New and Changed Features

Information Assurance Features

This section describes the new Information Assurance features added as part of Cisco Unified Communications Manager Release 10.5(2).

Login Attempt Information

When you log in to web applications for Cisco Unified Communications Manager or IM and Presence Service, the main application window displays the last successful system login attempt and the last unsuccessful system login attempt for the current user along with the user ID, date, time, and IP address.

The following web applications display the login attempt information:

- Cisco Unified Communications Manager:
  - Cisco Unified CM Administration
  - Cisco Unified Reporting
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presence Administration

- Cisco Unified IM and Presence Reporting
- Cisco Unified IM and Presence Serviceability

You can use the **show logins unsuccessful** CLI command to view login information for the Disaster Recovery System and Cisco Unified OS Administration web applications.

User Interface Changes

In **Cisco Unified CM Administration** under **User Management** > **End User**, the following buttons were added to the **Find and List Users** window:

- **Enable Selected Local User**—The administrator can enable a single user or multiple users in bulk if needed.
- **Disable Selected Local User**—The administrator can disable a single user or multiple users in bulk if needed.

Note The **Enable Selected Local User** and the **Disable Selected Local User** buttons are visible only when the **Disable User Accounts unused for (days)** service parameter value is set to 1 or more days in the Cisco Database Layer Monitor service.

End User Settings

In **Cisco Unified CM Administration**, the following buttons were added in the **End User Configuration** window.

- **Enable Local User**—The administrator can enable a single user if the **User Status** is set to Disabled.

  Note This button appears only when the **User Status** is set to Disabled.

- **Disable Local User**—The administrator can disable a single user if the **User Status** is set to Enabled.

  Note This button appears only when the **User Status** is set to Enabled.

Note The **Enable Local User** and the **Disable Local User** buttons are visible only when the **Disable User Accounts unused for (days)** service parameter value is set to 1 or more days in the Cisco Database Layer Monitor service.

New Service Parameter

A new service parameter called **Disable User Accounts unused for (days)** was added in the **Service Parameter Configuration** window under the Cisco Database Layer Monitor service. This parameter specifies how often users must authenticate with Cisco Unified Communications Manager to prevent their account from being automatically disabled.

The user account is disabled if the user does not log in to Cisco Unified Communications Manager with their PIN or Password in the number of days that is specified in the **Disable User Accounts unused for (days)** field.

If both the **Disable User Accounts unused for (days)** field and the **Inactive Days Allowed** field in the **Credential Policy Configuration** window are configured, the field that has a lower value takes precedence.

For example: If the **Inactive Days Allowed** field is set to 30 days and the **Disable User Accounts unused for (days)** field is set to 45 days, and the user does not log in to Cisco Unified Communications Manager within 30 days, the user account remains enabled until 45 days but the user will not able to log in.

If the **Disable User Accounts unused for (days)** field is set to 30 days and the **Inactive Days Allowed** field is set to 45 days, and the user does not log in within 30 days to Cisco Unified Communications Manager, the user account is disabled.

Update to Default Threshold for Failed Logon Attempts

With release 10.5(2), the default value for the number of failed logon attempts for both administrator accounts and end user accounts has been changed to five. By default, if an administrator, or an end user, enters an incorrect username and password combination five times, the account is locked.

For end users, you can reconfigure the number of failed logon attempts by assigning a new credential policy in the **End User Configuration** window.

Administrators can reset the administrator password by using the `utils reset_application_ui_administrator_password`.

New System Roles

The following table summarizes the new standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager.

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

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting

For more information about the Roles and User Groups, see *Cisco Unified Communications Manager System Guide* .

Control of Security Status

For releases earlier than Cisco TelePresence Multipoint Control Unit (MCU) Release 4.5 and Cisco TelePresence Conductor Release XC2.3, Cisco Unified Communications Manager provides the call-security icon, according to security levels that are configured for the Cisco Unified Communications Manager servers and the conference participants. With Cisco TelePresence MCU Release 4.5 and Cisco TelePresence Conductor Release XC2.3, SIP video conferencing resources can determine the security status of video conferences and indicate the status to the participants. Sometimes, for Ad hoc and Meet-Me conferences, the security status determined by the SIP video conferencing resources conflicts with the security status determined by Cisco Unified Communications Manager. With Release 10.5(2), you can configure a SIP Cisco TelePresence MCU or a Cisco TelePresence Conductor to control the display of call-security icon in a video conference.

New to the User Interface

In Cisco Unified CM Administration, under **Media Resources** > **Conference Bridge**, an **Allow Conference Bridge Control of the Call Security Icon** check box is added to the **Device Information** area. This check box is unchecked by default. You must check the check box to allow the MCU or the Conductor to control the display of the call-security icon. You can leave the check box unchecked if you want Cisco Unified Communications Manager to control the display of the call-security icon.

