New and Changed Features

Addition of AXL Read Access Role to a User

Cisco Unified Communications Manager Release 11.5(1) onwards, an administrator can assign read-only access role to an AXL (Administrative XML layer) user. The AXL users with a read-only access can execute only read-only application programming interfaces (APIs) and have no access to execute the APIs that are used for system updates.

Following are the new standard access roles that are introduced in Cisco Unified Communications Manager Release 11.5(1):

- Standard AXL API users
- Standard AXL Read Only API Access

Administration Guide Updates

The following topic from the *Administration Guide for Cisco Unified Communications Manager* is updated for the Addition of AXL Read Access Role to a User feature.

Standard Roles and Access Control Groups

The following table includes the new fields for AXL users.

Table 1: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	

Authentication Security Updates for Applications

Starting with Release 11.5(1), administrators can now configure the system to use Form based authentication when connecting to API services for example AXL through a web browser. This update improves application security by offering a more secure authentication method. Previously, **Basic Authentication**, which allowed the browser to cache user credentials, was used for all API services accessible through a browser. To handle

this update, a new enterprise parameter, **Authentication Method for API Browser Access** has been added to allow administrators to configure the authentication method. Administrators can select from the following options:

- Basic - Users signing in to applications must authenticate themselves in the browser's sign in prompt. This is the default option.
- Form Based - Users signing in to an application are redirected to a form based sign in page. Form based authentication is more secure than Basic authentication.

Note This change does not affect web-based applications that already operate using form based authentication.

Call Preservation Duration Management

A new service parameter called **SIP Call Preservation Expires Timer** is added in the **Service Parameter Configuration** window under the Clusterwide Parameters (Device-SIP) service area. This parameter specifies the number of seconds for which a call remains active in the call preservation state. The default value is 0, to enable this feature you have to configure this service parameter within the range of 1- 86400. If you choose to retain the default value, the call is preserved until you hang up or until the device can determine that the media connection has been released. See the online help for more information about the fields and their configuration options.

Following are some of the use cases for this feature:

- Line to line call—If the call manager loses communication to the peer end, the SIP layer starts the preservation timer for the surviving leg and disconnect the leg once it expires.
- Call over SIP trunk—If the SIP Trunk loses communication to the destination, the SIP layer starts the preservation timer for the surviving leg and disconnect the leg once it expires.
- Call with phone-based recording enabled—When the recording leg moves into preservation, the SIP layer starts the preservation timer for the recording legs and disconnect the legs once it expires.
- Call with Gateway recording enabled—When the recording leg moves into preservation, the SIP layer starts the preservation timer for the recording legs and disconnect the legs once it expires.

Note SIP Call Preservation Expires Timer has no effect if Cisco Unified Communications Manager nodes that handle the call processing for the call lose connection to both devices/legs of the call.

Cisco Endpoints

Cisco IP Phones

Phone Firmware Versions

The following table lists the latest Cisco IP Phone firmware versions supported for Cisco Unified Communications Manager 11.5.

Table 2: Phone Firmware Versions

Phone Family	Firmware Release Number
Cisco Unified SIP Phone 3905	9.4(1)SR2
Cisco Unified IP Phones 6901 and 6911	9.3(1)SR2
Cisco Unified IP Phones 6921, 6941, 6945, and 6961	9.4(1)SR2
Cisco IP Phone 7800 Series	11.5(1)
Cisco Unified IP Phone 7900 Series	9.4(2)SR1
Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G	1.4(8)
Cisco IP Phone 8800 Series	11.5(1)
Cisco Unified IP Conference Phone 8831	10.3(1)SR2
Cisco Unified IP Phones 8941 and 8945	9.4(2)SR2
Cisco Unified IP Phones 8961, 9951, and 9971	9.4(2)SR2

Phone Documents in Cisco Unified Communications Manager Self Care Portal

The Cisco Unified Communications Manager Self Care Portal provide links to the IP Phone user guides in PDF format. These user guides are stored in the portal and match the phone firmware version that comes with the Cisco Unified Communications Manager release.

After a Cisco Unified Communications Manager release, subsequent updates to the user guides appear only on the Cisco website. The phone firmware release notes contain the applicable documentation URLs. In the web pages, updated documents display “Updated” beside the document link.

Note The Cisco Unified Communications Manager Device Packages and the Unified Communications Manager Endpoints Locale Installer do not update the English user guides on the Cisco Unified Communications Manager.

Administrators and users should check the Cisco website for updated user guides and download the PDF files. Administrators can also make the files available to the users on their company website.

Tip Administrators may want to bookmark the web pages for the phone models that are deployed in their company and send these URLs to their users.

Deprecated Endpoints

As of Cisco Unified Communications Manager Firmware Release 11.5, the following phones are not supported:

- Cisco IP Phone 12 SP+ and related models
- Cisco IP Phone 30 VIP and related models
- Cisco Unified IP Phone 7902
- Cisco Unified IP Phone 7905
- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone 7910SW
- Cisco Unified IP Phone 7912
- Cisco Unified Wireless IP Phone 7920
- Cisco Unified IP Conference Station 7935

If you use any of these phone models on an older release of Cisco Unified Communications Manager and you upgrade to Release 11.5, the phone will not work after the upgrade completes.

Cisco Unified SIP Phone 3905

The following table lists the features added to the Cisco Unified SIP Phone 3905 for Firmware Release 9.4(1)SR2. For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-sip-phone-3900-series/products-release-notes-list.html.

Feature Name	Firmware Release
Line Text Label	9.4(1)SR2

Cisco Unified IP Phone 6900 Series Features

No new features were introduced for the Cisco Unified IP Phones 6900 Series.

Cisco IP Phone 7800 Series Features

The following table lists the features added to the Cisco IP Phone 7800 Series for Firmware Releases 11.0(1) and 11.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html.

The phone Firmware Release 11.5 is not embedded in the Cisco Unified Communications Manager Release 11.5. The phone firmware needs to be downloaded from Cisco.com and installed separately.

The Cisco Unified Communications Manager Self Care portal contains the *Cisco IP Phone 7800 Series User Guide* for Firmware Release 11.0. For the user guide for Firmware Release 11.5, see: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-user-guide-list.html.

Feature Name	Firmware Release
Barge Enhancements	11.5(1)
Deferred Upgrade	11.5(1)
Disable Recents Softkey	11.5(1)
Enhanced Debugging Options	11.0(1)
External Dial Tone	11.5(1)
FIPS 140-2 Level 1 Support	11.5(1)
Mobile and Remote Access Through Expressway	11.0(1)
Opus Audio Codec	11.5(1)
Problem Report Tool	11.0(1)

Cisco Unified IP Phone 7900 Series Features

The following table lists the features added to the Cisco Unified IP Phone 7900 Series for Firmware Release 9.4(2)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-release-notes-list.html

Feature Name	Firmware Release
Configurable Default Audio Path	9.4(2)SR1

Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G Features

The following table lists the features added to the Cisco Unified Wireless IP Phone 7925G, 7925G-EX, and 7926G for Firmware Release 1.4(8). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-release-notes-list.html.

Feature Name	Firmware Release
Wireless Channel Updates	1.4(8)

Cisco IP Phone 8800 Series Features

The following table lists the features added to the Cisco IP Phone 8800 Series for Firmware Releases 10.3(2), 11.0(1), and 11.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html.

The phone Firmware Release 11.5 is not embedded in the Cisco Unified Communications Manager Release 11.5. The phone firmware needs to be downloaded from Cisco.com and installed separately.

The Cisco Unified Communications Manager Self Care portal contains the *Cisco IP Phone 8800 Series User Guide* for Firmware Release 11.0. For the user guide for Firmware Release 11.5, see: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-user-guide-list.html.

Feature Name	Firmware Release
Application Dial Rules	11.0(1)
Audio Voicemail Access from Visual Voicemail	11.0(1)
Barge Enhancements for Cisco IP Phone 8800 Series	11.0(1)
Cisco IP Phone 8845 and 8865	10.3(2)
Deferred Upgrade	11.5(1)
Enhanced Debugging Options	11.0(1)
Enhanced Do Not Disturb	11.5(1)
Enhanced Line Mode	11.5(1)
External Dial Tone	11.5(1)
FIPS 140-2 Level 1 Support	11.5(1)
Mobile and Remote Access Through Expressway	11.0(1)
Opus Audio Codec	11.5(1)
Problem Report Tool	11.0(1)
User Interface Enhancements	11.0(1)
Wi-Fi Security Enhancements	11.5(1)
Wireless LAN Profile for Cisco IP Phone 8861 and 8865	11.5(1)
X.509 Digital Certificates Support for EAP-TLS, SCEP, PEAP-GTC	11.0(1)

Cisco Unified IP Conference Station 8831 Features

The following table lists the features added to the Cisco Unified IP Conference Station 8831 Series for Firmware Release 10.3(1)SR2. For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html

Feature Name	Firmware Release
Downgrade Disabled	10.3(1)SR2

Feature Name	Firmware Release
HTTPS Support	10.3(1)SR2

Cisco Unified IP Phone 8941 and 8945 Features

No new features were introduced for the Cisco Unified IP Phone 8941 and 8945.

Cisco Unified IP Phone 8961, 9951, and 9971 Features

No new features were introduced for the Cisco Unified IP Phone 8961, 9951, and 9971

Cisco Desktop Collaboration Series

Cisco DX650, DX70, and DX80 Firmware

The following table lists the latest Cisco DX Series firmware versions supported for Cisco Unified Communications Manager 11.5.

Device	Firmware
Cisco DX650	10.2(5)SR2
Cisco DX70	10.2(5)SR2
Cisco DX80	10.2(5)SR2

Cisco DX650, DX70, and DX80 Features

The following table lists the features added to the Cisco DX Series for firmware release 10.2(5). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html.

Feature Name	Firmware Release
Access to Call Statistics	10.2(5)
Alternate Phone Book Server	10.2(5)
Automatic Problem Report Upload	10.2(5)
CA Trust List Update	10.2(5)
Contacts Search	10.2(5)
Default Wallpaper (DX650 Only)	10.2(5)
FIPS Mode	10.2(5)
HDMI Audio	10.2(5)
Password Protection for Settings	10.2(5)

Feature Name	Firmware Release
SIP URI	10.2(5)
Stay in PC Mode	10.2(5)
Support for No Radio Hardware (CP-DX70-W-NR-K9= and CP-DX80-NR-K9=)	10.2(5)
Use the System While an Outgoing Call is Ringing	10.2(5)

Cisco Spark Remote Device

Cisco Spark remote devices (Spark-RDs) are strongly recommended for your hybrid deployment because they do not require a license or MTP insertion, and contain further bug fixes. To use this option, you must use Unified CM 10.5(2)SU5, 11.0(1a)SU3, or 11.5(1)SU3. For unsupported releases, the CTI-RD is used instead, which requires a license and insertion of an MTP. For manual and automatic creation on a supported release, you must use Cisco Spark-RDs for new activations. CTI-RDs created with an earlier release will continue to work until they are migrated to Cisco Spark-RDs.

For more information about Cisco Spark remote devices and supported configuration for Hybrid Call Services, see http://www.cisco.com/go/hybrid-services-call

CLI Privilege Levels

During installation of Cisco Unified Communications Manager, an administrator with level 4 privilege is created at the platform level. This administrator has all privileges to execute all the command line interface (CLI) commands. Through the CLI commands, the administrator with level 4 privilege creates the following administrators:

- Administrator with level 0 privilege—This administrator has read-only access privilege on the interface.
- Administrator with level 1 privilege—This administrator has both read and write access privilege on the interface.

Note Administrators can execute CLI commands based on the privileges defined for each of them.

CLI Reference Guide Updates

The privilege levels of the following CLI commands have been changed in the *CLI Reference Guide for Cisco Unified Communications Solutions*:

- **show accountlocking**
- **show session maxlimit**
- **show csr own name**

- **show csr list type**
- **show password change-at-login userid**
- **show cli session timeout**
- **show process using-most memory**
- **show tech all**
- **show open files all**
- **show open files process**
- **show open files regexp**
- **show open ports all**
- **show open ports regexp**
- **set account name**
- **set account enable**
- **set accountlocking count**
- **set logging enable**
- **set logging disable**
- **set workingdir activelog**
- **set workingdir inactivelog**
- **set password inactivity enable**
- **set password inactivity disable**
- **set password inactivity period**
- **set network max_ip_conntrack**
- **set network cluster publisher hostname**
- **set network cluster publisher ip**
- **delete account**
- **delete dscp**
- **file list activelog**
- **file list inactivelog**
- **file list install**
- **file list salog**
- **file list partBsalog**
- **file list tftp**
- **file view system-management-log**

- **file dump sftpdetails**
- **file dump activelog**
- **file dump inactivelog**
- **file dump tftp**
- **utils ldap config ipaddr**
- **utils ldap config fqdn**
- **utils ldap config status**
- **utils diagnose version**
- **utils diagnose list**
- **utils diagnose test**
- **utils diagnose fix**
- **utils diagnose module**
- **utils firewall ipv6 enable**
- **utils firewall ipv6 disable**
- **utils iothrottle enable**
- **utils iothrottle disable**
- **utils iothrottle status**
- **utils service list**
- **utils system upgrade status**

For details on the above CLI commands, see *CLI Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

CTI Support for End to End Session ID

With release 11.5(1) of Cisco Unified Communications Manager, CTI support has been added for End to End Session ID for calls. The End to End Session ID allows Cisco Unified Communications Manager to track a call end to end with a single unique identifier. Previously, this feature was supported by SIP only. With this CTI update, CTI, and SIP have a common Session ID for calls.

For details on the CTI implementation of the End to End Session ID for Calls, see the "New and Changed Information" chapter of the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager*.

Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints

In previous releases, when a user with a Cisco mobile and remote access client (for example, Cisco Jabber) or endpoint (for example, Cisco DX 80 phone) performed a user search while outside the enterprise firewall, results were based on those user accounts that are saved in the Cisco Unified Communications Manager database. The database contains user accounts which are either configured locally or synchronized from the corporate directory.

With this release, Cisco mobile and remote access clients and endpoints can now search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Cisco Unified Communications Manager database.

Use this feature to achieve the following results:

- Deliver the same user search results regardless of geographic location—Mobile and remote access clients and endpoints can perform user searches by using the corporate directory; even when they are connected outside the enterprise firewall.
- Reduce the number of user accounts that are configured in the Cisco Unified Communications Manager database—Mobile clients can now search users in the corporate directory. In the previous releases, user search results were based on the users that are configured in the database. Now, administrators no longer need to configure or synchronize user accounts to the database solely for user searches. Administrators need to configure only those user accounts that are served by a cluster. Reducing the total number of user accounts in the database shortens software upgrade time frames while improving overall database performance.

To configure this feature, you must enable the **Enable user search to Enterprise Directory Server** option in the **LDAP Search Configuration** window, and configure the LDAP directory server details. For details, see the Configure Enterprise Directory User Search, on page 12 procedure.

System Configuration Updates

The *System Configuration Guide for Cisco Unified Communications Manager* is updated with the following new topics to describe the Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints feature:

- Configure Enterprise Directory Server User Search—Describes how to configure the system for enterprise directory server user searches.
- LDAP Attributes for UDS Search of Directory Server—Shows the UDS-LDAP attribute mapping for user searches to the enterprise directory server. For these types of search requests, UDS acts as a proxy and relays an LDAP request to the enterprise directory server.

Configure Enterprise Directory User Search

Use this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.

Before you begin

- Ensure that the primary, secondary, and tertiary servers, which you choose for LDAP user search, are network reachable to the Unified Communications Manager subscriber nodes.
- From **System** > **LDAP** > **LDAP System**, configure the type of LDAP server from the **LDAP Server Type** drop-down list in the **LDAP System Configuration** window.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Search**.

Step 2 To enable user searches to be performed using an enterprise LDAP directory server, check the **Enable user search to Enterprise Directory Server** check box.

Step 3 Configure the fields in the **LDAP Search Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

LDAP Attributes for UDS Search of Directory Server

The following table lists the LDAP attributes that UDS users search request uses when the **Enable user search to Enterprise Directory Server** option is enabled. For these types of directory requests, UDS acts as a proxy and relays the search request to the corporate directory server.

Note UDS users response tag may be mapped to one of the LDAP attributes. The mapping of the attributes is determined by the option you select from the **LDAP Server Type** drop-down list. Access this drop-down list from **System** > **LDAP** > **LDAP System Configuration** window.

UDS Users Response Tag	LDAP Attribute
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone

UDS Users Response Tag	LDAP Attribute
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
manager	manager
title	title
pager	pager

User Interface Updates for LDAP Search

The **LDAP Search Configuration** window has been added for this release. You can access this window by choosing **System** > **LDAP** > **LDAP Search** from Cisco Unified CM Administration.

Use the **LDAP Search Configuration** window to configure all endpoints and Cisco mobile and remote access clients in the enterprise to perform user searches against an enterprise directory server, even if those endpoints and clients are operating outside the enterprise firewall.

The following topic is added in the *Cisco Unified CM Administration Online Help* to describe the field options that are available for this configuration window.

LDAP Search Settings

Table 3: LDAP Search Settings

Field	Description
LDAP Search for enterprise users through UDS	
Enable user search to Enterprise Directory Server	To enable LDAP search, check this check box. After you check this check box, all the fields of the **LDAP Search Configuration** window become active. To disable the existing LDAP search, uncheck this check box and click **Save**. **Note** If you disable this checkbox, all the fields of the **LDAP Search Configuration** window become non-editable.

