings operations except Enterprise Parameters, Cluster, LDAP, SAML SSO, Service Parameters, Custom Roles and Plugins.
System Settings: Advanced - Full Access	Allows the administrator to manage advanced settings.
System Settings: General Configuration - Full Access	Allows the administrator to manage general configurations.
System Settings: Authentication Rules - Full Access	Allows the administrator to manage authentication rules.
System Settings: Cluster, Plugins, LDAP, SAML, Enterprise and Service Parameters - Full Access	Allows the administrator to manage Cluster, Enterprise Parameters, SAML SSO, LDAP, Service Parameters and Plugins.

System Settings: Restriction Tables - Full Access	Allows the administrator to manage restriction tables.
System Settings: Schedules, Holidays - Full Access	Allows the administrator to manage system schedules and holidays.
System Settings: Global Nicknames - Full Access	Allows the administrator to manage global nicknames.
System Settings: Subject Line Formats - Full Access	Allows the administrator to edit subject line formats.
System Settings: Attachment Descriptions - Full Access	Allows the administrator to manage attachment descriptions.
System Settings: Enterprise Passwords - Full Access	Allows the administrator to manage enterprise password settings.
System Settings: Fax Server - Full Access	Allows the administrator to manage fax servers.
System Settings: SAML And LDAP - Full Access	Allows the administrator to integrate SAML and LDAP with Unity Connection.
System Settings: LDAP Phone Number Transforms - Full Access	Allows the administrator to manage ldap phone number transform settings.
System Settings: CORS - Full Access	Allows the administrator to manage cross origin resource sharing.
System Settings: SMTP Configuration - Full Access	Allows the administrator to manage SMTP configurations.
Privilege to Manage Phone System Integration	
Telephony Integrations - Full Access	Allows the administrator to manage telephony integrations.
Privileges to Manage Tools	
Tools: Task Management - Full Access	Allows the administrator to schedule and execute Unity Connection tasks.
Tools: Run Administration Tools	Allows the administrator to execute administrative tools such as Grammar Statistics , SMTP Address Search and Show Dependencies.
Tools: Custom Keypad Mapping - Full Access	Allows the administrator to manage custom keypad mappings.
Privileges to Manage User MWI and Password Settings	
Reset User MWI	Allows the administrator to reset user MWIs.
Reset User Passwords	Allows the administrator to reset user passwords.
Privilege to Run Unity Connection Serviceability	
Run Serviceability Page	Allows the administrator to access the Cisco Unity Connection Serviceability page.

To perform different operations on Unity Connection, administrator must provide the required privilege to the role and assign the role to a user. The table below describes different Unity Connection operations and the privileges required to perform the operations.

Table 1: Privileges Required for Each Unity Connection Operation

Operation	Sub - Operation	Set of Privileges
Manage Users This operation allows you to manage user accounts on Unity Connection.	Users	Manage Users - Full Access **Note** Select the Manage "Users: Assign/Unassign Roles" privilege for custom role assignment or unassignment.
	Import Users	
	Synch Users **Note** For Import Users and Sync Users operation, you must have LDAP or AXL configured on Unity Connection.	
Manage Class of Service (COS) This operation allows you to manage class of services and assign them to different users through Class of Service Membership page on Unity Connection.	Class of Service	Class Of Service - Full Access
	Class of Service Membership	
Manage Templates This operation allows you to manage different types of templates. For each sub operation associated with the templates, separate privileges are defined to provides access only to that sub operation.	User Templates	Templates: User Templates - Full Access
		Manage Users - Full Access
	Call Handler Template	Manage Users - Full Access Manage Call Handler Templates And System Call Handlers- Full Access
	Contact Template	Templates: User Templates - Full Access
	Notification Template	Templates: Notification Templates - Full Access
Manage Contacts This operation allows you to manage contacts.	Contacts	Manage Users - Full Access
Manage Distribution Lists This operation allows you to manage distribution lists..	System Distribution List	Distribution Lists - Full Access

Operation	Sub - Operation	Set of Privileges
Manage Call Management This operation allows you to manage System Handlers and Call Routing rules. For each sub operation associated with the call management, separate privileges are defined to provides access only to that sub operation.	System Call Handler	Manage Users - Full Access Manage Call Handler Templates and System Call Handlers - Full Access
	Directory Handler	Call Management: Directory Handlers - Full Access
	Interview Handler	Call Management: Interview Handlers - Full Access
	Custom Recordings	Manage Call Handler Templates and System Call Handlers - Full Access
	Call Routing	Call Management: Call Routing Rules - Full Access
Manage Message Storage This operation allows you to manage the mailbox and message storage settings.	Mailbox Stores	Message Storage - Full Access
	Mailbox Stores Membership	
	Mailbox Quotas	
	Message Aging	
Manage Networking This operation allows you to manage networking on Unity Connection server.	Legacy Link	Manage Networking and Server Roles/ Activation/Deactivation - Full Access
	Branch Management	
	HTTPS Links	
	Locations	
	VPIM (Full Access)	Networking: VPIM - Full Access
	Connection Location Passwords	Manage Enterprise Passwords- Add/Delete/Modify passwords
Manage Unified Messaging This operation allows you to manage unified messaging services and assign them to users.	Unified Messaging Services	Unified Messaging: Configuration - Full Access Manage Users - Full Access
	Unified Messaging Account Status	
	SpeechView Transcription	Unified Messaging: SpeechView Transcription - Full Access
Manage Video This operation allows you to manage Video services and assign the services to the users.	Video Services	Video Service - Full Access
	Video Services Account Status	
Manage Dial Plan This operation allows you to manage Unity Connection partitions and search spaces.	Partitions	Dial Plan: Partitions and Search Spaces - Full Access
	SearchSpaces	