This check box is displayed only if you select the **Conference Bridge Type** as **Cisco Telepresence MCU** or **Cisco TelePresence Conductor**.

Touchless Installation for Virtual Machine

Previous releases of Cisco Unified Communications Manager cluster environment required you to install the publisher node first before you proceed to install the subscriber nodes. You had to install the subscriber nodes after adding them to the server page of the publisher node and repeat the same procedure for each subscriber node. With the touchless installation feature, the subscriber nodes are configured dynamically along with the publisher node during their installation.

Touchless installation is a new feature in Cisco Unified Communications Manager. This feature makes the installation process seamless and promotes simplified cluster installation. The touchless installation proceeds

without the requirement to provide any subscriber details in the installation wizard. Subscribers are not dependent on the installation of the publisher. This feature has the following benefits:

- No manual intervention and scheduling during the deployment of a new cluster.
- No manual entry of each subscriber and simplifies the addition of new subscribers to an existing cluster.
- No requirement to wait until the publisher node is active.

Automatic Sequencing of Touchless Server

Automatic sequencing is an approach that facilitates the installations of both the publisher node and the subscriber nodes in a cluster at the same time without manual intervention. Subscriber nodes wait for the publisher node to complete its installation, and then get added to the database of the publisher node to continue with their own installation. After the publisher node is installed, it authenticates each subscriber. After authentication, each subscriber node receives a signal from the publisher node and the installation of that subscriber node continues automatically.

Initiate automatic sequencing by enabling the **Dynamic Cluster Config Enable** timer checkbox and providing a value in the **Dynamic Cluster Config Timer** field. You can enable this timer by using one of the following methods:

- Answer File Generator (AFG) tool.
- Command line interface (CLI) command on the Cisco Unified Communications Manager publisher node.

Answer File Generator

Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to generate the answer files or floppy image files for configuration. These files include `clusterConfig.xml` and `platformConfig.xml` files. The `clusterConfig.xml` file is a new file in Cisco Unified Communications Manager Release 10.5(2).

Start the virtual machine on which you mounted the ISO and floppy image to start the Cisco Unified Communications Manager installation. No manual intervention is required during installation of a standalone node or a cluster.

In a cluster environment, you can install both the publisher node and the subscriber nodes simultaneously. Sometimes, the installation of the subscriber nodes can stop during the installation of the publisher node. In this case, after the publisher node installation is complete, it generates a signal for the subscriber nodes to continue their installation.

Predefined Cluster Configurations (AFG Process)

With the implementation of this feature, the Answer File Generator (AFG) tool generates the `clusterConfig.xml` file along with the existing the `platformConfig.xml` file. If you provide the details of subscriber nodes to the AFG tool, the `clusterConfig.xml` file includes those details. After the Cisco Unified Communications Manager publisher is installed, it reads the `clusterConfig.xml` file and if the publisher finds any subscriber nodes, it adds them to its processnode tables. Adding the subscribers to processnode tables eliminates the need to wait for the Cisco Unified Communications Manager publisher to finish its installation, and then manually add the subscribers on the server page. The entire installation process occurs automatically.

Touchless Installation Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate and Download a Floppy Image, on page 6.	Generate the floppy image using the Answer File Generator tool. The floppy image consists of two precreated answer files—`platformConfig.xml` and `ClusterConfig.xml` files that are downloaded automatically when you download the floppy image.
Step 2	Install a Cluster, on page 7 • Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 7 • Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 8	Install a cluster in one of the following ways: • Install the publisher node and subscriber nodes with no manual intervention by enabling the **Dynamic Cluster Config Enable** timer. • Install the subscriber nodes when you do not enable the **Dynamic Cluster Config Enable** timer while generating the answer files.

Generate and Download a Floppy Image

The Cisco Unified Communications Answer File Generator web application generates the answer files for Cisco Unified Communications installations. These precreated answer files are `platformConfig.xml` and `ClusterConfig.xml` files and are included in the floppy image.

Perform the following procedure to generate and download the floppy image:

Procedure

Step 1 Log in to the Cisco Unified Communications Answer File Generator application.

Step 2 Enter details in the **Clusterwide Configuration** section.

Step 3 Enter details for the primary node in the **Primary Node Configuration** section.

Step 4 To enable Dynamic Cluster Configuration, from the **Dynamic-Cluster-Configuration** section, enable the **Dynamic Cluster Config Enable** timer check box and enter a value in the **Dynamic Cluster Config Timer** field.

Specify a value from 1 to 24 for this field, where the number indicates hours.