Field	Description
LDAP Manager Distinguished Name	Enter a unique name for an entry in the Directory Service.
LDAP Password	Enter a password to access the LDAP server.
Confirm Password	Enter the same password that you entered in the **LDAP Password** field.
LDAP User Search Base 1	Enter the value for the LDAP user search in first search base. For example, a search base value can be **`cn=users,dc=citglab,dc=india,dc=com`**. **Note** This field is mandatory.
LDAP User Search Base 2	(Optional) Enter the value for the LDAP user search in second search base. **Note** You can enter value for this search base if the user information is not found in the first search base.
LDAP User Search Base 3	(Optional) Enter the value for the LDAP user search in third search base. **Note** You can enter value for this search base if the user information is not found in the first and second search bases.
LDAP Custom Filter for Users	From this drop-down list, select one of the filter options as search criteria for users. The options that appear in the drop-down list are defined in the **LDAP Custom Search Filter** window.
Recursive Search on All Search Bases	Check this check box so that the system searches the user information from the second and third search bases also. By default, the system searches for information in first search base only. By checking the **Recursive Search on All Search Bases** checkbox, the system continues to search for the user information in the second and third search bases if the user information is not found in first search base.
UDS Tag to LDAP Attribute Mapping View or select the LDAP attributes for the following UDS tags:	
userName	Displays the attribute name as **sAMAccountName**.
firstName	Displays the attribute name as **givenName**.
middleName	Choose one of the following attributes: • **middleName** • **initials**

Field	Description
lastName	Displays the attribute name as **sn**.
manager	Displays the attribute name as **manager**.
department	Displays one of the following attributes: • **department** • **departmentNumber**
phoneNumber	Choose one of the following attributes: • **telephone** • **ipPhone**
email	Displays the attribute name as **mail**.
title	Displays the attribute name as **title**.
homeNumber	Displays the attribute name as **homephone**.
mobileNumber	Displays the attribute name as **mobile**.
pager	Displays the attribute name as **pager**.
directoryUri	Choose one of the following attributes: • **msRTCSIP-primaryuseraddress** • **mail** • **none**
displayName	Displays the attribute name as **displayName**.
UC Service Directory Information	
Primary Server	From the drop-down list, select one of the existing unified communications (UC) services for LDAP search. After you select a UC service from the drop-down list, the IP address details appear in **Host Name or IP address of Server**, **Port Number**, and **Protocol** columns. In addition, the **View Details** link appears, which you can click to view the UC service configuration details of the UC service that you selected. If the UC service that you want to choose is not listed in the drop-down list, you can create a new UC service. To add a new UC service, click the **Add UC Service** button. The newly added UC service appears in the **Primary Server** drop-down list. **Note** This field is mandatory.

Field	Description
Secondary Server	(Optional) From the drop-down list, select one of the existing UC services for LDAP search. After you select a UC service from the drop-down list, the IP address details appear in **Host Name or IP address of Server**, **Port Number**, and **Protocol** columns. In addition, the **View Details** link appears, which you can click to view the UC service configuration details of the UC service that you selected. If the UC service that you want to choose is not listed in the drop-down list, you can create a new UC service. To add a new UC service, click the **Add UC Service** button. The newly added UC service appears in the **Secondary Server** drop-down list.
Tertiary Server	(Optional) From the drop-down list, select one of the existing UC services for LDAP search. After you select a UC service from the drop-down list, the IP address details appear in **Host Name or IP address of Server**, **Port Number**, and **Protocol** columns. In addition, the **View Details** link appears, which you can click to view the UC service configuration details of the UC service that you selected. If the UC service that you want to choose is not listed in the drop-down list, you can create a new UC service. To add a new UC service, click the **Add UC Service** button. The newly added UC service appears in the **Tertiary Server** drop-down list.
Add UC Service	Click this button to configure primary, secondary, and tertiary directory servers. In the **UC Service Configuration** window, enter the values in the required fields. The values entered in this window appear as UC services in the **Primary Server**, **Secondary Server**, and **Tertiary Server** fields. For more information about the configuration fields of UC services, see the *UC Service Settings* section in the online help.

Note If the primary, secondary, and tertiary servers that you choose for LDAP user search are not network-reachable to the Cisco Unified Communications Manager subscriber nodes, the system shows the failed connection status for each server after you save the values in the **LDAP Search Configuration** window. The status of this configuration is successful after you select a UC service having an IP address of server that is network reachable to the Cisco Unified Communications Manager subscriber nodes.

Directory Server Support

With this release, Cisco Unified Communications Manager can integrate with following LDAP directories. These directories are supported for user account synchronization and authentication.

- Microsoft Active Directory 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Oracle Directory Services Enterprise Edition 11gR1 (11.1.1.7.x or newer)
- Oracle Unified Directory 11gR2 (11.1.2.2.0 or 11.1.2.3.0)
- OpenLDAP 2.4.40 or later

Display Name Configuration Using Unified Communications Self Care Portal

Use Unified Communications Self Care Portal of Cisco Unified Communications Manager Release 11.5 to modify your display name that appears to other users instead of your user ID.

This functionality is handled by **Display Name** field that appears on Unified Communications Self Care Portal. The behavior of this field changes when you log in as the following users:

- Local User—When you log in as local user that is not synchronized with Lightweight Directory Access Protocol (LDAP), you can modify your display name through the **Display Name** field.
- LDAP Synchronized user—When you log in as an LDAP synchronized user, the **Display Name** field becomes non-editable.

View and Modify Display Name

When you log in as a local user who is not synchronized with Lightweight Directory Access Protocol (LDAP), you can view and modify your display name by using the following procedure.

Note When you log in to Unified Communications Self Care Portal, the link to log out of the application shows the display name, if it has been configured earlier. Otherwise, the link to log out shows the User ID.

Procedure

Step 1 From Unified Communications Self Care Portal, click the **General Settings** tab.

Step 2 Click **Display Name**.

The **Display Name** text box appears.

Step 3 In the **Display Name** text box, enter a name that you want other users to see instead of your user ID.

Note
- If you had previously configured a display name, this field is auto-populated with that configured name.
- If you log in as an LDAP synchronized user, the display name is non-editable and so, the **Save** and **Cancel** buttons do not appear for this field.

Step 4 Click **Save**.

Step 5 (Optional) To revert to the previously configured display name, click **Cancel**.

Enable Hunt Log Status with CTI

With release 11.5(1) of Cisco Unified Communications Manager, you can now sign in and sign out of hunt groups through applications. Previously, this functionality was only available from Cisco Unified CM Administration interface. Following are some of the use cases for this feature:

- You can sign-in and sign out of a phone from a hunt group through applications.
- You get a notification whenever there is a change in log on status of the hunt group.

For details on the enabling the hunt log status, see the "New and Changed Information" chapter of the *Cisco Unified JTAPI and TAPI Developers Guide* for Cisco Unified Communications Manager.

EC Ciphers on Tomcat Interface

Elliptic Curve (EC) ciphers on the Tomcat interface are disabled by default. You can enable them using the **HTTPS Ciphers** enterprise parameter on Cisco Unified Communications Manager or on IM and Presence Service. If you change this parameter the Cisco Tomcat service must be restarted on all nodes.

Enhance ILS Certificate Management

With Release 11.5(1), the administrator can enable Transport Layer Security (TLS) authentication together with Password based authorization at the same time to setup a ILS network using common Certificate Authority (CA) signed certificates without exchanging self-signed certificates between clusters. To use Transport Layer Security (TLS) authentication and password authorization between clusters, you must upload the certificate authority root certificates to the Tomcat trust and get the Tomcat certificate signed by the certificate authority root certificate for all clusters. The certificate is then imported back on the same cluster. The clusters can be connected to Intercluster Lookup Service (ILS) network once the Tomact certificates are uploaded and the same password is set on all the clusters. For more information on enabling these options, see the "Configure Intercluster Lookup Service" chapter in the *System Configuration Guide for Cisco Unified Communications Manager* guide at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide.html.

Enhanced Security Updates

For Release 11.5(1), a number of security enhancements have been added to Cisco Unified Communications Manager and IM and Presence Service. These updates improve the security of your system by implementing a stricter set of controls. The updates include:

- Contact Search authentication—When this feature is enabled, users must authenticate in order to use the company directory
- Audit logging—The audit log framework has been updated to include TCP as the transfer protocol for remote audit logs. Previously, only UDP was offered. In addition, a detailed audit logging option is now available to log configuration changes to the database.
- SHA-512 Support—The system now supports SHA-512 for digital signatures.

Contact Search Authentication

With this release, the Contact Search Authentication feature has been added to Cisco Unified Communications Manager. This feature enhances directory security by requiring that users authenticate themselves before they search the company directory. You can configure this feature using the Command Line Interface.

CLI Command Updates

To configure this feature in Cisco Unified Communications Manager, the following new CLI commands are added:

- **utils contactsearchauthentication enable**—Run this command to enable authentication for contact searches that use UDS.
- **utils contactsearchauthentication disable**—Run this command to disable authentication for contact searches that use UDS.
- **utils contactsearchauthentication status**—Run this command to verify that contact search authentication is enabled.

User Interface Updates

The **Secure Contact Search URL** enterprise parameter has been added specifying the directory server URL where secure contact search requests that use UDS are directed. This parameter gets used only if contact search authentication is enabled.

Audit Logging Updates

The audit log framework has been enhanced to include:

- Remote logging with TCP—To guarantee log delivery, TCP is now offered as the transfer protocol for remote audit logging. You can configure this feature using a CLI command.
- Detailed Audit Logging—Detailed audit logging is an optional audit log feature that saves additional configuration information in the audit log. In addition to the information that is stored in standard audit logs, detailed audit logging includes items that were added, updated, and deleted, including the modified

values. Detailed audit logging is disabled by default, but you can enable it in the **Audit Log Configuration** window.

CLI Command Updates

To configure the transfer protocol for remote audit logging, the following CLI commands are now available in Cisco Unified Communications Manager and IM and Presence Service:

- **utils remotesyslog set protocol tcp**—Run this command to set TCP as the transmission protocol for remote audit logs.
- **utils remotesyslog set protocol udp**—Run this command to set UDP as the transmission protocol for remote audit logs.
- **utils remotesyslog show protocol**—Run this command to verify the transmission protocol that is used for remote audit logs.

User Interface Updates

The following user interface updates have been made for audit logging:

- The **Overflow Warning Threshold** text box has been added to the **Audit Log Configuration** window in Cisco Unified Serviceability—The system can alert you when the audit logs are approaching the level where they will be overwritten. Use this field to set the threshold at which the system sends you an alert that the audit logs are approaching the level where they will be overwritten. Possible values are 1-99%. The default value is 80%.
- The **Detailed Audit Logging** check box has been added to the **Audit Log Configuration** window. When the check box is checked, detailed audit logging is enabled.

Audit Log Field Updates

Due to new audit logging requirements, a new **CorrelationID** parameter is added within the audit log itself. If a single log message exceeds the maximum size, the system splits that message into smaller messages and assigns a common **CorrelationID** value to link the messages. If the log message falls within the maximum threshold, a single log message gets written to the audit log with the **CorrelationID** field being empty.

The following two audit log messages form a single large message. In the following example, the common **CorrelationID** value links the messages.

```
09:45:38.800
|LogMessage   UserID : admin  ClientAddress : 10.10.10.10  Severity : 6  EventType :
GeneralConfigurationUpdate  ResourceAccessed: CUCMServiceability  EventStatus : Success
CompulsoryEvent : No  AuditCategory : AdministrativeEvent  ComponentID : Cisco CCM
Servicability  CorrelationID: 123456789 AuditDetails : <first part of the message> App ID:
 Cisco Tomcat Cluster ID
```

```
09:45:38.800
|LogMessage   UserID : admin  ClientAddress : 10.10.10.10  Severity : 6  EventType :
GeneralConfigurationUpdate  ResourceAccessed: CUCMServiceability  EventStatus : Success
CompulsoryEvent : No  AuditCategory : AdministrativeEvent  ComponentID : Cisco CCM
Servicability  CorrelationID: 123456789 AuditDetails : <remainder of the message> App ID:
Cisco Tomcat Cluster ID:  Node ID: sampleNodeHostname
```

New Alarms and Alerts

The **TCPRemoteSyslogDeliveryFailed** alarm and alert have both been added to the Cisco Unified Real-Time Monitoring Tool. When TCP is configured as the remote audit log transfer protocol, and a TCP transmission failure occurs, the alarm gets triggered. In addition, a matching alert gets emailed to the administrator.

You must configure the alert notification in the Cisco Unified Real Time Monitoring Tool.

SHA-512 Digital Signature Support

With this release, you have the option of configuring the system to use SHA-512 for digital signatures. When SHA-512 is configured, legacy phones that do not support SHA-512 will not work.

User Interface Updates

The **TFTP File Signature Algorithm** enterprise parameter has been added speciying the type of digest algorithm to be used while generating the CTL, ITL, and TFTP configuration files. You can select **SHA-1** (the default) or **SHA-512**.

Enhanced Security Configuration Task Flow

Complete the following tasks to configure the security enhancements that are a part of the11.5(1) release on your system.

Procedure

	Command or Action	Purpose
Step 1	Contact Search Authentication Configuration Task Flow, on page 23	Enable Contact Search Authentication in Cisco Unified Communications Manager. When this feature is enabled, phone users must authenticate themselves in order to search the directory for other users.
Step 2	Configure Remote Audit Logging, on page 24	Configure remote audit logging for Cisco Unified Communications Manager and IM and Presence Service. This includes setting up remote syslog servers for all audit logs and alarms. Optionally, you can also enable detailed audit logging if you want audit logs to include details on configuration updates.
Step 3	Update the System to Use SHA-512 Digital Signature Encryption, on page 27	Upgrade your system to use SHA-512 for digital signatures.
Step 4	Reset Phones, on page 29	You must reset your phones in order for the updates to take effect.

Contact Search Authentication Configuration Task Flow

Complete the following tasks to set up Contact Search Authentication in Unified Communications Manager. When this feature is configured, users must authenticate themselves before searching the directory for other users.

Procedure

	Command or Action	Purpose
Step 1	Confirm Phone Support for Contact Search Authentication, on page 23	Confirm that your phones support this feature. Run the **Unified CM Phone Feature List** report in Cisco Unified Reporting to get a list of phone models that support the feature.
Step 2	Enable Contact Search Authentication, on page 23	Configure Unified Communications Manager for Contact Search Authentication.
Step 3	Configure Secure Directory Server for Contact Search, on page 24	Use this procedure to configure Unified Communications Manager with the URL to which phone users are directed when they search the directory for other users.

Confirm Phone Support for Contact Search Authentication

Confirm that the phones in your deployment support contact search authentication. Run a Phone Feature List report to obtain a full list of phone models that support the feature.

Procedure

Step 1 From Cisco Unified Reporting, click **System Reports**.

Step 2 Select **Unified CM Phone Feature**.

Step 3 Click the **Unified CM Phone Feature** report.

Step 4 Leave the **Product** field at the default value.

Step 5 From the **Feature** drop-down, choose **Authenticated Contact Search**.

Step 6 Click **Submit**.

What to do next

Enable Contact Search Authentication, on page 23

Enable Contact Search Authentication

Use this procedure on Unified Communications Manager to configure contact search authentication for phone users.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils contactsearchauthentication status** command to confirm the contact search authentication setting on this node.

Step 3 If you need to configure contact search authentication:

- To enable authentication, run the **utils contactsearchauthentication enable** command.
- To disable authentication, run the **utils contactsearchauthentication disable** command.

Step 4 Repeat this procedure on all Unified Communications Manager cluster nodes.

Note You must reset phones in order for the changes to take effect.

What to do next

Configure Secure Directory Server for Contact Search, on page 24

Configure Secure Directory Server for Contact Search

Use this procedure to configure Unified Communications Manager with the directory server URL to which UDS sends user search requests. The default value is `https://<cucm-fqdn-or-ip>:port/cucm-uds/users`.

Note The default UDS port is 8443. When contact search authentication becomes enabled, the default UDS port switches to 9443. If you then disable contact search authentication, you must change the UDS port back to 8443 manually.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In the **Secure Contact Search URL** text box, enter the URL for secure UDS directory requests.

Note We recommend that for the URL, you choose a node that is not running the Cisco TFTP service. The CiscoTFTP and UDS services may disrupt each other if either service gets restarted.

Step 3 Click **Save**.

Configure Remote Audit Logging

Complete these tasks for Cisco Unified Communications Manager and IM and Presence Service to set up remote audit logging.

Procedure

	Command or Action	Purpose
Step 1	Configure Remote Audit Log, on page 25	Set up your audit log configuration for remote audit logging. If you want to log configuration changes, enable Detailed Audit Logging.,
Step 2	Configure Remote Audit Log Transfer Protocol, on page 26	Optional. Configure the transfer protocol for remote audit logging. The system default in normal operating mode is UDP, but you can also configure TCP.
Step 3	Configure Email Server for Alert Notifications, on page 26	In RTMT, set up the email server for email alerts.
Step 4	Enable Email Alerts, on page 26	Set up the email notification for the **TCPRemoteSyslogDeliveryFailed** alert.

Configure Remote Audit Log

Use this procedure to set up remote audit logging in Cisco Unified Communications Manager and IM and Presence Service.

Before you begin

- You must have already set up your remote syslog server.
- You must also have configured IPSec between each cluster node and the remote syslog server, including connections to any gateways in between. For IPSec configuration, see the *Cisco IOS Security Configuration Guide*.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Audit Log Configuration**.

Step 2 From the **Server** drop-down menu, select any server in the cluster and click **Go**.

Step 3 Check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the **Detailed Audit Logging** check box.

Step 6 Complete the remaining fields in the **Audit Log Configuration** window. For help with the fields and their descriptions, see the online help.

Step 7 Click **Save**.

What to do next

Configure Remote Audit Log Transfer Protocol, on page 26

Configure Remote Audit Log Transfer Protocol

Use this procedure to change the transfer protocol for remote audit logs. The system default is UDP, but you can reconfigure to TCP.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

- To configure TCP, run the **utils remotesyslog set protocol tcp** command.
- To configure UDP, run the **utils remotesyslog set protocol udp** command.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Unified Communications Manager and IM and Presence Service cluster nodes.

What to do next

Configure Email Server for Alert Notifications, on page 26

Configure Email Server for Alert Notifications

Use this procedure to set up your email server for alert notifications.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to do next

Enable Email Alerts, on page 26

Enable Email Alerts

If you have remote audit logging with TCP configured, use this procedure to set up an email alert to notify you of transmission failures.

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 In the **Alert Central** window, select **TCPRemoteSyslogDeliveryFailed**

Step 3 Choose **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 5 In the **Alert Action** popup, **Add** a recipient.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.

Update the System to Use SHA-512 Digital Signature Encryption

Complete the following tasks to upgrade Cisco Unified Communications Manager to use SHA-512 for digital signatures.

Before you begin

To use digital signatures, cluster security must be set to mixed mode.

Procedure

	Command or Action	Purpose
Step 1	Confirm that your phones support SHA-512.	To check phone support for specific phone models, refer to your phone documentation.
Step 2	Upgrade Device Firmware, on page 27	Optional. If you need to upgrade device firmware for any phones, use this procedure to install the new firmware.
Step 3	Plan how to handle non-supported phones.	Optional. Legacy phones that do not support SHA-512 will not work once you upgrade your system. You may need to upgrade to newer phone models or remove the non-supported phones from the system.
Step 4	Enable SHA-512 Usage, on page 28	Enable SHA-512 usage clusterwide for digital signatures.
Step 5	Update CTL File, on page 29	If cluster security is set to mixed mode, regenerate the CTL security file.
Step 6	Restart Services, on page 29	Restart the Cisco CallManager and Cisco TFTP services.

Upgrade Device Firmware

Use this procedure to upgrade device firmware. You may need to do this to upgrade phones to support SHA-512.

Note If you have legacy phones that do not support SHA-512, you may need to upgrade those phones to newer phone models.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Install/Upgrade**.