Operation	Sub - Operation	Set of Privileges
Manage System Settings This operation allows you to manage system configurations. Along with the privilege to manage all the System Settings operations, separate privileges are defined for each sub operation to provide access only to that sub operation.	System Settings	Manage System Settings - Full Access **Note** This privilege provides access to manage the complete System Settings operations except Custom Roles, Cluster, LDAP, SAML SSO and Enterprise Parameters, Service Parameters and Plugins.
	General Configuration	System Settings: General Configuration - Full Access
	Cluster	System Settings: CUCM Inherited Settings - Full Access
	Authentication Rules	System Settings: Authentication Rules - Full Access
	Restriction Table	System Settings: Restriction Tables - Full Access
	Schedules	System Settings: Schedules, Holidays - Full Access
	Holiday Schedules	
	Global Nicknames	System Settings: Global Nicknames - Full Access
	Subject Line Format	System Settings: Subject Line Formats - Full Access

Operation	Sub - Operation	Set of Privileges
	Attachment Description	System Settings: Attachment Descriptions - Full Access
	Enterprise Parameters	System Settings: Cluster, Plugins, LDAP, SAML, Enterprise and Service Parameters - Full Access
	Service Parameters	
	Plugins	
	Fax Server	System Settings: Fax Server - Full Access
	LDAP	System Settings: SAML And LDAP - Full Access
	SAML Single Sign On	
	Cross Origin Resource Sharing	System Settings: CORS - Full Access
	SMTP Configurations	System Settings: SMTP Configuration - Full Access
	Advanced	System Settings: Advanced - Full Access
Manage Telephony Integrations This operation allows you to manage Telephony Integrations.	Phone System	Telephony Integrations - Full Access
	Port Group	
	Port	
	Speech Connect Port	
	Trunk	
	Security	
Manage Tools This operation allows you to access different tools and utilities for administering Unity Connection along with scheduling tasks for various operations.	Task Management	Tools: Task Management - Full Access
	Bulk Administration Tool	Manage Users In Bulk - Full Access
	Custom Keypad Mapping	Tools: Custom Keypad Mapping - Full Access
	Migration Utilities	Manage Users In Bulk - Full Access
	Grammar Statistics	Tools: Run Administration Tools
	SMTP Address Search	
	Show Dependencies	

Operation	Sub - Operation	Set of Privileges
Manage Serviceability This operation allows you to access both the Unity Connection and the Unified Communication Serviceability page.	Cisco Unified Serviceability	Run Serviceability Page
	Cisco Unity Connection Serviceability	System Settings: Cluster, Plugins, LDAP, SAML, Enterprise and Service Parameters - Full Access Run Serviceability Page

Example to Use Custom Roles

Unity Connection offers a predefined system role **Technician** to manage various system settings and networking related operations along with the administrative tasks such as reset of user MWI etc.

If you want a user to perform all the operations of the technician role along with some additional operations such as reset passwords and managing Unity Connection tasks, you must create a custom role with the same privileges as of the technician role, provide the privileges for password reset and task management to the role, and assign the role to user.

To create a custom role as per the above example, do the following:

Step 1 *(For Unity Connection 12.0(1) and 11.5(1))* Create a new role **Custom Technician** and provide the following privileges to create a custom role equivalent to the Technician system role:

- Read Access to System Configuration Data - Read Access
- System Settings: Advanced - Full Access
- System Settings: LDAP Phone Number Transforms - Full Access
- Dial Plan: Partitions and Search Spaces - Full Access
- Telephony Integrations - Full Access
- System Settings: Cluster, Plugins, LDAP, SAML, Enterprise and Service Parameters - Full Access
- Manage Networking And Server Roles/Activation/Deactivation - Full Access
- Networking: VPIM - Full Access
- Reset User MWI
- Tools: Run Administration Tools

With Unity Connection 12.5(1) and later, the creation of a new role **Custom Technician** is simplified by selecting the **Technician** system role from **Inherit System Role** field.

Step 2 Provide the following additional privileges to the custom role:

- Reset User Passwords
- Tools: Task Management - Full Access

Step 3 Assign the role to the user.

For more information on configuring Custom Roles, see the Configuring Roles section of **System Settings** chapter.