Note If you do not enable the **Dynamic Cluster Config Enable** timer and specify its value in the **Dynamic Cluster Config Timer** field while you to generate the answer files, you will have to enable this timer later when the publisher node gets installed automatically but the subscriber nodes are waiting for installation. Then, you will have to add the subscriber nodes manually so that their installation occurs automatically.

Step 5 Enter details for the secondary node in the **Secondary Node Configuration** section.

Step 6 In the **List of Secondary Nodes** list box, select **Add Secondary Node**.
The node that you add as secondary node appears in this list box.

Step 7 Repeat Steps 5 and 6 for additional secondary nodes.

Step 8 Click **Generate Answer Files**.
A dialog box appears showing the details for the primary node, the secondary node, and the `clusterConfig` file.

Step 9 In the **Communications Answer File Generator** dialog box, follow the download instructions, and then click the **Download File** button to download the answer files to your computer.

Install a Cluster

Depending on whether you enabled the **Dynamic Cluster Config Enable** timer in the Answer File Generator tool or not, you can choose one of the following ways to install a cluster:

- Install the publisher node and subscriber nodes with no manual intervention by enabling the **Dynamic Cluster Config Enable** timer. See Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 7.
- Install the subscriber nodes when you do not enable the **Dynamic Cluster Config Enable** timer while generating the answer files. See Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 8.

Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled

Before you begin

Enable the **Dynamic Cluster Config Timer** field by one of the following ways:

- Click the **Dynamic Cluster Config Enable** timer checkbox and enter a value in the **Dynamic Cluster Config Timer** field in the Answer File Generator tool. For details, see Step 4 of the Generate and Download a Floppy Image, on page 6 procedure.
- Enter the **set network cluster subscriber dynamic-cluster-configuration** {*default* | *no. of hours*} CLI command.

Procedure

Step 1 Mount the floppy image on the virtual machine.

Note If the virtual machine is Cisco Unified Communications Manager publisher node, then the floppy image contains both the `platformConfig.xml` and `ClusterConfig.xml` files. However, if the virtual machine is Cisco Unified Communications Manager subscriber node or IM and Presence publisher node or subscriber nodes, the floppy image contains only the `platformConfig.xml` file.

For details on how to create a floppy a new virtual floppy image, see http://docwiki.cisco.com/wiki/How_to_Use_the_AFG_with_the_Virtual_Floppy_Drive.

Step 2 Start the publisher node and all subscriber nodes.
Publisher node and subscriber nodes get installed automatically with no manual intervention. Each subscriber node gets automatically added to the publisher through the automatic sequencing approach.

Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled

If you do not enable the **Dynamic Cluster Config Timer** field in the Answer File Generator tool, the publisher node gets installed automatically. However, the subscriber nodes will be waiting for their installation.

To avoid the waiting time of the subscriber nodes so that the cluster installation continues, perform one of following tasks:

- From the Cisco Unified Communications Manager, select the **Web Interface** and click the **Server** tab and add the subscriber nodes manually.
- Enable the **Dynamic Cluster Config Timer** field from the CLI of the publisher node with the new CLI command that is available in Cisco Unified Communications Manager Release 10.5(2)—**set network cluster subscriber dynamic-cluster-configuration** {*default* | *no. of hours*}. After you enable this timer, the subscriber nodes get added to the publisher automatically and the installation of the subscriber nodes proceeds.

Note

- If you need to add one or more subscribers as specified for the publisher node, you can add them while you generate the `platformconfig.xml` file. You have to specify the publisher node and the subscriber nodes. If the **Dynamic Cluster Config Timer** timer is still active, subscribers get automatically added to the publisher and the installation of the subscriber nodes continues.
- This feature has no limitation on predefining the number of subscriber nodes that you need to add to a publisher node.

Use the WinImage tool to create the disk images. Mount the ISO images through VMware ESXi.

Before you begin

Place the floppy image at datastore from where it is accessible to virtual machine for mounting.

Procedure

Step 1 Start the virtual machine to start the cluster installation.

Step 2 From the **VM** menu, choose **Edit settings** to mount the floppy image that you have created from the Answer File Generator tool.
The **Virtual Machine Properties** dialog box appears.

Step 3 From the available hardware list, select **Floppy drive 1**.

Step 4 In the **Device Type** section, select **Use the existing floppy image in the database**, and then click **Browse** to navigate to the floppy image.

Step 5 Click **OK**.
The floppy image is attached.

Step 6 Select the **CD/DVD Drive 1** > **Connect to ISO image on local disk** option from the toolbar and choose **CD/DVD Drive1** > **Connect to ISO image on a datastore**, navigate to the data store to select the installer ISO image, and click **OK**.
The ISO image is attached and the installation starts.

Step 7 (Optional) If you want to test the media before the installation, click **OK** in the **Disc Found** message box, or click **Skip** to skip testing the media before the installation.
The installation proceeds without any manual intervention. The publisher is installed and the subscribers are added to the publisher.