Step 2 Fill in the applicable values in the Software Location section and click **Next**.

Step 3 In the **Available Software** drop-down list, select the device package file and click **Next**.

Step 4 Verify that the MD5 value is correct, and then click **Next**.

Step 5 In the warning box, verify that you selected the correct firmware, and then click **Install**.

Step 6 Check that you received a success message.

Note Skip to Step 8 if you are rebooting the cluster.

Step 7 Restart the **Cisco TFTP** service on all nodes where the service is running.

Step 8 Reset the affected devices to upgrade the devices to the new load.

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the load file (for specific devices) to the new load.

Step 10 Click **Save**, and then reset the devices.

Step 11 Restart the **Cisco Tomcat** service on all cluster nodes.

Step 12 Restart the **Cisco CallManager** service on the publisher node.

Note If you're running the **Cisco CallManager** service on subscriber nodes only, you can skip this step.

What to do next

Once you are sure that all your phones support SHA-512, Enable SHA-512 Usage, on page 28

Enable SHA-512 Usage

Use this procedure to configure Cisco Unified Communications Manager to require SHA-512 digital signatures from phones.

Note Once you complete this procedure, legacy phones that don't support SHA-512 won't work.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 2 Go to the **Security Parameters** pane.

Step 3 From the **TFTP File Signature Algorithm** drop-down list, choose **SHA-512**.

Step 4 Click **Save**.

Update CTL File

If your cluster security is set to mixed mode, after you have upgraded your system to use SHA-512, use this procedure to regenerate the CTL file.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 On the publisher node, run the **utils ctl update CTLfile** command.

What to do next

Restart Services, on page 29

Restart Services

Use this procedure to restart the Cisco TFTP and Cisco CallManager services. After you have enabled SHA-512 in the cluster, you must restart services.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center – Feature Services**.

Step 2 Choose the following two services, and click **Stop**:

- Cisco CallManager
- Cisco TFTP

Step 3 After both services are stopped, choose them again, and then click **Restart**.

Reset Phones

Use this procedure to reset your phones. You must reset your phones in order for the configuration changes that you made with Contact Search Authentication and in SHA-2 digital signatures to take effect.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phones**.

Step 2 Click **Find**.

Step 3 Click **Select All**.

Step 4 Click **Reset Selected**.

Enhanced TLS Encryption

Cisco Unified Communications Manager and IM and Presence Service Release 11.5(1), inlcudes Elliptic Curve Digital Signature Algorithm (ECDSA) support for Tomcat, SIP Proxy, and XMPP interfaces on TLS version 1.2 connections.

We recommended that when you create a certificate, that you configure both an RSA-based certificate and an ECDSA-based certificate. For example, if you configure a tomcat certificate, you should then also configure a tomcat-ECDSA certificate, and vice-versa.

Note If an IM and Presence Service peer does not support TLS version 1.2, then the connection falls back to TLS version 1.0 and the existing behavior is retained.

As part of this support four new ciphers have been introduced for use on TLS connections supporting the Tomcat, SIP Proxy, and XMPP interfaces. Two of these new ciphers are RSA-based and two are ECDSA-based.

For further information on ECDSA-based cipher support see, ECDSA Support for Common Criteria for Certified Solutions, in the Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.0(1).

The new ciphers which are being introduced are:

- ECDHE ECDSA Ciphers
  - **`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`**
  - **`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`**
- ECDHE RSA Ciphers
  - **`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`**
  - **`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`**

For the RSA-based ciphers, existing security certificates are used. However, the ECDSA-based ciphers require the following additional security certificates:

- `cup-ECDSA`
- `cup-xmpp-ECDSA`
- `cup-xmpp-s2s-ECDSA`
- `tomcat-ECDSA`

If the certificate name ends in `-ECDSA`, then the **certificate/key** type is Elliptic Curve (EC). Otherwise, it is RSA. The Common Name (CN) of an EC certificate has `-EC` appended to the hostname and EC certificates also contain the FQDN or hostname of the server in the SAN field.

Note We recommend that you do not use -EC in the Common Name (CN) field of the RSA-based certificates: Tomcat, XMPP, XMPP-s2s, and CUP. If you do this, the existing EC-based certificate will be overwritten.

For further information on configuring security certificates on IM and Presence Service see, IM and Presence Service Certificate Types, Multi-Server CA Signed Certificate Upload to IM and Presence Service, and Single-Server CA Signed Certificate Upload to IM and Presence Service.

For information on configuring the TLS ciphers see, Configure TLS Cipher Mapping.

Enterprise Group Updates

For this release of Cisco Unified Communications Manager and IM and Presence Service, the following updates were introduced to the Enterprise Groups feature:

- Security Group Support in LDAP Sync
- Enterprise Groups LDAP Configuration Parameter

Security Group Support in LDAP Sync

The enterprise groups feature has been updated to support the synchronization of security groups from an external LDAP directory. Cisco Jabber users can search the directory for security groups, and add the group members to a contact list.

For information on how to configure this feature, refer to the Enterprise Groups chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Enterprise Groups LDAP Configuration Parameter

For IM and Presence Service Release 11.5(1), the **Enterprise Groups LDAP Configuration** parameter has been added to the Inter-cluster peer table. You can use this parameter to check that there are no configuration errors between IM and Presence Service peers. To view the Inter-cluster peer table, click **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter-Clustering**.

If there are conflicts, click the Enterprise Group Conflicts link. Click the **Details** button that appears in order to see a detailed report.

As part of this update, the permitted range for **Maximum Enterprise Group Size to allow Presence Information** enterprise parameter is 1 to 200 users. The default value is 100 users.

Hitless Install of Device Packs

Starting with Cisco Unified Communications Manager Release 11.5(1), a cluster-wide reboot is no longer required to apply a device pack to update an existing firmware or a configuration and to enable new device support. The cached information gets updated at runtime while installing the new device. This update allows you to upgrade device firmware or test new phone models without interrupting services.

Administration Guide Updates

The "Install a Device Pack or Cisco Options Package File" procedure in the *Administration Guide for Cisco Unified Communications Manager* has been updated. The note that specifies a cluster-wide reboot has been removed. For more information on upgrading device firmware, see the 'Manage Device Firmware' chapter of the Administration Guide for Cisco Unified communications Manager.

H.265 Video Codec Support

With the 11.5 release, Cisco Unified Communications Manager supports the H.265 video codec for SIP–SIP video calls. H.265 is supported for MTP/TRP/RSVP Agent pass-through cases. MTP passthrough must be configured in order to use H.265.

For a complete list of supported video codecs for this release, see Video Codec Preference Updates, on page 89.

High Availability for Persistent Chat on IM and Presence Service

High Availability for Persistent Chat Overview

From the current release the persistent chat feature is highly available. In the event of IM and Presence Service node failure or Text Conferencing (TC) service failure, all persistent chat rooms hosted by that service are automatically hosted by the backup node TC service. After failover jabber clients can seamlessly continue to use the persistent chat rooms.

For further information on high availability, see the Configure Presence Redundancy Groups chapter of the System Configuration Guide for Cisco Unified Communications Manager.

For this example there are three users: A, B, and C and three IM and Presence Service nodes: 1A, 2A, and 1B. Node 1A and Node 1B are part of the same Presence Redundancy Group and form a High Availability (HA) pair. The users are assigned to the following nodes:

- User A is on Node 1A
- User B is on Node 2A
- User C is on Node 1B

1. Users A, B, and C are in a chat room hosted on Node 1A.
2. The Text Conferencing (TC) service fails on Node 1A.
3. The IM and Presence Service administrator starts a manual fallback.
4. Node 1B transitions to the HA state **Failed Over with Critical Services not Running**, before transitioning to the HA state **Running in Backup Mode**.
5. In line with the HA Failover Model, User A is signed out automatically and is signed in to the backup Node 1B.
6. Users B and C are not affected but continue to post messages to the chat room hosted on Node 2A.
7. Node 1A transitions to **Taking Back** and Node 1B transitions to **Falling Back**.

8. User A is signed out of Node 1B. Users B and C continue to use the persistent chat room, and once **Fallback** has occurred the room is moved back to Node 1A.
9. Node 1B moves from the HA state **Taking Back** to **Normal** and it unloads its peer node rooms.
10. Node 1A moves from the HA state **Failing Over** to **Normal** and it reloads rooms associated with pubalias.cisco.com.
11. User A signs in again to Node 1A, enters the persistent chat room and continues to read or post messages to the room.

Table 4: Group Chat and Persistent Chat Restrictions

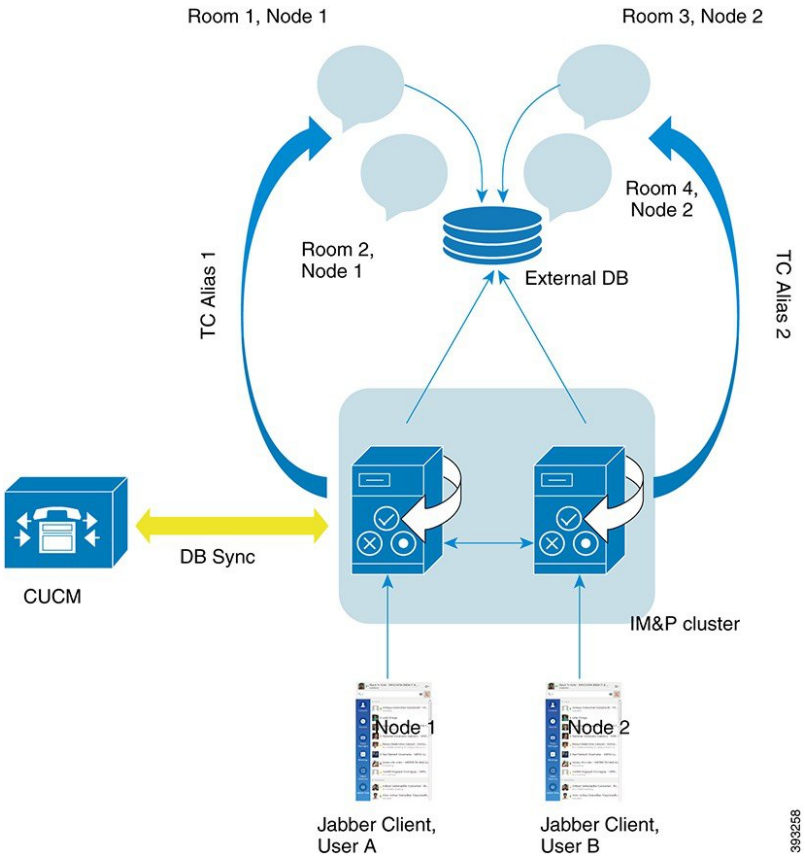
Feature	Restriction
Chat with anonymous rooms	If you are deploying chat via Cisco Jabber (either group chat or persistent chat), make sure that the **Rooms are anonymous by default** and **Room owners can change whether or not rooms are anonymous** options are not selected in the **Group Chat and Persistent Chat Settings** window. If either check box is checked, chat will fail

High Availability for Persistent Chat Flows

The following flows demonstrate the high availability for persistent chat flows for failover and failback.

Note For this enhancement the Text Conferencing (TC) service has been made a critical service. As a result, the TC high availability failover flow remains the same even if the failover has been caused by the failure of another critical service on the node, such as the Cisco XCP Router service.

Figure 1: High Availability for Persistent Chat Structure



High Availability for Persistent Chat Failover Flow

For this example, there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

Subcluster 1	Subcluster 2
• Andy is on Node 1A—Node 1A hosts the chat room • Bob is on Node 1B	• Catherine is on Node 2A • Deborah is on Node 2B

1. All four users are chatting in the same chat room, which is hosted on Node 1A.
2. The Text Conferencing (TC) service fails on Node 1A.
3. After 90 seconds, the Server Recovery Manager (SRM) determines the failure of the TC critical service and starts an automatic failover.
4. Node 1B takes over the users from 1A and transitions to the **Failed Over with Critical Services not Running** state, before transitioning to the HA state **Running in Backup Mode**.
5. In line with the HA Failover Model, Andy is signed out from node 1A automatically and is signed in to the backup Node 1B.

6. The other users are not affected, but continue to post messages to the chat room, which is now hosted on Node 1B.
7. Andy enters the persistent chat room, and continues to read or post messages to the room.

High Availability for Persistent Chat Fallback Flow

For this example there are four users on four IM and Presence Service nodes with two High Availability (HA) pairs or subclusters. The users are assigned as follows:

Subcluster 1	Subcluster 2
• Andy is on Node 1A—Node 1A hosts the chat room • Bob is on Node 1B	• Catherine is on Node 2A • Deborah is on Node 2B

1. All four users are chatting in the same chat room, which is hosted on Node 1A.
2. The Text Conferencing (TC) service fails on Node 1A.
3. Node 1B takes over the users from 1A and transitions to the **Failed Over with Critical Services not Running**, before transitioning to the HA state **Running in Backup Mode**.
4. In line with the HA Failover model, Andy is signed out automatically and is signed in to the backup Node 1B.
5. Bob, Catherine and Deborah are unaffected, but continue to post messages to the chat room, which is now hosted on Node 1B.
6. The IM and Presence Service administrator starts a manual fallback.
7. Node 1A transitions to **Taking Back** and Node 1B transitions to **Falling Back**.
8. Andy is signed out of Node 1B. Bob, Catherine, and Deborah continue to use the persistent chat room, and once **Fallback** has occurred, the room is moved back to Node 1A.
9. Node 1B moves from the HA state **Falling Back** to **Normal** and unloads its peer node rooms.
10. Node 1A moves from the HA state **Taking Back** to **Normal** and it reloads the chat room.
11. Andy enters the persistent chat room, and continues to read or post messages to the room.

Enable and Verify High Availability for Persistent Chat

To enable and verify that high availability for persistent chat is working correctly, carry out the steps in the following procedure:

Procedure

Step 1 Ensure that high availability is enabled in the presence redundancy group:

a) From **Cisco Unified CM Administration**, click **System** > **Presence Redundancy Groups**.

b) On the **Find and List Presence Redundancy Groups** window, click **Find** and choose the Presence Redundancy Group you want to check.

c) On the **Presence Redundancy Group Configuration** window, ensure that the **Enable High Availability** check box is checked.

Step 2 Ensure that persistent chat is enabled on the presence redundancy group:

a) From **Cisco Unified CM IM and Presence Administration UI**, click **Messaging** > **Group Chat and Persistent Chat**.

b) On the **Group Chat and Persistent Chat Settings** window, ensure that the **Enable Persistent Chat** check box is checked.

Step 3 Ensure that both presence redundancy group nodes are assigned to to the same external database. See image.

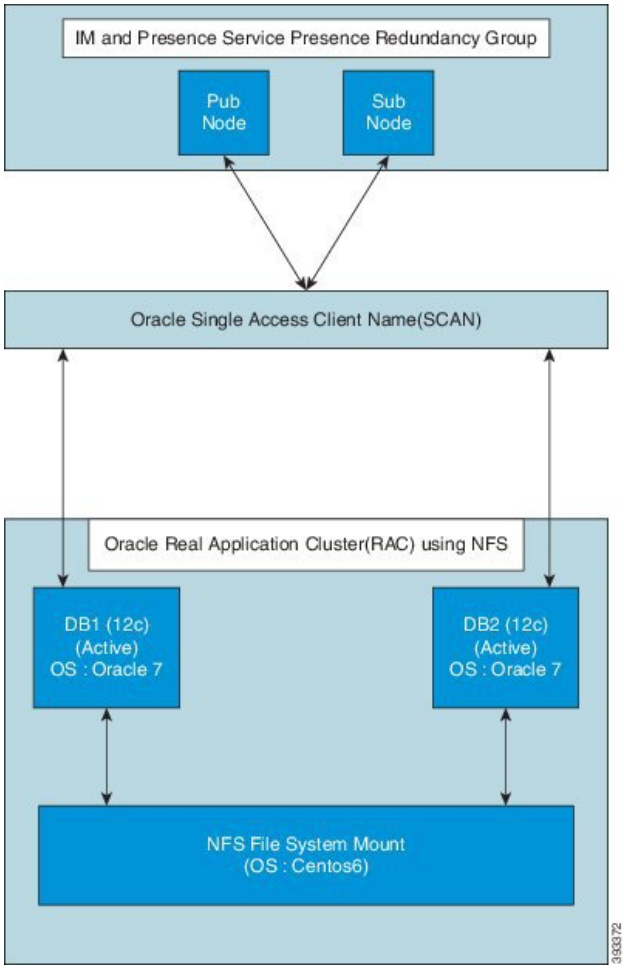
Step 4 To verify that high availability for persistent chat is enabled, check the **System** > **Presence Topology** window. In the Node Status section of the **Node Detail** pane, in the **Service Column**, check that the **Cisco XCP Text Conference Manager** entry has Yes in its **Monitored** column.

If it is a monitored service, this means that it is a critical service and that high availability has been successfully enabled. If it is not, then check that your presence redundancy group has been configured correctly.

External Database for Persistent Chat High Availability

For information on supported versions, refer to the External Database Setup Requirements section of the *Database Setup Guide for IM and Presence Service*.

Figure 2: Oracle High Availability Setup



Merge External Database Tables

The External Database Merge Tool allows persistent chat data which is stored on multiple external database partitions to be merged into a single database.

On earlier versions, each IM and Presence Service node in a presence redundancy group was assigned to a unique external database. From the current release, to enable High Availability for Persistent Chat, nodes in a presence redundancy group must be assigned to only one external database. The External Database Merge Tool allows you to quickly combine these two databases.

The External Database Merge Tool can be used on Oracle and Postgres databases.

Note To use the External Database Merge Tool on an Oracle database, the **Oracle SID** field must have the same value as the **Database Name** field. Otherwise, the merge will fail. For more information, see CSCva08935.

External Database Merge Tool

Use this procedure to merge the two databases in an IM and Presence Service presence redundancy group.

Before you begin

- Ensure that the two source destination databases are assigned correctly to each IM and Presence Service node in the presence redundancy group. This verifies that both of their schemas are valid.
- Back up the tablespace of the destination database.
- Ensure that there is enough space in the destination database for the new merged databases.
- Ensure that the database users, created for the the source and destination databases, have the permissions to run these commands:
  - `CREATE TABLE`
  - `CREATE PUBLIC DATABASE LINK`

  If your database users do not have these permissions, you can use these commands to grant them:
  - `GRANT CREATE TABLE TO <user_name>;`
  - `GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;`

Procedure

Step 1 Sign in to **Cisco Unified CM IM and Presence Administration** on the IM and Presence Service publisher node.

Step 2 Stop the Cisco XCP Text Conference Service on the **System** > **Services** window for each IM and Presence Service node in the presence redundancy group.