IM and Presence Service Integration

This feature supports heterogeneous cluster-wide installation that includes Cisco Unified Communications Manager and IM and Presence Service nodes. The concept and installation process for IM and Presence Service is same as the installation process for Cisco Unified Communications Manager in a cluster.

From the AFG tool, check the **Dynamic Cluster Config Timer** check box, select IM and Presence Service, and enter the details for Cisco Unified Communications Manager publisher node, IM and Presence Service publisher node, and IM and Presence Service subscriber details (if any). Then, AFG tool generates the `clusterConfig.xml` file along with `platformConfig.xml` file for each node. You can use this `clusterConfig.xml` file only with Cisco Unified Communications Manager publisher node along with `platformConfig.xml` file that is generated for this node. For all other nodes, only `platformConfig.xml` file is used.

Answer File Generator (AFG) saves the domain name of IM and Presence Service publisher in the `clusterConfig.xml` file along with the existing details.

The integration of Cisco Unified Communications Manager with IM and Presence includes the following tasks:

- The IM and Presence Service publisher is added to the processnode table with domain name after the installation of Cisco Unified Communications Manager.
- Cisco Unified Communications Manager and IM and Presence Service nodes are added to the processnode table using the IP address, if available.
- When you add the IM and Presence Service publisher through CLI, the domain is added.

CLI Commands

Cisco Unified Communications Manager Release 10.5(2) includes the following new CLI commands:

Note For details on CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* and the *Installing Cisco Unified Communications Manager*.

set network cluster subscriber details

Use this command to add subscriber to the processnode or appserver table when Tomcat Webserver is server down and GUI is inaccessible.

set network cluster subscriber details *servertype hostname ip domainname*

Syntax Description

Parameter	Description
servertype	Choose one of these products for this parameter— Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection. This field is mandatory.
hostname	The hostname of the node that you add to the cluster. The hostname is supported on the same domain. This field is mandatory.
ip	The IPv4 address of the node that you add to the cluster. This field is mandatory for IM and Presence publisher and Cisco Unity Connection.
domainname	The domain name of the IM and Presence Service publisher. This field is mandatory for IM and Presence publisher.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

set network cluster subscriber dynamic-cluster-configuration

Use this command to enable the Dynamic Cluster Configuration on the publisher. Use this command to specify the duration in which you can add subscriber nodes to the publisher server table. The addition of subscriber nodes is authenticated immediately and those nodes need not wait for the publisher details during the installation of the subscriber nodes.

set network cluster subscriber dynamic-cluster-configuration {**default** | **no. of hours**}

Syntax Description

Parameter	Description
default	Enables the Dynamic Cluster Configuration for 24 hours.
no. of hours	Specifies a value from 1 to 24 hours.

Command Modes

Administrator (admin)

Requirements

Applies to Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

show network cluster

This command is enhanced to show the remaining timer value when you enable Dynamic Cluster Configuration.

show network cluster

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Cisco Unified Communications Manager, IM and Presence Service on Cisco Unified Communications Manager, and Cisco Unity Connection

unset network cluster subscriber details

This command shows the message that you need to delete a subscriber node from the GUI instead of the command prompt.

unset network cluster subscriber details

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Unified Communications Manager, IM and Presence Service on Communications Manager, and Cisco Unity Connection

Message to delete the subscriber from GUI

```
admin: unset network cluster subscriber details
Please use the Cisco Unified Communications Manager on the first node.
Navigate to System > Server and click “Find”.
   Unable to del: NULL
Executed command unsuccessfully.
```

unset network cluster subscriber dynamic-cluster-configuration

This command disables Dynamic Cluster Configuration on the publisher. The value of **Dynamic Cluster Configuration** option is set to zero on publisher.

unset network cluster subscriber dynamic-cluster-configuration

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

show logins unsuccessful

Use this command to list recent unsuccessful login attempts to the following web applications:

- On Unified Communications Manager
  - Disaster Recovery System
  - Cisco Unified OS Administration
- On IM and Presence Service
  - IM and Presence Disaster Recovery System
  - Unified IM and Presence OS Administration

show logins unsuccessful [*number*]

Syntax Description

Parameters	Description
number	Specifies the number of most recent logins to display. The default is 20.

Command Modes

Administrator (admin)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Unified Communications Manager and IM and Presence Service

Support Removed for utils vmtools status

The `utils vmtools status` CLI command is no longer supported. For VMware status, check the vSphere client instead.

Single Sign-On Updates

The following SAML SSO - related enhancements are introduced in Cisco Unified Communications Manager, Release 10.5(2).