Step 3 Click **Messaging** > **External Server Setup** > **External Database Jobs**.

Step 4 Click **Find** if you want to see the list of merge jobs. Choose **Add Merge Job** to add a new job.

Step 5 On the **Merging External Databases** window, enter the following details:

- Choose Oracle or Postgres from the **Database Type** drop-down list.
- Choose the IP address and hostname of the two source databases and the destination database that will contain the merged data.

If you chose Oracle as the **Database Type** enter the tablespace name and database name. If you chose Postgres as the **Database Type** you provide the database name.

Step 6 In the **Feature Tables** pane, the Text Conference(TC) check-box is checked by default. For the current release, the other options are not available.

Step 7 Click **Validate Selected Tables**.

Note If the Cisco XCP Text Conference service has not been stopped you receive an error message. Once the service has been stopped, validation will complete.

Step 8 If there are no errors in the **Validation Details** pane, click **Merge Selected Tables**.

Step 9 When merging has completed successfully, the **Find And List External Database Jobs** window is loaded. Click **Find** to refresh the window and view the new job.

Click the **ID** of the job if you want to view its details.

Step 10 Restart the Cisco XCP Router service.

Step 11 Start the Cisco XCP Text Conference Service on both IM and Presence Service nodes.

Step 12 You must reassign the newly merged external database (destination database) to the presence redundancy group.

In Memory Database Replication

For this release the `utils imdb_replication replication status` command was introduced. This command validates that In Memory Database (IMDB) replication between the node pairs in each subcluster of the deployment has run correctly.

The command also performs writes and reads on IMDB tables in each relevant Datastore using a utility from the calling IM and Presence Service node.

Note If you want to run the Administration CLI Diagnostic Utility using this command, ports 6603, 6604, and 6605 must be open on all firewalls that are configured between IM and Presence Service nodes in the cluster. This setup is not required for normal operation.

Interwork External Multicast MOH to Unicast MOH

Cisco Unified Communications Manager Releases 9.x and earlier ran on either Cisco Media Convergence Server (MCS) or virtual machines. By using MCS, you could use the universal serial bus (USB) cable plug for music on hold (MOH) device, such as a compact disk or Jukebox. The device is known as fixed audio source and is used for playing both unicast and multicast music on hold.

Cisco Unified Communications Manager Releases 10.x and later run on virtual machine only. Hence, USB MOH devices are no longer supported, which limits Cisco Unified Communications Manager to play the locally uploaded wav files as MOH. To overcome this limitation, you can configure a Cisco Unified Survivable Remote Site Telephony (SRST) router as an audio source. This router provides multicast MOH audio for devices that are capable of multicast reception. In this approach, devices act as if Cisco Unified Communications Manager is sending the multicast MOH audio. However, devices that are capable of only the unicast reception cannot hear the MOH audio that an external MOH source (for example, Cisco Unified SRST router) sends. Examples of devices that are capable of unicast reception only can be public switched telephone network (PSTN) phones, destination to session border controllers (SBC), and Session Initiation Protocol (SIP) trunks.

In Cisco Unified Communications Manager Release 11.5, this feature is an enhancement to receive multicast MOH audio from an external audio source and send it as unicast MOH audio. Cisco Unified Communications Manager uses this feature to play multicast MOH audio as unicast MOH for the devices that are capable of unicast MOH reception only. Examples of an external MOH audio source can be a Cisco Unified SRST router or software that can send multicast MOH audio.

An administrator configures the fields for this feature from Cisco Unified CM Administration **Music On Hold Audio Source Configuration** window.

Note

- This feature has no impact on existing functionality of playing multicast MOH audio using an external audio source for the devices that are capable of multicast reception.
- For the unicast media connection, Cisco Unified Communications Manager MOH Server plays the initial announcement and periodic announcement even if you configure the MOH audio source with external multicast source.

Configuration Tips for the Codec-Specific Inbound Audio Stream

Configure an external multicast audio source, such as Cisco Unified SRST router, to MOH server for streaming the required audio feed.

To configure an external multicast audio source, such as a Cisco Unified SRST router, you must configure the **Source IPv4 Multicast Address** and **Source Port Number** fields in the **MOH Audio Source Configuration** window.

- Cisco Unified Communications Manager listens to multicast G.711 mu-law stream on external multicast IP address and port that you configured on the **MOH Audio Source configuration** window. An MOH server can transcode between the G.711 mu-law or a-law or L16 256K wideband MOH codecs. The external multicast RTP stream uses G.711 mu-law codec for MOH as a source for G.711 mu-law or a-law or L16 256K wideband MOH codecs. For G.711 a-law and wideband calls, Cisco Unified Communications Manager MOH server transcodes the inbound G.711 mu-law stream to outbound G.711 a-law or wideband stream before sending it to the device.
- Cisco Unified Communications Manager listens to multicast G.729 stream on external multicast IP and port value added with four that is configured on the **MOH audio source configuration** window. For example, if you configure an MOH audio Source with 239.1.1.1:16384, Cisco Unified Communications Manager listens to G.711 mu-law stream on 239.1.1.1:16384 and G.729 stream on 239.1.1.1:16388 (port value added with four). An MOH server cannot transcode for G.729 codecs. Callers who are using MOH G.729 codec require an external multicast RTP stream using G.729 or G.729a codec.

Audio Source Fields for Music On Hold

Note

- Cisco Unified Communications Manager MOH server receives multicast MOH audio from an external source, which is configured on MOH audio source, and sends it as unicast to the devices that are capable of only unicast reception.
- An administrator can use same MOH audio source that is configured with the external multicast source to play multicast MOH for the devices that are capable of multicast reception. To do so, configure the MOH audio source with same source IPv4 multicast address and port as base multicast IP address and base multicast port number that you configured on MOH server.
- An administrator can also configure MOH server to send multicast MOH audio, which is received from source IPv4 address, from a different multicast IPv4 address. Through the **Music On Hold Audio Configuration** window, an administrator can configure different multicast IPv4 addresses on MOH audio source and base multicast IP address on MOH server.

Field	Description
Music On Hold Audio Source Information	
MOH Audio Stream Number	Use this field to choose the stream number for this MOH audio source. Click the drop-down arrow and choose a value from the list. For existing MOH audio sources, the value appears in the MOH Audio Source title.
MOH Audio Source File	Use this field to choose the file for this MOH audio source. Click the drop-down arrow and choose a value from the list.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name includes up to 50 valid characters, such as letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multi-casting	Check this check box to specify that the selected MOH audio source allows multicasting.
Use MOH WAV file source	Click this option to select the MOH audio source. Use this field if you do not have a multicast source. **Note** • The **MOH Audio Source File** field is enabled when you select this option. • If you click the **Rebroadcast External Multicast Source** field, do not select the **MOH Audio Source File** field.
Rebroadcast External Multicast Source	Select this option to rebroadcast MOH audio that an external multicast source sends. Use this field if you have a multicast source.
Source IPv4 Multicast Address	Enter the IPv4 multicast address for the source. This multicast address and the port destination that an external source (for example, Cisco Unified SRST router) is configured to send the audio RTP stream to. **Note** SRST router does not support IPv6 addresses.
Source Port Number	Enter the port number of the multicast source that an external source uses to send multicast MOH audio.

Field	Description
MOH Audio Source File Status	This pane displays the following information about the source file for the selected MOH audio source: • InputFileName • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • OutputFileList • MOH Audio Translation completion date **Note** OutputFileList includes information on ULAW, ALAW, G.729, and Wideband wav files and status options.
Announcement Settings	
Initial Announcement	Choose an initial announcement from the drop-down list. **Note** To select MoH with no initial announcement, choose the **Not Selected** option. Click the **View Details** link to view the following Initial Announcement information: • Announcement Identifier • Description • Default Announcement **Note** • Played by MOH server only when the Audio Source has “Allow Multi-casting” unchecked and “Initial Announcement Played” set to 'Only for queued calls'. • Played by ANN if “Allow Multi-casting” is checked or if “Initial Announcement Played” is set to 'Always.'
Initial Announcement Played	Choose one of the following to determine when to play the initial announcement: • Play announcement before routing to Hunt Member • Play announcement if call is queued

Field	Description
Periodic Announcement	Choose a periodic announcement from the drop-down list. **Note** To select MoH with no periodic announcement, choose the **Not Selected** option. Click the **View Details** link to view the following Periodic Announcement information: • Announcement Identifier • Description • Default Announcement **Note** • The MOH server always plays the periodic announcement regardless of other settings. • If you use an external multicast source, only the unicast or multicast streams from the MOH server contain the periodic announcement. The external multicast stream from the external broadcasting source does not have the periodic announcement.
Periodic Announcement Interval	Enter a value (in seconds) that specifies the periodic announcement interval. Valid values are 10 to 300. The default value is 30.
Locale Announcement	Locale Announcement depends upon the locale installation package that has been installed. **Note** • Prompts played by MOH will use the setting for Locale Announcement. • Prompts played by ANN will use the User Locale of the calling party.
MoH Audio Sources	

Field	Description
(list of MoH audio sources)	This list box shows the MOH audio source that you add. Select the audio stream number of an MOH audio source to configure that MoH audio source. Audio source ID is an ID that represents an audio source in the Music On Hold server. The audio source can include either a file on a disk or a fixed device from which a source stream Music On Hold server obtains the streaming data. An MOH server can support up to 51 audio source IDs. Each audio source, represented by an audio source ID, can stream as unicast and multicast mode, if needed. **Note** If you select **<None>** , the system default MoH audio source service parameter (**Default Network Hold MoH Audio Source ID**) is used for the MoH audio source.
Upload File	To upload an MOH audio source file that does not appear in the drop-down list, click **Upload File**. In the **Upload File** window, either enter the path of an audio source file or navigate to the file by clicking **Browse**. After you locate the audio source file, click the **Upload File** button to complete the upload. After the audio file gets uploaded, the Upload Result window displays the result of the upload. Click **Close** to close this window. **Note** When you upload a file, the file is uploaded to the Cisco Unified Communications Manager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete. **Note** Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco Unified Communications Manager Administration on each server. MOH audio source files do not automatically propagate to other MOH servers in a cluster.

iX Transport Encryption

Starting with Cisco Unified Communications Manager Release 11.5, encryption is newly added on top of existing iX channel support using DLTS. This feature provides the support to encrypt the iX application media channel in video conferences, so that the privacy of information transmitted in this channel, such as the identities of meeting participants is protected.

To include iX media line encryption for call encryption status consideration, within the **service parameter configuration** window **Clusterwide Parameters (Feature - Call Secure Status Policy)** section, select **All media except BFCP transport must be encrypted** from the **Secure Call Icon Display Policy** drop-down list.

Location Awareness

Location Awareness is a new feature for Release 11.5(1). The feature allows administrators to import network infrastructure devices into the Cisco Unified Communications Manager database. Cisco Unified Communications Manager uses this information to map phones to a specific switch or wireless access point.

Location Awareness provides the following benefits:

- Allows Cisco Unified Communications Manager to determine the physical location of a user who places a call within the enterprise network. Even mobility calls in a roaming situation can be tracked to a wireless access point.
- For emergency calls, Cisco Emergency Responder uses Location Awareness to direct emergency services to the emergency caller's physical location.
- Allows administrators to view and manage network infrastructure devices such as access points and switches from within the Cisco Unified CM Administration interface.

Location Awareness Overview

Location Awareness allows administrators to determine the physical location from which a phone connects to the company network. For wireless networks, you can view the wireless access point infrastructure, and which mobile devices currently associate to those access points. For wired networks, you can view the ethernet switch infrastructure and see which devices are currently connect to those switches. This allows you to determine the building, floor, and cube from which a call was placed.

You can view your network infrastructure from the **Find and List Switches and Access Points** window in Cisco Unified Communications Manager.

This feature updates the Unified Communications Manager database dynamically with the following information:

- Network infrastructure devices such as switches and wireless access points, including IP addresses, hostnames, and BSSID info (where applicable) for each infrastructure device.
- Associated endpoints for each infrastructure device, including:
    - For wireless networks, the list of devices that are currently associated to a wireless access point.

- For wired networks, the list of devices and device types that are currently connected to an ethernet switch.

Cisco Emergency Responder Integration

Location Awareness helps integrated applications such as Cisco Emergency Responder to determine the physical location of a user who places an emergency call. When Location Awareness is enabled, Cisco Emergency Responder learns of a new device to infrastructure association within minutes of a mobile device associating with a new wireless access point, or a desk phone being connected to a new ethernet switch.

When Cisco Emergency Responder first starts up, it queries the Unified Communications Manager database for the current device to network infrastructure associations. Every two minutes following, Cisco Emergency Responder checks for updates to the existing associations. As a result, even if a mobile caller places an emergency call while in a roaming situation, Cisco Emergency Responder can quickly determine the physical location of the caller and send emergency services to the appropriate building, floor, or cube.

Wireless Network Updates

To enable Location Awareness for your wireless infrastructure, you can configure Unified Communications Manager to synchronize with a Cisco Wireless LAN Controller. You can synchronize Unified Communications Manager with up to fifty controllers. During the synchronization process, Unified Communications Manager updates its database with the access point infrastructure that the controller manages. In Cisco Unified CM Administration, you can view the status for your wireless access points, including the list of mobile clients that are associated to each access point.

As mobile clients roam between access points, SIP and SCCP signaling from the endpoint communicates the new device to access point association to Unified Communications Manager, which updates its database. Cisco Emergency Responder also learns of the new association by querying the Unified Communications Manager database every few minutes for new endpoints that have changed their association. As a result, if a mobile client places an emergency call, Cisco Emergency Responder has accurate information on the physical location of the user whom placed the call.

If you have a regular synchronization schedule for your Wireless Access Point controllers, Unified Communications Manager adds and updates access points from the database dynamically following each synchronization.

Using Bulk Administration to insert Access Points

If you are using a third-party wireless access point controller, or if you want to export your access points from Cisco Prime Infrastructure, you can use the Bulk Administration Tool to bulk insert your wireless access point infrastructure from a CSV file into the Unified Communications Manager database. Following the bulk insert, the next location update from the mobile device updates the database with the current access point association.

However, Bulk Administration does not allow you to update your access point infrastructure dynamically as new access points get added to your wireless network. If a mobile call gets placed through an access point that was added after the bulk insert, that access point will not have a record in the database, Unified Communications Manager will not be able to match the BSSID of the new access point, and will mark the infrastructure for the wireless device as UNIDENTIFIED AP.

For detailed information on the Bulk Administration Tool, refer to the "Manage Infrastructure Devices" chapter of the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Wired Network Updates

No configuration is required to enable Location Awareness for your wired infrastructure–the feature is enabled automatically.

As your wired phones register, signaling between the phone and Cisco Unified Communications Manager updates the database dynamically with the switch infrastructure. You can view details on your company's switch infrastructure in Cisco Unified CM Administration, including the list of phones that are connected to a specific switch.

Unlike mobile devices, wired devices do not typically roam from one switch to another. If a phone does get moved, such as could happen if a worker switches desks within a company, the database gets updated with the new switch information after the phone re-registers from the new location. In Cisco Unified Communications Manager, the new switch displays the moved phone as a connected endpoint.

If a switch gets deprecated and removed from the network infrastructure, that switch remains visible within Cisco Unified Communications Manager. To remove the old switch from the infrastructure view, you must deactivate the switch from the **Access Point and Switch Configuration** window.

Location Awareness Prerequisites

This feature allows you to synchronize the Cisco Unified Communications Manager database with multiple Cisco Wireless LAN Controllers. You must also set up your Cisco Wireless LAN Controller hardware and your infrastructure of access points. For details, see your controller documentation.

Location Awareness Configuration Task Flow

Complete the following tasks to set up Location Awareness in Cisco Unified Communications Manager.

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Start Services for Wireless Infrastructure Synchronization, on page 48	In Cisco Unified Serviceability, start services that support the Location Awareness feature.
Step 2	Configure Wireless Access Point Controller, on page 48	Synchronize the database with a Cisco wireless access point controller. The sync imports the wireless infrastructure into the database. **Tip** Set up a sync schedule for automatic updates.
Step 3	Insert Infrastructure Devices, on page 49	Optional. If you want to add your wireless infrastructure from Cisco Prime Infrastructure, or if you are using a third-party wireless LAN controller, use Bulk Administration to update the database from a CSV file. **Note** This method does not allow you to set up automatic updates.

	Command or Action	Purpose
Step 4	Deactivate Infrastructure Device from Tracking, on page 50	Optional. If your synchronization includes access points that you do not want to track (for example, if the synchronization pulls in access points from a lab), you can deactivate the access point and Cisco Unified Communications Manager will not track updates to the access point.

Start Services for Wireless Infrastructure Synchronization

Use this procedure to start services that support synchronization with a Cisco Wireless LAN Controller in support of the Location Awareness feature.

Procedure

Step 1 Log in to Cisco Unified Serviceability and choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, select the publisher node.

Step 3 Make sure that the following services are checked:

- **Cisco CallManager**
- **Cisco AXL Web Service**
- **Cisco Wireless Controller Synchronization Service**

Step 4 Optional. If you want to use Bulk Administration to import your network infrastructure from a CSV file, make sure that **Bulk Provisioning Service** is checked.

Step 5 Click **Save**.

Configure Wireless Access Point Controller

Use this procedure to synchronize the database with a Cisco wireless access point controller. During the sync, Unified Communications Manager updates its database with the wireless access point infrastructure that the controller manages. You can add up to fifty wireless access point controllers.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Wireless Access Point Controllers**.

Step 2 Select the controller that you want to configure:

- Click **Find** and select the controller to edit an existing controller.
- Click **Add New** to add a new controller.

Step 3 In the **Name** field, enter the IP address or hostname for the controller.

Step 4 Enter a **Description** for the controller.

Step 5 Complete the SNMP settings that will be used for SNMP messaging to the controller:

a) From the **SNMP Version** drop-down list, select the SNMP version protocol that the controller uses.
b) Complete the remaining SNMP authentication fields.For more information on the fields and their configuration options, see system Online Help.
c) Click the **Test SNMP Settings** to confirm that you entered valid SNMP settings.

Step 6 If you want to configure scheduled syncs to regularly update the database:
a) Check the **Enable scheduled synchronization to discover Infrastructure Devices** check box.
b) In the **Perform a Re-sync Every** fields, create the synchronization schedule.

Step 7 Click **Save**.

Step 8 (Optional) To update the database immediately, click **Synchronize**.

Optional. If the synchronization pulls in access points that you do not want to track (for example, lab equipment or access points that are not in use) you can remove the access point from tracking.

Insert Infrastructure Devices

Use this procedure to complete a bulk import of your wireless access point infrastructure from a CSV file into the Cisco Unified Communications Manager database. You can use this procedure to import a CSV file that was exported from Cisco Prime Infrastructure or if you want to import access points from a third-party wireless access point controller.