Export/Import of SSO Metadata

In **Cisco Unified Communications Manager Administration**, under **System** > **SAML Single Sign-On**, the **Export All Metadata** button is enabled by default, regardless of whether the SAML SSO state is set to active.

Enable SAML SSO

The following note was added to the Enable SAML SSO procedure in the *Features and Services Guide*.

Note After you click **Import IdP Metadata** and click **Next**, a status message appears in the **SAML Single Sign-On Configuration** window. It displays information to either skip or continue further with steps to upload the server metadata to the IdP.

Increased Capacity of IP Voice Media Streaming Application and Expanded MOH Audio Source

Cisco IP Voice Media Streaming application is installed automatically when you install Cisco Unified Communications Manager. Activate this application to enable the Music On Hold (MOH) feature.

With this release, the capacity of Cisco Unified Communications Manager to support unique and concurrent MOH audio sources, while the Music On Hold service is running on the MOH server, is increased from 51 to 501. The MOH audio sources are numbered from 1 to 501 with the fixed MOH audio source remaining at the number 51.

The fixed MOH device cannot use an audio source that connects through a USB MOH device, because Cisco Unified Communications Manager does not support USB when running on VMware. Use of the fixed MOH USB device is not supported on VMware. However, provision the external sound device for use with deployments that utilize Cisco Unified Survivable Remote Site Telephony (SRST) multicast MOH.

You can configure each MOH audio source to use a custom announcement as an initial greeting and/or an announcement that is played periodically to callers who are hearing the music. Cisco Unified Communications Manager provides 500 custom announcements that you can use on one or multiple MOH audio sources. These announcements are not distributed between the Cisco Unified Communications Manager servers within a cluster. You have to upload these custom announcement files to each server that provides the MOH and announcement services. You must also upload each custom music file for MOH audio sources to each server.

Performance Impact of Media Devices with Services

The Cisco IP Voice Media Streaming application runs as a service for four media devices—annunciator (ANN), software conference bridge, Music On Hold (MOH), and software media termination point. Activate this service on a Cisco Unified Communications Manager server as coresident with call processing. When you activate this service, ensure that you configure these media devices for limited capacity to avoid any impact on the call processing. The default settings for the media devices are defined based on this coresident operation. You can adjust these settings by reducing the use of one or more media devices to increase other settings.

For example, if you are not using software media termination point devices, you can choose the **Run Flag** setting for the SW MTP to **False**, select **System** > **Service Parameters** > **Cisco IP Voice Media Streaming App service** > **MTP Parameters** , and add the **MTP Call Count** setting to **Media Resource** > **MOH Server** > **Maximum Half Duplex Streams** configuration. Depending on the call traffic, you can modify the default settings. However, monitor the server performance activity for CPU, memory, and IO wait. For higher capacity clusters, such as the ones using 7500 user OVA configuration, it is possible to increase the default media device settings for Call Count by 25%.

For installations where you expect high usage of the media devices, such as Music On Hold, or where high call volumes require higher number of media connections, activate the Cisco IP Voice Media Streaming application service on one or more of the Cisco Unified Communications Manager servers which do not have call processing activated. Activating this service limits the impact of media device usage to other services, such as call processing. Then, you can increase the configuration settings for maximum number of calls for the media devices.

When you activate Cisco IP Voice Media Streaming application as co-resident with Cisco Unified Communications Manager service, it can impact call processing performance. To increase the capacity settings for Music On Hold or annunciator from the default settings, it is suggested to activate Cisco IP Voice Media Streaming application on a server without activating Cisco Unified Communications Manager.

The CPU performance is impacted by MOH when active callers are on hold or when multicast MOH audio streams are configured.

Table 2: General Performance Results

Configuration Notes	CPU Performance
Dedicated MOH server, 1000 held calls, 500 MOH sources with greeting and periodic announcements.	25–45% (7500 user OVA configuration)
Native call queuing with dedicated MOH server and annunciator server, 1000 queued calls, 500 MOH sources with greeting and periodic announcements. An annunciator can play up to 300 simultaneous greeting announcements.	25–45% (7500 user OVA configuration)
Dedicated MOH server, 500 held calls, 500 MOH sources with greeting and periodic announcements.	15–35% (7500 user OVA configuration)

Table 3: Extrapolated Recommendations

Configuration	Recommendation Limit
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 2500 OVA (moderate call processing).	MOH: 500 held callers, 100 MOH sources, and 48 to 64 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 2500 OVA.	MOH: 750 held callers, 250 MOH sources, and 250 annunciator callers.
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 7500/10K OVA (moderate call processing).	MOH: 500 held callers, 250 MOH sources, and 128 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 7500/10K OVA.	MOH: 1000 held callers, 500 MOH sources, and 300-700 annunciator callers (with 1 MOH codec). **Note** Reduce annunciator to 300 for two MOH codecs.