Before you begin

You must have a data file in comma separated value (CSV) format with the following delineated columns:

- AccessPoint or Switch Name
- IPv4 Address
- IPv6 Address
- BSSID—Required for Wireless Access Protocol (WAP) infrastructure devices
- Description—A location identifier, a combination of switch type and location, or another meaningful identifier

Note You can define both an IPv4 and IPv6 address, or you can define an IPv4 or an IPv6 address.

Note For the BSSID value, enter the BSSID mask, ending in 0, that uniquely identifies the access point as opposed to the BSSIDs for the individual channels on the access point.

Procedure

Step 1 Choose **Bulk Administration** > **Infrastructure Device** > **Insert Infrastructure Device**.
The **Insert Infrastructure Device Configuration** window displays.

Step 2 In the **File Name** field, choose the CSV data file that you created for this transaction.

Step 3 In the **Job Information** area, enter the Job description.

The default description is **Insert Infrastructure Device**.

Step 4 Select when you want to run the job:

- Select the **Run Immediately** radio button, if you want to run the job immediately.
- Select the **Run Later** radio button, if you want to schedule the job for later.

Step 5 Click **Submit**.
If you chose to run the job immediately, the job runs.

Step 6 If you chose to run the job later, schedule when the job runs:

a) Choose **Bulk Administration** > **Job Scheduler**.
b) Click **Find** and select the job that you just created.
c) In the **Job Scheduler** window, schedule when you want to run the job.
d) Click **Save**.
At the scheduled time, the job runs.

Deactivate Infrastructure Device from Tracking

If the synchronization includes access points or switches that you do not want to track (for example, if the sync pulls in lab equipment or access points that are not in use), you can deactivate the access point or switch from tracking. Unified Communications Manager will not update the status for the access point or switch.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find** and select the switch or access point that you want to stop tracking.

Step 3 Click **Deactivate Selected**.

Manage Infrastructure with Location Awareness

You can manage network infrastructure devices such as switches and wireless access points as a part of the Location Awareness feature. When Location Awareness is enabled, the Cisco Unified Communications Manager database saves status information for the switches and access points in your network, including the list of endpoints that currently associate to each switch or access point.

The infrastructure device–endpoint mapping helps Cisco Unified Communications Manager and Cisco Emergency Responder to determine the physical location of a caller. For example, if a mobile client places an emergency call while in a roaming situation, Cisco Emergency Responder uses the mapping to determine where to send emergency services.

The Infrastructure information that gets stored in the database helps you to monitor your infrastructure usage. From the Cisco Unified Communications Manager interface you can view network infrastructure devices such as switches and wireless access points. You can also see the list of endpoints that currently associate to

a specific access point or switch. If infrastructure devices are not being used, you can activate or deactivate infrastructure devices from tracking.

Manage Infrastructure Prerequisites

You must configure the Location Awareness feature before you can manage wireless infrastructure within the Cisco Unified Communications Manager interface. For your wired infrastructure, the feature is enabled by default. For configuration details, see the following chapter:

"Location Awareness", System Configuration Guide for Cisco Unified Communications Manager.

You must also install your network infrastructure. For details, see the hardware documentation that comes with your infrastructure devices such as wireless LAN controllers, access points, and switches.

Manage Infrastructure Task Flow

Complete the following tasks to monitor and manage your network infrastructure devices.

Procedure

	Command or Action	Purpose
Step 1	View Status for Infrastructure Device, on page 51	Get the current status of a wireless access point or ethernet switch, including the list of associated endpoints.
Step 2	Deactivate Tracking for Infrastructure Device, on page 52	If you have a switch or access point that is not being used, mark the device inactive. The system will stop updating the status or the list of associated endpoints for the infrastructure device.
Step 3	Activate Tracking for Deactivated Infrastructure Devices, on page 52	Initiate tracking for an inactive infrastructure device. Cisco Unified Communications Manager begins updating the database with the status and the list of associated endpoints for the infrastructure device.

View Status for Infrastructure Device

Use this procedure to get the current status of an infrastructure device such as a wireless access point or an ethernet switch. Within the Cisco Unified Communications Manager interface, you can view the status for an access point or switch and see the current list of associated endpoints.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find**.

Step 3 Click on the switch or access point for which you want the status.

The **Switches and Access Point Configuration** window displays the current status including the list of endpoints that currently associate to that access point or switch.

Deactivate Tracking for Infrastructure Device

Use this procedure to remove tracking for a specific infrastructure device such as a switch or access point. You may want to do this for switches or access points that are not being used.

Note If you remove tracking for an infrastructure device, the device remains in the database, but becomes inactive. Cisco Unified Communications Manager no longer updates the status for the device, including the list of endpoints that associate to the infrastructure device. You can view your inactive switches and access points from the **Related Links** drop-down in the **Switches and Access Points** window.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find** and select the switch or access point that you want to stop tracking.

Step 3 Click **Deactivate Selected**.

Activate Tracking for Deactivated Infrastructure Devices

Use this procedure to initiate tracking for an inactive infrastructure device that has been deactivated. Once the switch or access point becomes active, Cisco Unified Communications Manager begins to dynamically track the status, including the list of endpoints that associate to the switch or access point.

Before you begin

Location Awareness must be configured. For details, see the "Location Awareness" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 From **Related Links**, choose **Inactive Switches and Access Points** and click **Go**.
The **Find and List Inactive Switches and Access Points** window displays infrastructure devices that are not being tracked.

Step 3 Select the switch or access point for which you want to initiate tracking.

Step 4 Click **Reactivate Selected**.

Microsoft SQL External Database Support on IM and Presence Service

For IM and Presence Service Release 11.5(1), external database support for Microsoft SQL has been introduced.

Install and Setup Microsoft SQL Server

Before you begin

- Read the security recommendations for the Microsoft SQL database in the About Security Recommendations section.
- For information on supported versions, see External Database Setup Requirements.
- To install the MS SQL Server, refer to your Microsoft documentation.

Note In compliance with XMPP specifications, the IM and Presence Service node uses UTF8 character encoding. This allows the node to operate using many languages simultaneously and to display special language characters correctly in the client interface. If you want to use Microsoft SQL with the node, you must configure it to support UTF8.

Connect to the MS SQL Server using **Microsoft SQL Server Management Studio**.

Create a New Microsoft SQL Server Database

Use this procedure to create a new Microsoft SQL Server database.

Procedure

Step 1 Enable SQL server and Windows authentication:

a) In the left navigation pane, right-click the name of the Microsoft SQL Server, then click **properties**.

b) Click **Enable SQL Server and Windows Authentication mode**.

Step 2 In the left navigation pane, right-click **Databases** and click **New Database**.

Step 3 Enter an appropriate name in the **Database name** field.

Step 4 Click **OK**. The new name appears in the left navigation pane nested under databases.

Create a new Login and Database User

Use this procedure to create a new login and Microsoft SQL database user.

Procedure

Step 1 In the left navigation pane, right-click **Security** > **Login** and click **New Login**.

Step 2 Enter an appropriate name in the **Login name** field.

Step 3 Check the **SQL Server authentication** check box.

Step 4 Enter a new password in the **Password** field and confirm the password in the **Confirm password** field.

Step 5 Check the **Enforce password policy** check box.

Note Ensure that the **Enforce password expiration policy** is not checked. This password is used by IM and Presence Service to connect to the database and must not expire.

Step 6 Choose the database you want to apply this new user to from the **Default database** drop-down list.

Step 7 In the left navigation pane of the **Login - New** window, click **User Mapping**.

Step 8 Under the **Users mapped to this login** list, check the database to which you want to add this user.

Step 9 Click **User Mapping**, in the **Map** column of the **Users mapped to this pane** pane, check the check box of the database you have already created.

Step 10 In **Server Roles**, ensure that only the **public** role check box is checked.

Step 11 Click **OK**. In **Security** > **Logins**, the new user is created.

Grant Database User Owner Privileges

Use this procedure to grant ownership of a Microsoft SQL database to a database user.

Procedure

Step 1 In the left navigation pane click **Databases**, then click on the name of the database that you have created and click **Security** > **Users**.

Step 2 Right-click on the name of the database user to who you want to add owner privileges, then click **Properties**.

Step 3 In the Database User pane, click **Membership**.

Step 4 In the **Role Members** list, check the **db_owner** check box.

Step 5 Click **OK**.

[Optional] Database User Access Restrictions

Use this procedure if you want to remove the database user as the database owner and apply further optional restrictions to the database user on the Microsoft SQL Server external database.

Caution If during an IM and Presence Service upgrade, there is a database schema upgrade, then the database user must have owner privileges for the database.

Procedure

Step 1 Create a new database role for executing stored procedures:

a) In the left navigation pane click **Databases**, then click the name of the database to which you want to add new database roles.

b) Right-click **Roles**, and click **New Database Role**.

c) In the **Database Role** window, click **General**.
d) Enter an appropriate name in the **Role name** field.
e) Click **Securables**, then click **Search** to open the **Add Objects** window.
f) Choose the **Specific Objects** radio button, and click **OK**.
g) Click **Object Types** to open the **Select Object Types** window.
h) In the **Select Object Types** window, check the **Stored procedures** check box and click **OK**. Stored procedures is then added to the **Select these object types** pane.
i) Click **Browse**.
j) In the **Browse for Objects** window, check the following check boxes:

- [dbo][jabber_store_presence]
- [dbo][ud_register]
- [dbo][ps_get_affiliation]
- [dbo][tc_add_message_clear_old]
- [dbo][wlc_waitlist_update]

k) Click **OK**. The new names appear in the **Enter the object names to select** pane.
l) On the **Select Objects** window, click **OK**.
m) From the **Database Role** window, click the first entry in the list of objects in the **Securables** list.
n) In the **Explicit** list, check the **Grant** check box for the **Execute** permission.
o) Repeat step 13 and 14 for all objects in the **Securables** list.
p) Click **OK**.

A new database role is created in **Security** > **Roles** > **Database Roles**.

Step 2 To update the database user's database role membership:

a) Under **Security** > **Users**, right-click on the database user you have created, then click **Properties**.
b) In the **Database User** window, click **Membership** in the left navigation pane.
c) In the **Role Members pane**, uncheck the **db_owner** check box.
d) Check the check boxes for **db_datareader**, **db_datawriter**, and the database role which you created in step 1.

Step 3 Click **OK**.

Multiple Device Messaging Overview

With Multiple Device Messaging (MDM), you can have your one-to-one instant message (IM) conversations tracked across all devices on which you are currently signed in. If you are using a desktop client and a mobile device, which are both MDM enabled, messages are sent, or carbon copied, to both devices. Read notifications are also synchronized on both devices as you participate in a conversation.

For example, if you start an IM conversation on your desktop computer, you can continue the conversation on your mobile device after moving away from your desk. See Multiple Device Messaging Flow, on page 56.

MDM supports quiet mode, which helps to conserve battery power on your mobile devices. The Jabber client turns quiet mode on automatically when the mobile client is not being used. Quiet mode is turned off when the client becomes active again.

MDM maintains compatibility with the Cisco XCP Message Archiver service and other third-party clients which do not support MDM.

MDM is supported by all Jabber clients from version 11.7 and higher.

The following limitations apply:

- Clients must be signed-in - Signed-out clients do not display sent or received IMs or notifications.
- File transfer is only available on the active device which sent or received the file.
- Group chat is only available on the device which joined the chat room.
- MDM is not supported on clients which connect to IM and Presence Service from the cloud through Cisco Expressway, on Expressway versions prior X8.8.

For further information on how MDM operates, see the following two flows:

Multiple Device Messaging Flow

This flow describes how messages and notifications are handled when a user, Alice, has MDM enabled on her laptop and mobile device.

1. Alice has a Jabber client open on her laptop, and is also using Jabber on her mobile device.
2. Alice receives an instant message (IM) from Bob.

   Her laptop receives a notification and displays a new message indicator. Her mobile device receives a new message with no notification.

Note IMs are always sent to all MDM-enabled clients. Notifications are displayed either on the active Jabber client only or, if no Jabber client is active, notifications are sent to all Jabber clients.

3. Alice chats with Bob for 20 minutes.

   Alice uses her laptop as normal to do this, while on her mobile device new messages are received and are marked as read. No notifications are sent to her mobile device.
4. When Alice receives three chat messages from a third user, Colin, Alice's devices behave as they did in step 2.
5. Alice does not respond, and closes the lid on her laptop. While on the bus home Alice receives another message from Bob.

   In this case, both her laptop and mobile device receive a new message with notifications.
6. Alice opens her mobile device, where she finds the new messages sent from Bob and Colin. These messages have also been sent to her laptop.
7. Alice reads through her messages on her mobile device, and as she does so, messages are marked as read on both her laptop and on her mobile device.

Multiple Device Messaging Quiet Mode Flow

This flow describes the steps Multiple Device Messaging uses to enable quiet mode on a mobile device.

1. Alice is using Jabber on her laptop and also on her mobile device. She reads a message from Bob and sends a response message using Jabber on her laptop.
2. Alice starts using another application on her mobile device. Jabber on her mobile device continues working in the background.
3. Because Jabber on her mobile device is now running in the background, quiet mode is automatically enabled.
4. Bob sends another message to Alice. Because Alice's Jabber on her mobile device in quiet mode, messages are not delivered. Bob's response message to Alice is buffered.
5. Message buffering continues until one of these triggering events occur:
   - An `<iq>` stanza is received.
   - A `<message>` stanza is received when Alice has no other active clients currently operating on any other device.

     Note An active client is the last client that sent either an Available presence status or an instant message in the previous five minutes.

   - The buffering limit is reached.
6. When Alice returns to Jabber on her mobile device, it becomes active again. Bob's message, which had been buffered is delivered, and Alice is able to view it.

Enable Multiple Device Messaging

Multiple Device Messaging is enabled by default. You can use this procedure to disable or enable the feature.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the IM and Presence Service Publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.

Step 4 Choose Enabled or Disabled, from the **Enable Multi-Device Messaging** drop-down list.

Step 5 Click **Save**.

Step 6 Restart the Cisco XCP Router service.

Counters for Multiple Device Messaging

Multiple Device Messaging (MDM) uses the following counters from the Cisco XCP MDM Counters Group:

Table 5: Counter Group: Cisco XCP MDM Counters

Counter Name	Description
MDMSessions	The current number of MDM enabled sessions.
MDMSilentModeSessions	The current number of sessions in silent mode.
MDMQuietModeSessions	The current number of sessions in quiet mode.
MDMBufferFlushes	The total number of MDM buffer flushes.
MDMBufferFlushesLimitReached	The total number of MDM buffer flushes due to reaching the overall buffer size limit.
MDMBufferFlushPacketCount	The number of packets flushed in the last timeslice.
MDMBufferAvgQueuedTime	The average time in seconds before the MDM buffer is flushed.

Serviceability Updates for Location Awareness

A new feature service, **Cisco Wireless Controller Synchronization Service** has been added to Cisco Unified Serviceability under the **Location Based Tracking Services** heading. This service supports the Location Awareness feature, which provides a status of your network's wireless access points and associated mobile devices.

The **Cisco Wireless Controller Synchronization Service** service must be running to synchronize Cisco Unified Communications Manager with a Cisco wireless access point controller. When the service is running, and synchronization is configured, Cisco Unified Communications Manager syncs its database with a Cisco wireless access point controller and saves status information for the wireless access points that the controller manages. You can schedule syncs to occur at regular intervals so that the information stays current.

User Interface Updates for Location Awareness

Two new user interface windows have been added for the Location Awareness feature. Documentation for the user interface is available via the online help system.

- The **Switches and Access Point Configuration** window can be accessed from Cisco Unified CM Administration by choosing **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**. In this configuration window you can view details for specific switches or access points that are imported as a part of the Location Awareness feature.
- The **Cisco Wireless Access Point Controller Configuration** window can be accessed from Cisco Unified CM Administration by choosing **Advanced Features** > **Device Location Tracking Services** > **Cisco Wireless Access Point Controllers**. In this configuration window, you can configure Cisco Unified Communication Manager to synchronize its list of wireless access points with a Cisco wireless LAN controller.

Switches and Access Point Configuration

The **Switches and Access Point Configuration** window allows you to view the network settings for your switches or wireless access points. You can view two main types of information:

- In the **Infrastructure Details** section, view the network settings, such as IP address, hostname, and BSSID (if applicable) for a specific switch or access point.
- In the **Associated Endpoints** section, view the endpoints that are currently connected to a switch, or which are associated with a wireless access point.

Click the **Deactivate** button to remove the switch or access point from the list of devices that tracks. does not track updates for this switch or access point and no endpoint information get tracked for this switch or access point.

Wireless Access Point Controller Configuration

The following table displays the field settings in the Wireless Access Point Controller Configuration window.

Table 6: Wireless Access Point Controller Configuration

Field	Definition
Controller Name	Enter a hostname or IP address for the wireless access point controller.
Description	(Optional) Enter a description for the server. The description can include up to 50 characters in any language. Description cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).
SNMP Version	From the drop-down list, choose the SNMP Version that Cisco Unified Communications Manager uses to communicate with the wireless access point controller. The possible versions are **1**, **2c**, and **3**. **Note** The remaining SNMP configuration settings differs depending on which SNMP version you select.
SNMP Community String	Enter the Community String value that will be used for SNMP requests. This field appears only if you are configuring SNMP version 1 or 2c.
SNMP User Id	Enter the User Id that will be used for SNMP communications. This field appears only for SNMP version 3.
SNMP Authentication Protocol	From the drop-down, select the protocol that will be used to authenticate SNMP messages. The available options are **SHA** or **MD5**. This field appears only for SNMP version 3.
SNMP Authentication Password	In the text box, enter the password that, along with the SNMP User Id, uses to authenticate SNMP messages. This field appears only for SNMP version 3.
SNMP Privacy Protocol	From the drop-down menu, select the protocol that will be used to encrypt SNMP messages. The available options are **AES-128** or **DES**. This field appears only for SNMP version 3.

Field	Definition
SNMP Privacy Password	From the drop-down list, enter the password that will be used to encrypt SNMP messages. This field appears only for SNMP version 3.
Test SNMP Settings	Click this button to confirm that the SNMP settings that you configured enable to communicate with the controller. Refer to the **Status** section for the test results.
Wireless Access Point Controller Synchronization Schedule	
Enable scheduled synchronization to discover Infrastructure Devices	Check this check box to set up a synchronization schedule for to synchronize with the wireless access point controller. You can set synchronization to occur hourly, daily, weekly, or monthly. **Note** Before you can synchronize with a wireless access point controller, the following services must be running: **Cisco Wireless Controller Synchronization Service** and **Cisco AXL Web Service**.
Perform a Re-sync Every	Configure a synchronization schedule. For example, if you enter **2** in the text box and choose **Weekly** from the drop-down menu, synchronization will occur bi-weekly.
Next Re-sync time (YYYY-MM-DD hh:mm)	Displays the next time that a synchronization is scheduled to occur between and this wireless access point controller.