Note These recommendations are specific to MOH/ANN devices. If you combine these devices with the software media termination point (MTP) and call forward busy (CFB) devices, reduce the limits to provide streams.

Configuration Limitations for Capacity Planning

The Cisco IP Voice Media Streaming application and Self Provisioning IVR services use a media kernel driver to create and control Real-time Transfer Protocol (RTP) streams. This media kernel driver has a capacity of 6000 streams. These streams allow the media devices and IVR to make resource reservations.

These reservations are based on the following capacity calculations:

Media Device	Capacity
Annunciator	(Call Count service parameter) * 3 Where 3 indicates total of receiving (RX) and transmitting (TX) calls for endpoint and 1 for .wav file.
Software Conference Bridge	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Software Media Termination Point	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Music On Hold	((Maximum Half Duplex Streams) * 3) + (501 * 2 * [number of enabled MOH codecs]) Where: • (Maximum Half Duplex Streams) is a configuration setting on the MOH device configuration administration web page. • 3 indicates total steams of RX, TX, and greeting announcement .wav file. • 501 indicates the maximum number of Music On Hold (MOH) sources. • 2 indicates music .wav stream and possible multicast TX stream. • [number of enabled MOH codecs] is based on how many MOH codecs are enabled in the Cisco IP Voice Media Streaming application service parameters.
Self Provisioning IVR Service	(500 * 2) Where 500 indicates callers, and 2 indicates total streams from RX and TX streams.

Hence, to enable MOH to support a maximum of 1000 callers, use the following equation: `1000 * 3 + 501 * 2 * 1 = 4002` driver streams with one enabled codec and `1000 * 3 +501 * 2 * 2 = 5004` with two enabled codecs. Reduce the remaining devices and deactivate the Self Provisioning IVR service to limit total reservations to 6000, which allows the MOH device to make these reservations. It may

also require that you do not activate the Self Provisioning IVR service on the same server with Cisco IP Voice Media Streaming application.

If configuration settings of the media devices exceed the capacity of the media device driver, the media devices that register with the device driver first will be able to reserve their required stream resources. The media devices that register later are restricted to fewer than requested stream resources. The later registered media devices result in logging some alarm messages and automatically reducing the call count for the restricted media device.

Note A media kernel driver with a capacity of 6000 streams might not support that many simultaneous media device connections.

Configure Music On Hold Audio Source

Use this procedure to configure Music On Hold audio sources. You can configure audio streams and associate uploaded files to an audio stream. You can configure up to 500 audio streams.

Note If a new version of an audio source file is available, perform the update procedure to use the new version.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Audio Source**.

Step 2 Do either of the following:

- Click **Find** and select an existing audio stream.
- Click **Add New** to configure a new stream.

Step 3 From the **MOH Audio Stream Number**, select an audio stream.

Step 4 Enter a unique name in the **MOH Audio Source Name** field.

Step 5 Optional. Check the **Allow Multi-casting** check box if you want to allow this file to be multi-casted.

Step 6 Configure the audio source:

- Check the **Use MOH WAV file** source radio button and from the **MOH Audio Source File**, select the file you want to assign.
- Check the **Rebroadcast External Multicast Source** radio button and enter the multicast source IP Address details.

Step 7 In the **Announcement Settings for Held and Hunt Pilot Calls** section, assign the announcements that you want to use for this audio source.

Step 8 Configure the remaining fields in the **Music On Hold Audio Source Configuration** window. For help with the fields and their settings, see the online help.

Step 9 Click **Save**.

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration Solutions use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) for signaling and media encryption. Currently, Advanced Encryption Standard (AES) with a 128-bit encryption key is used as the encryption cipher. AES also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method. These algorithms cannot effectively scale to meet the required changing security and performance needs. To meet escalating security and performance requirements, the algorithms and protocols for encryption, authentication, digital signatures, and key exchange in Next-Generation Encryption (NGE) are developed. Also, AES 256 encryption support is provided instead of AES 128 for TLS and Session Initiation Protocol (SIP) SRTP that supports NGE.

With Unified Communications Manager Release 10.5(2), the AES 256 encryption support for TLS and SIP SRTP is enhanced to focus on AES 256 cipher support in signaling and media encryption. This feature is useful for the applications that run on Unified Communications Manager to initiate and support TLS 1.2 connections with the AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and is Federal Information Processing Standards (FIPS) compliant.

This feature has the following requirements:

- The connection that the SIP trunk and SIP line initiates.
- The ciphers that Unified Communications Manager supports for SRTP calls over SIP line and SIP trunk.

Note With this release, TLS 1.2 is supported on some interfaces like SIP, but is not supported on all interfaces. It is recommended that you leave TLS 1.0 and 1.1 enabled in your Collaboration deployment.