New Alarms for Location Awareness

The following new Real-Time Monitoring Tool alarms have been added for the Location Awareness feature. In Cisco Unified Serviceability, go to **Alarm** > **Definitions** to view alarm definitions.

- SwitchesAndAccessPointReached75PercentCapacity
- SwitchesAndAccessPointReached90PercentCapacity
- SwitchesAndAccessPointReached95PercentCapacity
- CiscoWLCSyncServiceDown
- CiscoWLCSyncStarted
- CiscoWLCSyncStartFailure
- CiscoWLCSyncDBAccessFailure
- CiscoWLCSyncDBInsertFailure
- CiscoWLCSyncProcessStarted
- CiscoWLCSyncProcessFailToStart
- CiscoWLCSyncProcessCompleted
- CiscoWLCSyncProcessStoppedManually
- CiscoWLCSyncNoSchedulesFound
- CiscoWLCSyncInvalidScheduleFound

- CiscoWLCSyncSNMPResponseTimeout
- CiscoWLCSyncSNMPv2CommunityStringError
- CiscoWLCSyncSNMPv3AuthenticationError

LSC Reporting, Bulk Update, and Monitoring Enhancement

As of release 11.5(1), Cisco Unified Communications Manager stores Locally Significant Certificate (LSC) information for endpoints in the database. Administrators can monitor, generate a report, and do a bulk update of the LSC expiry information from within the Cisco Unified Communications Manager interface.

The following updates are made to this feature:

- The administrator can monitor the LSC expiry status in the **Find and List Phones to Update** window of Bulk Administration and **Device** > **Phone**. Administrators can then use the Bulk Administration Tool (BAT) to do a bulk update of phone LSCs.
- Administrators can view and generate a "CAPF Report in File" using the LSC expiry date, LSC Issuer Name, and LSC Issuer Expiry date search filters in Cisco Unified CM Administration.
- The administrators can now monitor the LSC expiry status, and configure the system to send them an email warning that certificates are about to expire. For details on how to set up the email option for certificate monitoring, see the "Manage Certificates" chapter of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
- Administrators can now configure the validity period between 1 to 1825 days from the date of issue in the **Cisco Certificate Authority Proxy Function(Active)**, service parameter. Previously, the validity period was set to 1825 days, with no option to reconfigure.

Note The above functionality is only available if LSCs are generated on Cisco Unified Communication Manager 11.5(1). If LSCs were previously allocated before the upgrade to 11.5(1), you must renew the LSCs to use this functionality for reporting and monitoring of LSCs. There is no other impact on the previously available LSC functionality without the renewal.

User Interface Updates

In Cisco Unified CM Administration, under both the **Device** > **Phone** menu and the **Bulk Administration** > **Phones** menu.

The following filters are added to the **Find and List Users** window: Administrators can use these filters to monitor LSC expiry information from within the Cisco Unified Communications Manager interface:

- LSC Expires—Displays the LSC expiry date on the phone.
- LSC Issued By—Displays the name of the issuer which can either be CAPF or third party.
- LSC Issuer Expires By—Displays the expiry date of the issuer.

In Cisco Unified OS Administration, the following button is added in the **Certificate Monitor Configuration** window:

- **Enable LSC Monitoring**—The check box is checked by default. Check the check box to receive an email on the LSC expiry status. You can either enable or disable the check box to monitor the LSC expiry status.

Administration Guide Updates

The following topic in the Administration Guide is updated for the "LSC Reporting, Bulk Update, and Monitoring Enhancement" feature. Use this procedure to locate phones that have LSCs that are about to expire.

View LSC Status and Generate a CAPF Report for a Phone

Use this procedure to monitor Locally Significant Certificate (LSC) expiry information from within the Cisco Unified Communications Manager interface. The following search filters display the LSC information:

- LSC Expires—Displays the LSC expiry date on the phone.
- LSC Issued By—Displays the name of the issuer which can either be CAPF or third party.
- LSC Issuer Expires By—Displays the expiry date of the issuer.

Note The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to "NA" when there is no LSC issued on a new device.

The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to " Unknown" when the LSC is issued to a device before the upgrade to Cisco Unified Communications Manager 11.5(1).

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the first **Find Phone where** drop-down list, choose one of the following criteria:

- LSC Expires
- LSC Issued By
- LSC Issuer Expires By

From the second **Find Phone where** drop-down list, choose one of the following criteria:

- is before
- is exactly
- is after
- begins with
- contains
- ends with
- is exactly

- is empty
- is not empty

Step 3 Click **Find**.
A list of discovered phones displays.

Step 4 From the **Related Links** drop-down list, choose the **CAPF Report in File** and click **Go**.
The report gets downloaded.

Bulk Administration Updates

The Update Phones Using Query topic is updated for the“ LSC Reporting, Bulk Update, and Monitoring Enhancement ” feature. Use this procedure to locate phones that have LSCs that are about to expire.

After you determine which phones to update, you can use existing procedures in the “Phone Updates ” chapter of the *Bulk Administration Guide for Cisco Unified Communications Manager* to update LSCs for your phones.

Native Queuing Announcement Enhancement

Starting with Cisco Unified Communications Manager Release 11.5(1), you can configure the inbound calls to change to the connected call state before playing the queuing announcement, while the call is extended to a hunt member in the queuing-enabled hunt pilot.

The new **Connect Inbound Call before Playing Queuing Announcement** check box is added to the following trunk and gateway configuration windows:

- H.225 Trunk (Gatekeeper Controlled)
- Inter-Cluster Trunk (Non- Gatekeeper Controlled)
- Inter Cluster Trunk(Gatekeeper Controlled)
- H.323 Gateway(Gateway Type)
- SIP Profile (Trunk Specific Configuration)
- MGCP (E1 PRI, T1 PRI, T1 CAS, and BRI)

The following restriction is added as part of the Native Queuing Announcement Enhancement feature. For more information, see the Call Queuing section in the *System Configuration Guide for Cisco Unified Communications Manager*:

- In a H323 to SIP interworking scenario, you may not hear initial announcement, MoH, periodic announcement or observe call failure in a native call queuing flow due to interworking delays. In such a scenario, only use SIP protocol.

Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS

This release of Cisco Unified Communications Manager introduces the opt-in configuration option to control Cisco Jabber on iOS SSO login behavior with an Identity provider (IdP). Use this option to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.

You can configure the opt-in control through the **SSO Login Behavior for iOS** enterprise parameter in Cisco Unified Communications Manager.

Note Before you change the default value of this parameter, see the Cisco Jabber feature support and documentation at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html to ensure Cisco Jabber on iOS support for SSO login behavior and certificate-based authentication.

To enable this feature, see the Configure SSO Login Behavior for Cisco Jabber on iOS, on page 64 procedure.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 To configure the opt-in control, in the SSO Configuration section, choose the **Use Native Browser** option for the **SSO Login Behavior for iOS** parameter:

Note The **SSO Login Behavior for iOS** parameter includes the following options:

- **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. This option is enabled by default.
- **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform certificate-based authentication with an Identity Provider (IdP) in the MDM deployment.

  Note We don't recommend to configure this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser.

Step 3 Click **Save**.

PIN Synchronization

The PIN Synchronization feature is a new feature for Release 11.5(1) that allows you to sign in to Extension Mobility, Conference Now, Mobile Connect, and their Cisco Unity Connection Voicemail using the same end user PIN credential.

To enable the feature:

- The **End User PIN Synchronization** check box in **Cisco Unified Communications Manager's Application Server Configuration** window must be checked for the connection to the Cisco Unity Connection server.

Enable PIN Synchronization

Use this procedure to enable PIN synchronization so that the users can sign in to Extension Mobility, Conference Now, Mobile Connect, and the Cisco Unity Connection Voicemail using the same PIN.

Note The pin synchronization between Cisco Unity Connection and Cisco Unified Communications Manager is successful, only when Cisco Unified Communications Manager publisher database server is running and completes its database replication. Following error message is displayed when the pin synchronization fails on Cisco Unity Connection: `Failed to update PIN on CUCM. Reason: Error getting the pin.`

Note If the pin synchronization is enabled and the end user changes the pin, then pin is updated in Cisco Unified Communications Manager. This happens only when the pin update is successful in at least one of the configured Unity Connection Application server(s).

Before you begin

This procedure assumes that you already have your application server connection to Cisco Unity Connection setup. If not, for more information on how to add a new application server, see the "Integrate Applications, Configure Application Servers "chapter in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

To, enable PIN Synchronization feature you need to first upload a valid certificate for the Cisco Unity Server connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager tomcat-trust. For more information on how to upload the certificate, see the "Manage Security Certificates" chapter in the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

The user ID in the Cisco Unity Connection Server must match the user ID in Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Application Servers**.

Step 2 Select the application server that you set up for Cisco Unity Connection.

Step 3 Check the **Enable End User PIN Synchronization** check box.

Step 4 Click **Save**.

Self Care User Guide Updates

The following topic from the *Self Care User Guide* is updated for the Common PIN feature.

Set Phone Services PIN

The Phone Services PIN is used for enabling different services such as extension mobility, conference calls, mobile connect, and for self-provisioning of new phones. The PIN that you enter must meet the credential policy defined in Unified Communications Manager. For example, if the credential policy specifies a minimum PIN length of 7 digits, the PIN that you enter should be at least 7 digits long and cannot exceed 128 digits. For more information, contact your system administrator.

Procedure

Step 1 From Unified Communications Self Care Portal, choose **General Settings** and click **Phone Services PIN**.

Step 2 In the **New Phone PIN** text box, enter the PIN and re-enter the PIN in the **Confirm New Phone PIN** text box to confirm.

Step 3 Click **Save**.

Note If your network administrator has enabled PIN Synchronization, you can use the same PIN to log into Extension Mobility, Conference Now, Mobile Connect, and your Cisco Unity Connection voicemail box.

Bulk Administration Updates

The following topics from the *Bulk Administration Guide* are updated for the Common PIN feature.

Reset User Password and PIN Using Query

You can use a query to locate users and reset passwords and PINs to a default value.

Procedure

Step 1 Choose **Bulk Administration** > **Users** > **Reset Password/PIN** > **Query**.

The Find and List Users window displays.

Step 2 To locate the users that you want to reset, define the query filter.

Step 3 From the first **Find User where** drop-down list, choose one of the following criteria:

- User ID
- First Name
- Middle Name
- Last Name
- Manager
- Department

From the second **Find User where** drop-down list box, choose one of the following criteria:

- begins with
- contains
- is exactly
- ends with
- is empty
- is not empty

Step 4 Specify the appropriate search text, if applicable, and click **Find**.

Note To choose users from more than one department, enter multiple departments separated with a comma in this field. For example, to choose users from departments 12 and 14, enter 12, 14 in the third box instead of performing two operations.

Tip To find all users that are registered in the database, click **Find** without entering any search text.

Step 5 To further define your query, you can choose AND or OR to add multiple filters and repeat Step 3, on page 67 and Step 4, on page 67.

Step 6 Click **Find**.

A list of discovered users displays by

- User ID
- First Name
- Middle Name
- Last Name
- Manager
- Department Name
- LDAP Sync Status

Step 7 Click **Next**.

Step 8 Enter the values that you want to update for all the records that you defined in your query.

- Password—Enter the default password that users use when they log on to the Cisco Unified IP Phone Self Care Portal window.
- Confirm Password—Reenter the password.
- PIN—Enter the default PIN for the extension mobility feature that users should use when they log in to a Cisco Unified IP Phone.
- Confirm PIN—Reenter the PIN.

Note If you want your end users to be able to use this PIN to access their Cisco Unity Connection Voicemail, the **Enable End User PIN Synchronization** check box in the **Application Server Configuration** window must be checked for the connection to the Cisco Unity Connection server. The PIN in Cisco Unified Communications Manager gets updated only if the PIN in Cisco Unity Connection gets updated successfully.

Step 9 In the **Job Information** area, enter the Job description.

Step 10 Choose a method to change passwords or PINs. Do one of the following:

a) Click **Run Immediately** to change passwords or PINs immediately.
b) Click **Run Later** to change them at a later time.

Step 11 To create a job for resetting passwords or PINs, click **Submit**.

Step 12 To schedule and activate this job, use the Job Scheduler option in the Bulk Administration main menu.

To schedule and/or activate this job, use the Job Scheduler option in the **Bulk Administration** main menu.

Tip The log file displays the number of users that were updated and the number of records that failed, including an error code.

Reset User Password and PIN Using Custom File

To locate users and to reset passwords and PINs to default values, you can create a custom file of user IDs by using a text editor.

Before you begin

1. Create a text file that lists each user ID on a separate line for which you want to reset password or PIN.
2. Upload the custom file into Cisco Unified Communications Manager first node.

Note Do not use the insert or export transaction files that are created with bat.xlt for the reset transaction. Instead, you must create a custom file with details of the user records that need to be reset. Use only this file for the reset transaction. In this custom reset file, you do not need a header, and you can enter values for user ID.

Procedure

Step 1 Choose **Bulk Administration** > **Users** > **Reset Password/PIN** > **Custom File**.

The **Find and List Users** window displays.

Step 2 In the **Find and List Users** window, choose the field that you used in the custom file from the following options:

- User ID
- First Name
- Middle Name
- Last Name
- Department

Step 3 In the **In Custom File** drop-down list box, choose the filename for the custom file.

Step 4 Click **Next**.

Step 5 In the **Reset Password/PIN for Users** window, enter the values that you want to update for all the records.

- Password—Enter the default password that users use when they log on to the **Cisco Unified IP Phone Self Care Portal** window.
- Confirm Password—Reenter the password.
- PIN—Enter the default PIN for the extension mobility feature that users should use when they log in to a Cisco Unified IP Phone.
- Confirm PIN—Reenter the PIN.

Note If you want your end users to be able to use this PIN to access their Cisco Unity Connection Voicemail, the **Enable End User PIN Synchronization** check box in the **Application Server Configuration** window must be checked for the connection to the Cisco Unity Connection server. The PIN in Cisco Unified Communications Manager gets updated only if the PIN in Cisco Unity Connection gets updated successfully.

Step 6 In the **Job Information area**, enter the Job description.

Step 7 Choose a method to change passwords or PINs. Do one of the following:

a) Click **Run Immediately** to change passwords or PINs immediately.
b) Click **Run Later** to change them at a later time.

Step 8 To create a job for resetting passwords or PINs, click **Submit**.

Step 9 To schedule and activate this job, use the Job Scheduler option in the Bulk Administration main menu.

To schedule and/or activate this job, use the Job Scheduler option in the **Bulk Administration** main menu.

Tip The log file displays the number of users that were updated and the number of records that failed, including an error code.

User Interface Field Description Updates

The following Application Server field descriptions have been updated.

Application Server Settings

The following table describes all the available settings in the Application Server window. Because each server requires different settings, not all the settings in the table below apply to each server.

Table 7: Application Server Settings

Field	Description
Application Server Information	
Application Server Type	Choose the application server for the type of application to which you want to connect.
Name	Enter a name to identify the application server that you are configuring.

Field	Description
IP Address	Enter the IP address of the server that you are configuring. **Note** Ensure the IP address is numeric with a number pattern between 1-255 (for example, 10.255.172.57). **Tip** For Cisco Unity and Cisco Unity Connection, you must use the same Administrator user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. This user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration.
URL	Enter a URL for the application server.
End User URL	Enter a URL for the end users that are associated with this application server.
Available Application Users	This pane displays the application users that are available for association with this application server. To associate an application user with this application server, select the application user (for example, CCMAdministrator, CCMSysUser, UnityConnection, and so on) and click the Down arrow below this pane.
Selected Application Users	This pane displays the application users that are associated with the application server. To remove an application user, select the application user and click the Up arrow above this pane. To add an application user, select an application user in the Available Application Users pane and click the Down arrow. **Note** If you want to configure Cisco Unified Communications Manager to integrate with **Cisco Unity Connection**, you must select a single application user for the connection. You cannot select more than one.

Field	Description
Enable End User Pin Synchronization	Check this checkbox to enable the End User PIN synchronization between Cisco Unified Communications Manager and Cisco Unity Connection. End users can use the same PIN to log in to Extension Mobility and to access their Voicemail. To enable this checkbox, you need to upload a valid certificate for the Cisco Unity Server connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager **tomcat-trust**.For more information on how to upload the certificate, see the "Manage Security Certificates" chapter in the *Administration Guide for Cisco Unified Communications Manager*.

Remote Call Control using Upgraded Skype for Business Clients

With this release, the Remote Call Control feature of IM and Presence Service supports Skype for Business 2015 clients that were upgraded from Lync 2013 clients, and which are registered to a Lync 2013 server. With this feature, users can use the upgraded Skype for Business client to control their Cisco Unified IP Phone.

Note The Skype for Business 2015 client must have been upgraded from a Lync 2013 client, and must be registered to a Lync 2013 server.

For details on how to configure Remote Call Control, refer to *Remote Call Control with Microsoft Lync for IM and Presence Service on Cisco Unified Communications Manager* at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html

RSA Security Certificate Support for Increased Key Lengths

On Cisco Unified Communications Manager and IM and Presence Service, new key length sizes of 3072 bits and 4096 bits have been introduced for self-signed certificates and CSR certificates of certificate/key type RSA.

SAML-Based Single Sign-On (SSO) for RTMT

With this release, the Windows version of Real-Time Monitoring Tool (RTMT) now supports Security Assertion Markup Language (SAML) SSO. If SAML SSO is enabled, you can launch the RTMT application or other supported applications, such as Cisco Unified Communications Manager, after a single sign-in with

an Identity Provider (IdP). You no longer need to sign in to each application separately or maintain separate credentials for each application.

In SAML SSO mode, RTMT first adds the certificate of Cisco Unified Communications Manager. Then, when RTMT attempts to access the IdP server, a certificate acceptance window pops up. Click the **View** button on this window to view the IdP server details. After you accept the certificate, RTMT displays the IdP sign-in page.

Note The certificate acceptance window pops up only when you sign in for the first time and does not appear for the subsequent sign-ins.

With this feature:

- RTMT automatically discovers if Cisco Unified Communications Manager is in SSO mode or non-SSO mode.
- SSO-enabled RTMT client also works with Cisco Unified Communications Manager that is not SSO-enabled to ensure compatibility.

For details on how to deploy SAML SSO in your environment, see *SAML SSO Deployment Guide for Cisco Unified Communications Applications* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note

- In RTMT, access to **Analysis Manager** tab and **System** > **Trace & Log Central** option is not supported in the SAML SSO mode. Hence, an authentication window pops up requesting you to enter your credentials when you try to access these options. Enter your credentials, which are saved in Cisco Unified Communications Manager instead of your IdP credentials, in the authentication window.