AES 256 and SHA-2 Support in TLS

The Transport Layer Security (TLS) protocol provides authentication, data integrity, and confidentiality for communications between two applications. TLS 1.2 is based on Secure Sockets Layer (SSL) protocol version 3.0, although the two protocols are not compatible with each other. TLS operates in a client/server mode where one side acts as a server and the other side acts as a client. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate securely over a network. To operate, TLS requires TCP as the reliable transport layer protocol.

In Unified Communications Manager Release 10.5(2), AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 is an enhancement to handle the connection that is initiated by the SIP Trunk and the SIP line. The supported ciphers, which are AES 256 and SHA-2 compliant, are listed as follows:

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256—The cipher string is ECDH-RSA-AES128-GCM-SHA256.
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384—The cipher string is ECDH-RSA-AES256-GCM-SHA384.

where:

- TLS is Transport Layer Security

- ECDH is Elliptic curve Diffie–Hellman, which is an algorithm
- RSA is Rivest Shamir Adleman, which is an algorithm
- AES is Advanced Encryption Standards
- GCM is Galois/Counter Mode

In addition to the newly-supported ciphers, Unified Communications Manager Release 10.5(2) continues to support TLS_RSA_WITH_AES_128_CBC_SHA. The cipher string of this cipher is AES128-SHA.

Note

- The Unified Communications Manager certificates are based on RSA.
- In Unified Communications Manager 10.5(2), Cisco Endpoints (phones) do not support the above mentioned new ciphers for TLS 1.2.
- With AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 enhancement in Unified Communications Manager 10.5(2), the default key size for Certificate Authority Proxy Function (CAPF) is increased to 2048 bits.

AES 256 Support in SRTP SIP Call Signaling

Secure Real-time Transport Protocol (SRTP) defines the methods of providing confidentiality and data integrity for both Real-time Transport Protocol (RTP) voice and video media and their corresponding Real-time Transport Control Protocol (RTCP) streams. SRTP implements this method through the use of encryption and message authentication headers. In SRTP, encryption applies to the payload of the RTP packet only, and not to the RTP header. However, message authentication applies to both the RTP header and the RTP payload. Also, SRTP indirectly provides protection against replay attacks because message authentication applies to the RTP sequence number within the header. SRTP uses Advanced Encryption Standards (AES) with a 128-bit encryption key as the encryption cipher. It also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method.

Unified Communications Manager 10.5(2) supports crypto ciphers for the SRTP calls over SIP line and SIP trunk. These crypto ciphers are AEAD_AES_256_GCM and AEAD_AES_128_GCM, where AEAD is Authenticated-Encryption with Associated-Data, and GCM is Galois/Counter Mode. These ciphers are based on GCM. If these ciphers are present in the Session Description Protocol (SDP), they are treated with higher priority as compared to the AES 128 and SHA-1 based ciphers. Cisco Endpoints (phones) do not support these new ciphers that you add for Unified Communications Manager 10.5(2) for SRTP.

In addition to the newly supported ciphers, Unified Communications Manager 10.5(2) continues to support the following ciphers:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 encryption is supported in the following calls:

- SIP line to SIP line call signaling
- SIP line to SIP trunk signaling

- SIP trunk to SIP trunk signaling

Cisco Unified Communications Manager Requirements

- Support for TLS Version 1.2 on the SIP trunk and SIP line connections is available.
- Cipher support—TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (cipher string ECDHE-RSA-AES256-GCM-SHA384) and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (cipher string ECDHE-RSA-AES128-GCM-SHA256)—is available when the TLS 1.2 connection is made. These ciphers are based on GCM and conform to SHA-2 category.
- Unified Communications Manager initiates TLS1.2 with the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ciphers. If the peer does not support TLS1.2, then Unified Communications Manager will fall back to TLS 1.0 with the existing AES128-SHA cipher.
- The SRTP calls over SIP line and SIP trunk support the GCM-based AEAD_AES_256_GCM and AEAD_AES_128_GCM ciphers.

Interactions and Restrictions

- Unified Communications Manager requirements apply to SIP line and SIP trunk, and basic SIP to SIP calls only.
- The device types that are based on non-SIP protocols will continue to support the existing behavior with the TLS versions with the supported ciphers. Skinny Call Control Protocol (SCCP) also supports TLS 1.2 with the earlier supported ciphers.
- SIP to non-SIP calls will continue to use AES 128 and SHA-1 based ciphers.

Remote Control of TelePresence Product Specific Configurations

Beginning with Release 10.5(2), Cisco Unified Communications Manager can remotely acquire and manage product specific settings for Cisco TelePresence endpoints on behalf of Cisco TelePresence users.