  Note To access both **Analysis Manager** tab and **System** > **Trace & Log Central** option, enter your credentials in one of the authentication windows only.

- SAML SSO is supported for Windows version of RTMT. However, the Linux version of RTMT does not support SAML SSO.

You can configure SAML SSO for RTMT through the **Use SSO for RTMT** enterprise parameter in Cisco Unified Communications Manager. To enable this feature, see the Configure SSO for RTMT, on page 72 procedure.

Configure SSO for RTMT

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 To configure SSO for RTMT, in the SSO Configuration section, choose **True** for the **Use SSO for RTMT** parameter:

Note The **Use SSO for RTMT** parameter includes the following options:

- **True**—If you choose this option, RTMT displays the SAML SSO-based IdP sign-in window.

  Note When you perform a fresh install, the default value of the **Use SSO for RTMT** parameter appears as **True**.

- **False**—If you choose this option, RTMT displays the basic authentication sign-in window.

  Note When you perform an upgrade from a Cisco Unified Communications Manager version where **Use SSO for RTMT** parameter does not exist, the default value of this parameter in the newer version appears as **False**.

Step 3 Click **Save**.

Single Sign on Single Service Provider Agreement

Single sign-on allows you to access multiple Cisco collaboration applications after logging on to one of them. In the releases earlier than Unified Communications Manager Release 11.5, when administrators enabled SSO, each cluster node generated its own service provider metadata (SP metadata) file with a URL and a certificate. Each generated file had to be uploaded separately on Identity Provider (IDP) server. As the IDP server considered each IDP and SAML exchange as a separate agreement, the number of agreements that were created was equivalent to the number of nodes in the cluster.

To improve the user experience and to reduce the total cost of the solution for large deployments, this release is enhanced. Now, it supports a single SAML agreement for a Unified Communications Manager cluster (Unified Communications Manager and Instant Messaging and Presence (IM and Presence)).

Note A cluster-wide single SSO agreement deployment requires a multiserver CA signed tomcat certificate. So, before using this feature, ensure that you install this Tomcat certificate on the Unified Communications Manager cluster. The SAML SSO configuration wizard checks for Tomcat Multi-Server certificate during the SSO enablement.

SAML SSO Deployment Guide Updates

The following topic from the *SAML SSO Deployment Guide for Cisco Unified Communications Applications* is updated for the Single Sign On Single Service Provider Agreement feature.

Configure Cisco Unified Communications Manager for SAML SSO Activation

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 2 From the **SAML Single Sign-On Configuration** window, click one of the following options for the **SSO Mode** field:

- **Per Node**—To upload the server metadata of a single node.
- **Cluster wide**—To upload the server metadata of multiple nodes of a cluster.

Step 3 Click **Enable SSO**.

Step 4 Click **Continue**.
The **SAML Single Sign-On Configuration** window displays the status and tomcat multiserver certificate details.

Step 5 If you selected the **Cluster wide** SSO mode, perform the following steps:

a) Click **Test for Multi-Server Tomcat Certificate**.

b) If the Tomcat certificate is valid, the **Next** button is enabled. Click **Next**.

Note If the Tomcat certificate is invalid, the **Next** button is disabled and you cannot proceed further.

The message and the procedure to download the IdP metadata trust file appears.

Step 6 Click **Export Metadata**.
Depending on the SSO mode you choose, the `single agreement.xml` file for the node or the cluster is downloaded.

What to do next

If you have not yet created a Circle of Trust, you can do it now or shift tasks while configuring the IdP. Create Circle of Trust before you configure the IdP for SAML SSO.

Online Help Updates

The following topic from the *Cisco Unified CM Administration Online Help* is updated for the Single Sign On Single Service Provider Agreement feature.

SAML Single Sign-On Fields

Setting	Description
SSO Mode	Select one of the following options: **Cluster wide** Click this option to select the single agreement per cluster mode **Per node** Click this option to select per node SSO mode.

Setting	Description
Server Name	Specifies the names of all the servers in the cluster.
SSO Status	Displays one of the following statuses: **SAML** Indicates that the SAML SSO is enabled on the server. **Disabled** Indicates that SAML SSO is disabled on the server. Cisco Unified Communications Manager: **Cisco Unified OS Administration** > **Security** > **Single Sign On** IM and Presence Service: **Cisco Unified IM and Presence OS Administration** > **Security** > **Single Sign On**
Re-import Metadata	Click the **Re-import Metadata** icon to import IdP metadata file from the publisher to the subscribers. **Note** This option is displayed as N/A (Not Applicable) for the publisher node.
Last Metadata Import	Specifies the time when the IdP metadata was last imported on the server. This field displays “Never” if you are running the SAML SSO setup for the first time.
Export Metadata	Based on the SSO mode you choose, clicking **Export Metadata** downloads the metadata file. If you choose the **Cluster wide** SSO mode, it downloads cluster metadata file. If you choose the **Per Node** SSO mode, it downloads the server metadata file. **Note** Ensure that the Export Metadata mode is in synchronization with the SSO mode that you choose to enable SSO. A SAML metadata file must be generated for the specified server, and downloaded using the browser. You must then import this metadata file to the IdP server. **Important** If you change the hostname or domain of a node, ensure that you download the metadata from that node and upload the file to the IdP server again. The **Export All Metadata** button is enabled by default, regardless of whether the SAML SSO state set to active.
Last Metadata Export	Specifies the time when the SAML metadata file of the specified server was last exported. This field displays “Never” if you are running the SAML SSO setup for the first time.

Setting	Description
SSO Test	Displays the test results of the SAML configuration with the IdP. The test ensures that the specified server trusts the IdP, and that the IdP trusts the specified server. The trust relationship between the server and the IdP depends on the success of exporting and importing of SAML metadata files. Displays one of the following values: **Never** Indicates that a test has not been performed on this server. **Passed** Indicates that a test has been successfully run on this server, and that the server and the IdP trust one another. **Failed** Indicates that a test was attempted on the specified server, but that either the server does not trust the IdP, or the IdP does not trust the server, or some other network or IdP issue prevented the test from passing.
Run Test	Click **Run Test** to run the SSO test. You must run this test before enabling SAML SSO. The SAML SSO setup cannot be completed until this test is successful. To run this test, there must be at least one LDAP synchronized user with administrator rights. You must also know the password for that user ID. **Note** You cannot run this test until the IdP metadata file is imported to the server, and the server metadata file is exported to the IdP server.
Enable SAML SSO	Click **Enable SAML SSO** to start the SAML SSO configuration.
Update IdP Metadata File	Click **Update IdP Metadata File** to update IdP metadata on all the servers in the cluster.
Export All Metadata	If you select the SSO mode as **Per Node** and click **Export All Metadata**, the SAML metadata files from each server are exported. These files are converted to a compressed file (.zip) for easy download. You must extract the file and then import each file to the IdP. If you select the SSO mode as **Cluster wide** and click **Export All Metadata**, a single SAML metadata file for a cluster is exported.
Fix All Disabled Servers	Click **Fix All Disabled Servers** to enable SAML SSO on the servers on which it is disabled.
View IdP Trust Metadata File	Click **View IdP Trust Metadata File** to download a copy of the IdP metadata file.

Self-Provisioning and Auto-Registration Support in Secure Clusters

Prior to this release, Auto-Registration and Self-Provisioning features were supported only while the cluster security was set to non-secure mode. With this release, you can use these features regardless whether the cluster security mode is non-secure or mixed-mode. This enhancement allows administrator to secure the UCM cluster without losing the advantage of Auto-Registration and Self-Provisioning.

Administrators can use Auto-Registration to provision a large number of new phones as they are plugged into the network. During the auto-registration process, Cisco Unified Communications Manager assigns a directory number from a pre-configured range. Cisco Unified Communications Manager also assigns default configurations to both the phone and directory number by applying Universal Device and Line Templates.

Self-Provisioning allows phone users to provision their own phone without the aid of an administrator. When a new phone is plugged into the network, it auto-registers to the system with a capability to dial to an IVR where the phone user can authenticate. If authentication succeeds, the phone is automatically configured in the system for that User.

For detailed information on configuring Auto-Registration and Self-provisioning, go to the 'Configure Auto-Registration' and 'Configure Self-Provisioning' chapters of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

User Interface Updates for Self-Provisioning and Auto-Registration

To support the updates for this feature, the following user interface updates were made in the *Cisco Unified Communications Manager Administration Online Help Guide*:

- GUI field behavior in the **Cisco Unified CM** and**Cisco Unified CM Group Configuration** window is now exactly the same whether you are in mixed mode or non-secure mode.
- The **Certificate Authority Proxy Function (CAPF) Settings** section of the Universal Device Template Configuration window now contains a **Certificate Operation** drop-down menu. You have to choose "Install/Upgrade" in the Certificate Operation field if you want phone to install LSC during Auto-Registration or Self-Provisioning.

Note For the phones auto-registering to **Cisco Unified CM** with this field set to "Install/Upgrade", the CAPF Operation Expiry time is controlled by an existing enterprise parameter "CAPF Operation Expires in (days)".

Command Line Interface Update

The following updates have been made to utils ctl in the *Command Line Interface Guide*:

set-cluster mixed-mode	Updates the CTL file and sets the cluster to mixed mode. You will see the following Warning Message if you change the cluster settings from nonsecure mode to mixed mode and Auto-Registration is already enabled on the cluster: "This operation will set the cluster to Mixed mode. Auto-Registration is enabled on at least one CM node. Do you want to continue? (Y/N)"

Support for v.150 Codec

Cisco Unified Communications Manager Release 11.5(1) onwards, configure IOS on SIP trunk, MLPP, and MTP gateway port setting for V.150 to make a secure call connection. For more information to configure IOS on Cisco Unified Communication Manager, see the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

V.150 Overview

The V.150 Minimum Essential Requirements feature allows you to make secure calls in a modem over IP network. The feature uses a dialup modem for large installed bases of modems and telephony devices operating on a traditional public switched telephone network (PSTN). The V.150.1 recommendation specifically defines how to relay data from modems and telephony devices on a PSTN into and out of an IP network through a modem. The V.150.1 is an ITU-T recommendation for using a modem over IP networks that support dialup modem calls.

The Cisco V.150.1 Minimum Essential Requirements feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements (MER) for V.150.1 recommendation. The SCIP-216 recommendation has simplified the existing V.150.1 requirements.

Cisco V.150.1 MER feature supports the following interfaces:

- Media Gateway Control Protocol(MGCP) T1(PRI and CAS) and E1(PRI) trunks
- Session Initiation Protocol (SIP) trunks
- Skinny Client Control Protocol (SCCP) for analog gateway endpoints
- Secure Communication Interoperability Protocol-End Instruments (SCIP-EI)

Prerequisites for Cisco V.150.1 MER

Your system should already be set up with basic call control functionality. For instructions on how to set up the call control system, refer to the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_0_1/sysConfig/CUCM_BK_C733E983_00_cucm-system-configuration-guide.html.

For Unified Communications Manager, you must have one of the following releases installed:

- The minimum version is Release 10.5(2) SU3
- For 11.0, the minimum version will be 11.0(1) SU2 available in Spring 2016
- All releases from 11.5(1) on support this feature

- You must have Cisco IOS Release 15.6(2)T or later.

V.150 is not supported with Media Termination Point (MTP). We recommend that you remove MTP from devices, trunks, and gateways that are handling V.150 calls.

Configure V.150 Task Flow

Complete these tasks to add V.150 support in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	To Configure Media Resource Group Task Flow, on page 79, perform the following subtasks: • Configure Media Resource Group for Non-V.150 Endpoints, on page 80 • Configure a Media Resource Group List for Non-V.150 Endpoints, on page 80 • Configure Media Resource Group for V.150 Endpoints, on page 81 • Configure a Media Resource Group List for V.150 Endpoints, on page 81	Add Media Resource Group and Media Resource Group List for V.150 and non V.150 devices.
Step 2	Configure the Gateway for Cisco V.150 (MER), on page 82	Add V.150 functionality to a gateway.
Step 3	Configure V.150 MGCP Gateway Port Interface, on page 82	If you want to use V.150 support across an MGCP gateway, add V.150 support to the port interface.
Step 4	Configure V.150 SCCP Gateway Port Interface, on page 83	If you want to use V.150 support across an SCCP gateway, add V.150 support to the port interface.
Step 5	Configure V.150 Support for Phone, on page 83	Add V.150 support to the phones that will be placing V.150 calls.
Step 6	To Configure SIP Trunk Task Flow, on page 84, perform one or both of the following subtasks: • Set the Clusterwide V.150 Filter, on page 85 • Add V.150 Filter to SIP Trunk Security Profile, on page 86	Add V.150 support to the SIP trunk that will be used for V.150 calls.

Configure Media Resource Group Task Flow

Complete these tasks to configure two sets of media resource groups: one media resource group with MTP resources for non-V.150 calls, and a media resource group without MTP resources for V.150 calls.

Procedure

	Command or Action	Purpose
Step 1	Configure Media Resource Group for Non-V.150 Endpoints, on page 80	You can configure the Media Resource Group with MTP that you want to be used by non-V.150 endpoints.
Step 2	Configure a Media Resource Group List for Non-V.150 Endpoints, on page 80	Configure a Media Resource Group list that includes your MTP Media Resources for non-V.150 endpoints.
Step 3	Configure Media Resource Group for V.150 Endpoints, on page 81	Configure Media Resource Group without MTP resources for secure V.150 calls.
Step 4	Configure a Media Resource Group List for V.150 Endpoints, on page 81	Configure a Media Resource Group list for non-V.150 endpoints without MTP after adding the required resources in the Media Resource Group.

Configure Media Resource Group for Non-V.150 Endpoints

Use this procedure to add a new media resource group that includes MTP resources for non-V.150 endpoints.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the media resource group name as “Do not use with V.150 devices”.

Step 4 From the **Available Media Resources** field, choose only MTP devices and click the down-arrow key. The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

What to do next

Configure a Media Resource Group List for Non-V.150 Endpoints, on page 80

Configure a Media Resource Group List for Non-V.150 Endpoints

Use this procedure to add new media resource group list with MTP resources for non-V.150 end points.

Before you begin

Configure Media Resource Group for Non-V.150 Endpoints, on page 80

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name for the media resource group list as " Non- V.150".

Step 4 From the **Available Media Resources** field, choose the V.150 MER resource group named "Do not use with V.150 Devices" and click the down-arrow key.
The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure Media Resource Group for V.150 Endpoints

Use this procedure to add new media resource group without MTP resources for V.150 devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the media resource group name as "For use with V.150 devices".

Step 4 From the **Available Media Resources** field, choose multiple devices except the MTP resources and click the down-arrow key.
The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

What to do next

Configure a Media Resource Group List for V.150 Endpoints, on page 81

Configure a Media Resource Group List for V.150 Endpoints

Use this procedure to add a media resource group list without MTP resources for V.150 devices.

Before you begin

Configure Media Resource Group for V.150 Endpoints, on page 81

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name for the media resource group list as "V.150".

Step 4 From the **Available Media Resources** field, choose the V.150 MER resource group named " For V.150 Devices" and click the down-arrow key.
The selected media resource groups appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure the Gateway for Cisco V.150 (MER)

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 Choose the gateway from the **Gateway Type** drop-down list.

Step 4 Click **Next**.

Step 5 From the **Protocol** drop-down list, choose a protocol.

Step 6 Depending on which Protocol you chose for the gateway, perform:

- For MGCP, in the **Domain Name** field, enter the domain name that is configured on the gateway.
- For SCCP, in the **MAC Address (Last 10 Characters)** field, enter the gateway MAC address.

Step 7 From the **Unified Communications Manager Group** drop-down list, choose **Default**.

Step 8 In the **Configured Slots, VICs and Endpoints** area, perform the following steps:

a) From each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.

b) From each **Subunit** drop-down list, select the VIC that is installed on the gateway.

c) Click **Save**.
The port icons appear. Each port icon corresponds to an available port interface on the gateway. You can configure any port interface by clicking the corresponding port icon.

Step 9 Complete the remaining fields in the **Gateway Configuration** window. See the online help for more information about the fields and their configuration options.

Step 10 Click **Save**.

What to do next

Perform one of the following:

- Configure V.150 MGCP Gateway Port Interface, on page 82 or
- Configure V.150 SCCP Gateway Port Interface, on page 83

Configure V.150 MGCP Gateway Port Interface

Before you begin

Configure the Gateway for Cisco V.150 (MER), on page 82

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Enter the appropriate search criteria to modify the settings for an existing gateway and click **Find**.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the module and subunit on which you want to configure a port for V.150 MER and click the corresponding port icon.

Step 4 From the **Device Protocol** drop-down list, choose **Digital Access T1** or **Digital Access PRI** and click **Next**.

Note The **Device Protocol** drop-down list is displayed only if T1 port is selected in the **Configured Slots, VICs, and Endpoints** area.

The **Gateway Configuration** window now displays the port interface configuration.

Step 5 Select the **Media Resource Group List** named "V.150".

Step 6 Check the **V150 (subset)** check box.

Step 7 Configure the remaining fields, if applicable. See the online help for more information about the fields and their configuration options.

Step 8 Click **Save**.

Step 9 Optional. If you want to configure additional port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**. You can select a different port interface

Configure V.150 SCCP Gateway Port Interface

Before you begin

Configure the Gateway for Cisco V.150 (MER), on page 82

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Enter the appropriate search criteria to modify the settings for an existing SCCP gateway and click **Find**.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the module and subunit on which you want to configure a port for V.150 MER and click the corresponding port icon.

Step 4 Select the **Media Resource Group List** named "V.150".

Step 5 In the **Product Specific Configuration Layout** area, if the **Latent Capability Registration Setting** drop-down list appears, select **Modem Relay** or **Modem Relay and Passthrough**.

Step 6 Configure the remaining fields, if applicable. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Configure V.150 Support for Phone

Use this procedure to add V.150 support for a phone. The following phone types support V.150:

- Cisco 7962—Third party SCCP end point registered as Cisco 7962
- Cisco 7961G-GE—Third party SCCP end point registered as Cisco 7961G-GE
- Third Party AS-SIP Endpoints

Before you begin

Ensure to create an End User with the User ID same as the intended phone number.

Ensure to configure the **Digest Credentials** field in the **End User Configuration** window for Third Party AS-SIP SIP endpoints.

For more information on how to configure a new End User, see the "Provision End Users Manually" chapter in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform either of the following steps:

- To configure V.150 on an existing phone, click **Find** and select the phone.
- To configure a new phone for V.150, click **Add New**.