When a Cisco TelePresence endpoint first registers with Cisco Unified Communications Manager, or if a Cisco TelePresence user modifies their product-specific settings from their endpoint, SIP signaling communicates those settings to the Cisco Unified Communications Manager database and the settings display under the Product-Specific-Configuration Layout heading of the Phone Configuration window.

Once those settings are obtained, Cisco Unified Communications Manager administrators can set and change product-specific settings, including administration passwords, on behalf of Cisco TelePresence users.

To communicate the new settings back to the phone, administrators must reset the phone.

IM and Presence Service Stream Management

Cisco Unified Communications Manager IM and Presence Service Release 10.5(2) supports Stream Management for instant messaging. Stream Management is implemented using the XEP-0198 specification,

which defines an Extensible Messaging and Presence Protocol (XMPP) extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption. For more information about XEP-0198, see the specification at http://xmpp.org/extensions/xep-0198.html.

If there is a temporary loss of communication between IM and Presence Service and Cisco Jabber, Stream Management ensures that any instant messages that are sent during the communications outage are not lost. A configurable timeout period determines how such messages are handled:

- If Cisco Jabber reestablishes communication with IM and Presence Service within the timeout period, the messages are resent.
- If Cisco Jabber does not reestablish communication with IM and Presence Service within the timeout period, the messages are returned to the sender.
- Messages that are sent after the timeout period lapses are stored offline and delivered when Cisco Jabber resumes communication with IM and Presence Service.

Administrators can enable Stream Management on a cluster-wide basis. Use the following Cisco XCP Router service parameters to configure Stream Management.

Service Parameter	Description
Enable Stream Management	Enables or disables Stream Management cluster-wide. The default setting is Enabled.
Stream Management Timeout	The maximum number of seconds that a session will wait before the stream is resumed and the message is resent. If connection to IM and Presence Service cannot be restored within this time frame, the message is returned to the sender. Any messages that are sent after this timeout ends and before Cisco Jabber logs in again with IM and Presence Service are stored offline and resent after relogin. The default setting is 60.
Stream Management Buffer Size	The maximum number of packets that can be stored in a buffer. If Cisco Jabber needs more space than is available in the buffer, IM and Presence Service starts to return messages to senders before they are removed from the buffer to make room for more messages. The default setting is 100.
Acknowledgement Request Rate	The number of stanzas sent by IM and Presence Service before Cisco Jabber is requested to provide the count of the last stanza it received. **Note** A smaller Acknowledgement Request Rate leads to increased network traffic but reduced memory use. The default setting is 5.

To configure these parameters, log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters** and choose the Cisco XCP Router Service.

IM and Presence Service Managed File Transfer

Managed file transfer (MFT) allows an IM and Presence Service client, such as Cisco Jabber, to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

The managed file transfer configuration is specific to this feature and has no impact on the message archiver feature for regulatory compliance.

For more information about the managed file transfer feature, see the *Configuration and Administration Guide of IM and Presence Service on Cisco Unified Communications Manager*.

Two New User Interface Windows

External File Servers

You use the controls in this window to configure an external file server on IM and Presence Service, including the user credentials and connection information.

File Transfer Configuration

You use the controls in this window to configure one of the following options for file transfers on IM and Presence Service: **Disable**, **Peer-to-Peer**, **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer**.

New File Server Troubleshooting Tests

There are seven new tests that are conducted after you complete the deployment of an external file server:

- Verify external file server reachability (pingable)
- Verify that the external file server is listening for connections
- Verify external file server public key is correct
- Verify node public key is configured correctly on the external file server
- Verify external file server directory is valid
- Verify external file server has been mounted successfully
- Verify that free disk space is available on the file server

New Real Time Monitoring Tool Managed File Transfer Alarms

There are three new alarms, two that test connection status between the IM and Presence Service and the external servers and one that tests disk space on the external file server.

- XcpMFTExtFsMountError—Cisco XCP File Transfer Manager has lost its connection to the external file server.
- XcpMFTExtFsFreeSpaceWarn—Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.

- XcpMFTDBConnectError—Cisco XCP data access layer was unable to connect to the database.

New Real Time Monitoring Tool Managed File Transfer Counters

The Real Time Monitoring Tool (RTMT) now contains one new folder and six new counters for the managed file transfer feature:

- Cisco XCP MFT Counters
  - MFTBytesDownloadedLastTimeslice
  - MFTBytesUpoadedLastTimeslice
  - MFTFilesDownloaded
  - MFTFilesDownloadedLastTimeslice
  - MFTFilesUploaded
  - MFTFilesUploadedLastTimeslice

Deprecated Setting

In the **Service Parameter Configuration** window for the Cisco XCP Router (Active) service, the **Enable file transfer** drop-down list has been removed from the XCP Router Global Settings (Clusterwide) area.