Step 3 From the **Phone Type** drop-down list, select one of the phone types that supports V.150, and click **Next**.

Step 4 For third party SCCP endpoints registered as Cisco 7962. From the **Device Protocol** drop-down list, select **SCCP** and click **Next**.

Step 5 From the **Media Resource Group List** drop-down menu, select **V.150**.

Step 6 Third Party AS-SIP SIP endpoints only. Configure the following fields:

- From the **Digest User** drop-down select the end user for this phone. The end user will be used for digest authentication.
- Leave the **Media Termination Point Required** check box unchecked.
- Check the **Early Offer support for voice and video calls** check box.

Step 7 Click **Save**.
A message window to **Apply Config** is displayed.

Step 8 Click **Apply Config**.

Step 9 Click **OK**.

Configure SIP Trunk Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile for V.150, on page 85	Configure a SIP Profile with SIP Best Effort Early Offer support for the SIP trunk.
Step 2	Set the Clusterwide V.150 Filter, on page 85	Optional. Configure a clusterwide default setting for SIP V.150 SDP Offer Filtering.

	Command or Action	Purpose
Step 3	Add V.150 Filter to SIP Trunk Security Profile, on page 86	Configure a V.150 Filter within a SIP Trunk Security Profile that you can assign to specific SIP trunks.
Step 4	Configure SIP Trunk for V.150, on page 86	Configure V.150 support for the SIP trunks that will handle V.150 calls.

Configure SIP Profile for V.150

Use this procedure to configure a SIP Profile with SIP Best Effort Early Offer support for the SIP trunk.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile** .

Step 2 Perform either of the following steps:

- To create a new profile, click **Add New**.
- To select an existing profile, click **Find** and select a SIP profile.

Step 3 In the **Name** field, enter the SIP name for V.150.

Step 4 In the **Description** field, enter the description for V.150.

Step 5 From the **Early Offer Support for Voice and video class** drop-down list, choose **Select Best Effort (no MTP inserted)**.

Step 6 Enter any other configuration settings that you want. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Set the Clusterwide V.150 Filter

Use this procedure to configure a clusterwide default setting for SIP V.150 SDP Offer filtering.

Note If you configure a **SIP V.150 SDP Offer Filtering** value within a SIP Trunk Security Profile that is different than the clusterwide service parameter setting, the security profile setting overrides the cluster-wide service parameter setting for the trunks that use that security profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose an active server.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 In the **Clusterwide Parameters (Device- SIP)** section, configure a value for the **SIP V.150 SDP Offer Filtering** service parameter.

Step 5 Choose **SIP V.150 SDP Offer Filtering** from the drop-down list.

Step 6 Specify the desired filtering action.

Step 7 Click **Save**.

What to do next

Add V.150 Filter to SIP Trunk Security Profile, on page 86

Add V.150 Filter to SIP Trunk Security Profile

Use this procedure to assign a V.150 Filter within a SIP Trunk Security Profile.

Note If you configure a **SIP V.150 SDP Offer Filtering** value within a SIP Trunk Security Profile that is different than the clusterwide service parameter, the security profile setting overrides the cluster-wide service parameter setting for the trunks that use that security profile.

Before you begin

Set the Clusterwide V.150 Filter, on page 85

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following tasks:

- To modify the settings for an existing SIP Trunk Security Profile, enter search criteria, click Find, and choose an existing profile from the list.
- To add a new SIP Trunk Security Profile, click **Add New**.

Step 3 Configure a value for the **SIP V.150 Outbound SDP Offer Filtering** drop-down list.

Note The default setting is to use the value of the **SIP V.150 Outbound SDP Offer Filtering** cluster-wide service parameter.

Step 4 Configure any remaining fields in the **SIP Trunk Security Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

What to do next

Configure SIP Trunk for V.150, on page 86

Configure SIP Trunk for V.150

Use this procedure to configure settings for a SIP trunk.

Before you begin

Add V.150 Filter to SIP Trunk Security Profile, on page 86

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Perform either of the following steps:

- To create a new profile, click **Add New**.
- To select an existing trunk, click **Find** and select a SIP trunk.

Step 3 For new trunks, do the following:

- From the **Trunk Type** drop-down list, choose **SIP Trunk**.
- From the **Protocol Type** drop-down list, choose **SIP**.
- From the **Trunk Service Type** drop-down list, choose **None(Default)**.
- Click **Next**.

Step 4 Enter the SIP trunk name in the **Name** field.

Step 5 Enter the SIP trunk description in the **Description** field.

Step 6 From the **Media Resource Group List** drop-down list, choose the Media resource group list named "V.150".

Step 7 Configure the destination address for the SIP trunk:

a) In the **Destination Address** text box, enter an IPv4 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.

b) If the destination is a DNS SRV record, check the **Destination Address is an SRV** check box.

c) To add additional destinations, click the **(+)** button. You can add up to 16 destinations for a SIP trunk.

Step 8 From the **SIP Trunk Security Profile** drop-down list, assign the SIP trunk security profile that you configured for this trunk.

Step 9 From the **SIP Profile** drop-down list, assign the SIP profile that you set up with the Best Effort Early Offer setting.

Step 10 Leave the **Media Termination Point Required** check box unchecked.

Step 11 Configure any additional fields in the **Trunk Configuration** window. See the online help for more information about the fields and their configuration options.

Step 12 Click **Save**.

Upgrade for Unified Communications Manager

Uneven Level Protection Forward Error Correction (ULPFEC) Support for Audio Stream

Previous releases of Cisco Unified Communications Manager supported forward error correction (FEC) for video stream only. With this release, Cisco Unified Communications Manager also supports X-ULPFECUC for audio stream. With this support, the endpoints and infrastructure applications are more resilient to media packet loss and provide higher audio quality to the users. This feature enhances the audio quality during conferences that traverse the public Internet, business-to-business (B2B), mobile and remote access (MRA) solutions.

User Authorization for SIP Registrations via Expressway

With Release 11.5(1), Cisco Unified Communications Manager supports user authorization for mobile and remote access users who register to Cisco Unified Communications Manager via Expressway. The SIP interface now includes a userid field in the Contact header of incoming SIP REGISTER requests that are received from Expressway.

After Expressway receives a SIP REGISTER message from a mobile or remote access phone, Expressway adds the userid field to the Contact header and relays the REGISTER message to Cisco Unified Communications Manager. Cisco Unified Communications Manager authorizes the user for the incoming registration request against the following values in the database, and either accepts or rejects the registration request:

- The **Owner User ID** for the phone as configured in the **Phone Configuration** window.
- The **User ID** of any user who is associated as device controller in **End User Configuration**.

You can enable or disable user authorization with the **SIP Registration Authorization Enabled** service parameter, which is new for this release. By default, user authorization is enabled.

Authorization Scenarios

Cisco Unified Communications Manager accepts registration for SIP REGISTER messages that arrive from Expressway in these scenarios:

- No userid field appears in the incoming SIP REGISTER message.
- The userid in the SIP REGISTER message matches ***either*** of the following: the phone owner as assigned in the **Phone Configuration** window's **Owner User ID** field, or the **User ID** of any user who has that device listed as a controlled device in the **End User Configuration** window.

Note Registration succeeds so long as there is a single match, even if the phone's **Owner User ID** setting is different from the **User ID** for the user who controls the device.

If multiple users are associated to the phone as device controllers, the registration request needs only a single match with a device controller or phone owner for registration to succeed.

- No user is configured as either owning or controlling the device in Cisco Unified Communications Manager. For example, the device does not have an **Owner User ID** assigned in the **Phone Configuration** window, and no user has that device listed as a controlled device in **End User Configuration**.

Cisco Unified Communications Manager rejects the registration request with a 401 UNAUTHORIZED response in these scenarios:

- The userid field in the REGISTER message does not match either the **Owner User ID** configured in the **Phone Configuration** window or the **User ID** of an end user configured as device controller.
- The SIP REGISTER message contains more than one userid in the Contact header.
- The userid="" in the SIP REGISTER message , but in Cisco Unified Communications Manager the device entry has an **Owner User ID** configured, or a user is associated to the phone as device controller.

New Alarm for SIP Registration Rejections

A new Severity 4 warning alarm, **AuthorizationError**, has been added to the Real-Time Monitoring Tool. The alarm covers instances where Cisco Unified Communications Manager rejects a registration attempt that is received from Expressway due to user authorization failure. The new alarm has been added as reason code **35** of the **EndpointTransientConnection** set of alarms.

Table 8: Authorization Alarm in the EndpointTransientConnection Set of Alarms

Alarm Value	Definition
35	**Authorization Error**—(SIP devices only) Device registration failed due to one of the following reasons: 1) userID in the Contact header of SIP REGISTER message does not match with any of the configured values in Unified CM (Owner User ID in phone configuration page and User ID associated with the device in End User page); or 2) there are multiple userIDs present in the Contact header of the SIP REGISTER message. Either situation is a security risk. Check the Unified CM configuration to see whether an authorized user is trying to register this particular device.

For the full list of EndpointTransientConnection alarms, see the *Managed Service Guide for Cisco Unified Communications Manager*.

Video Codec Preference Updates

In Cisco Unified Communications Manager Release 11.5(1), the negotiation order preference for video codecs has been updated. The following table displays the order preference for this release and previous releases:

Table 9: Updates to Video Codec Preference for 11.5(1)

New Preferred Order for 11.5(1)	Preferred Order for Previous Releases
• H.265 • H.264 AVC • H.264 SVC • H.264 UC • H.263 1998 • H.263 Orig • H.261	• H.265 • H.264 SVC • H.264 UC • H.264 AVC • H.263 1998 • H.263 Orig • H.261

As a part of this update, the H.264 AVC codec is now second in the order of preference (previously, it was fourth) and will be negotiated ahead of H.264 SVC or H.264 UC due to offering better interoperability than those codecs.

Note For previous releases, the H.265 video codec was supported on a 'Best Effort' basis only. For this release, H.265 is fully supported.

Web Browser Support

This feature offers web browser support for seamless access to each Unified Communications Manager Release 11.5 web application. For example, Cisco Unified CM Administration, Cisco Unified Serviceability, and Cisco Unified Operating System Administration. This release onwards, the following web browsers are supported:

- Firefox with Windows 10 (64 bit)—Latest browser version only
- Chrome with Windows 10 (64 bit)—Latest browser version only
- Internet Explorer 11 with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 8.1 (64 bit)
- Internet Explorer 11 with Windows 7 (64 bit)
- Edge browser with Windows 10 (32 bit/64 bit)
- Safari with MacOS (10.x)—Latest browser version only

Windows 10 Support for Cisco Unified Communications Manager Clients

This release of Cisco Unified Communications Manager supports the installation, operation, and uninstallation on both Microsoft Windows 7 and Microsoft Windows 10 (32–bit and 64–bit) operating systems. It supports these operations for the following Unified CM clients:

- Cisco Unified Communications Manager Security Token Advisory (CTL Client)
- Cisco Unified Real-Time Monitoring Tool (Unified RTMT) for Windows
- Cisco Unified CM Assistant Console (IPMA)

Manager Assistant User Guide and Online Help Updates

The following topic from the *Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager* is added for the Windows 10 support for Cisco Unified Communications Manager clients feature.

Supported Platforms

IP Manager Assistant (IPMA) plugin has been tested with and supports the following operating systems:

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10

Note IPMA plugin is not supported for Linux operating system.

RTMT Guide Updates

The following topics from the *Cisco Unified Real-Time Monitoring Tool Administration Guide* are updated for the Windows 10 support for Cisco Unified Communications Manager clients feature.

In addition, the instances of Windows 98 and XP have been removed as they are no longer supported.

Install and Set Up Cisco Unified Real-Time Monitoring Tool

This chapter provides information about installing and setting up the Cisco Unified Real-Time Monitoring Tool, which works for resolutions 800*600 and above on a computer that is running Windows 8.1, Windows 10, Windows 2000, Windows Vista, 7 or Linux with KDE or GNOME client.

Launch Unified RTMT

Before you begin

For single sign-on in Windows Vista, Windows 7, Windows 8.1 or Windows 10, run Unified RTMT as an administrator.

Note If your Root or Intermediate CA Certificate uses the RSASSA-PSS signature algorithm, do not sign the Tomcat certificate with this CA; otherwise RTMT will not launch. This is because the TLS versions through 1.2 does not support the RSASSA-PSS Signature Algorithm and a bug is opened against Java to add this support in a future TLS version.

Procedure

Step 1 After you install the plug-in, open Unified RTMT.

If you have a Windows Vista, Windows 7, Windows 8.1 or Windows 10 client and you want to use the single sign-on feature, right click the Unified RTMT shortcut on your desktop or start menu and click **Run as Administrator**. Please allow some time for the application to load and relaunch it if you choose to synchronize the time zone.

Important Before launching RTMT on Windows 7 or Vista, ensure that User Account Control (UAC) feature is disabled. For more information on UAC feature, refer https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac.

Step 2 In the **Host IP Address** field, enter either the IP address or hostname of the node or (if applicable) the node in a cluster.

Step 3 Click **OK**.

- If the single sign-on feature is enabled, Unified RTMT does not prompt for the username and password; proceed to step 8.
- If the single sign-on is not enabled, Unified RTMT displays another window prompting for the username and password. Enter the details as given in the following steps.

Step 4 In the **User Name** field, enter the Administrator username for the application.

Step 5 In the **Password** field, enter the Administrator user password that you established for the username.

Note If the authentication fails or if the node is unreachable, the tool prompts you to reenter the node and authentication details, or you can click the Cancel button to exit the application. After the authentication succeeds, Unified RTMT launches the monitoring module from local cache or from a remote node, when the local cache does not contain a monitoring module that matches the back-end version.

Step 6 When prompted, add the certificate store by clicking **Yes**.

Unified RTMT starts.

Note If you sign in using the single sign-on feature, Unified RTMT prompts once for a username and password after you click any one of the following menus:

- **System** > **Performance** > **Performance log viewer**
- **System** > **Tools** > **Trace and Log Central**
- **System** > **Tools** > **Job status**
- **System** > **Tools** > **Syslog Viewer**
- **Voice/Video** > **CallProcess** > **Session Trace**
- **Voice/Video** > **CallProcess** > **Called Party Tracing**
- **Voice/Video** > **Report** > **Learned Pattern**
- **Voice/Video** > **Report** > **SAF forwarders**
- **Analysis Manager**

What to do next

You can create a user with a profile that is limited only to Unified RTMT usage. The user will have full access to Unified RTMT but will not have permission to administer a node.

You can create a Unified RTMT user by adding a new application user in the administration interface and adding the user to the predefined Standard RealtimeAndTraceCollection group.

For complete instructions for adding users and user groups, see the *Administration Guide for Cisco Unified Communications Manager* and *System Configuration Guide for Cisco Unified Communications Manager* .

Cisco Unified Analysis Manager Installation and Setup

This chapter provides information to install Cisco Unified Real-Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 8.1, Windows 10, Windows 2000, Windows Vista, or Linux with KDE and/or Gnome client.

Note RTMT requires at least 128 MB in memory to run on a Windows operating system platform.

Security Guide Updates

The following topics from the *Security Guide for Cisco Unified Communications Manager* are updated for the Windows 10 support for Cisco Unified Communications Manager clients feature.

About Cisco CTL Setup

Device, file, and signaling authentication rely on the creation of the Certificate Trust List (CTL) file, which is created when you install and configure the Cisco Certificate Trust List (CTL).

The CTL file contains entries for the following servers or security tokens:

- System Administrator Security Token (SAST)
- Cisco CallManager and Cisco TFTP services that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall
- ITLRecovery

The CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability on all nodes that run these services. The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in .sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

After the Cisco CTL Client adds a server certificate to the CTL file, you can update the CTL file by running the following CLI commands:

utils ctl set-cluster mixed-mode
: Updates the CTL file and sets the cluster to mixed mode.

utils ctl set-cluster non-secure-mode
: Updates the CTL file and sets the cluster to non-secure mode.

utils ctl update CTLFile
: Updates the CTL file on each node in the cluster.

When you configure a firewall in the CTL file, you can secure a Cisco ASA Firewall as part of a secure Unified Communications Manage system. It displays the firewall certificate as a “CCM” certificate.

Note

- You must run the CLI commands on the publisher node.
- Be aware that regenerating the CallManager certificate changes the signer of the file. Phones that do not support Security by Default will not accept the new CTL file unless CTL files are manually deleted from the phone. For information on deleting the CTL files on the phone, see the *Cisco IP Phone Administration Guide* for your phone model.

Install Cisco CTL Client for Windows

To install the Cisco CTL Client for Windows Vista, Windows 7, Windows 8.1, and Windows 10, perform the following procedure:

Procedure

Step 1 From the Windows workstation or server where you plan to install the client, browse to Unified Communications Manager Administration, as described in the *Administration Guide for Cisco Unified Communications Manager*.

Step 2 In Unified Communications Manager Administration, choose **Application** > **Plugins**.

The **Find and List Plugins** window displays.

Step 3 From the Plugin Type equals drop-down list box, choose **Installation** and click **Find.**

Step 4 Locate the Cisco CTL Client.

Step 5 To download the file, click **Download** on the left side of the window, directly opposite the Cisco CTL Client plug-in name.

Step 6 Click **Save** and save the file to a location that you will remember.

Step 7 To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file).

Note You can also click **Open** from the Download Complete box.

Step 8 The version of the Cisco CTL Client displays; click **Next**.

Step 9 The installation wizard displays. Click **Next**.

Step 10 Accept the license agreement and click **Next**.

Step 11 Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.

Step 12 To begin the installation, click **Next**.

Step 13 After the installation completes, click **Finish**.

Change eToken Password for Windows

Important This information applies to the CTL Client encryption option. You may also set up encryption by using the **utils ctl** CLI command set, which does not require security tokens. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions.*

To change the security token password on a Windows Vista, Windows 7, Windows 8.1, and Windows 10 server or workstation, perform the following procedure:

Procedure

Step 1 Verify that you have installed the Cisco CTL Client on a Windows server or workstation.

Step 2 If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL Client.

Step 3 If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL Client.

Step 4 Choose **Start** > **Programs** > **etoken** > **Etoken Properties**, right-click **etoken**, and choose **Change etoken password**.

Step 5 In the **Current Password** field, enter the password that you originally created for the token.

Step 6 Enter a new password.

Step 7 Enter the new password again to confirm it.

Step 8 Click **OK**.

Windows 10 Support for TAPI and JTAPI Clients

This release of Cisco Unified Communications Manger supports the installation, operation, and uninstallation on Microsoft Windows 10 (32-bit and 64-bit) operating systems for the following clients:

- Cisco Unified TAPI Client (32-bit and x64 clients)
- Cisco Unified JTAPI Client for Windows (32-bit and x64 clients)