New and Changed Information for Cisco Unified Communications Manager, Release 10.0(1)

First Published: December 03, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-31056-01

CONTENTS

CHAPTER 1

Introduction

The *New and Changed Information for Cisco Unified Communications Manager, Release 10.0(1)* contains new and changed information for Cisco Unified Communications Manager (Unified Communications Manager), Release 10.0(1). The document is organized into the following chapters:

- Installation, Upgrade, Migration and Deployment
- Features
- Cisco Unified IP Phones

CHAPTER 2

Installation, Upgrade, Migration, and Deployment

This section contains information about the following topics:

Installation

There are no changes to the installation process for Cisco Unified Communications Manager (Unified Communications Manager); however, if you install the IM and Presence Service as part of your Unified Communications Manager system, the process has changed.

In this release, IM and Presence nodes are installed as subscribers to the Unified Communications Manager publisher node. A wizard guides you through the installation process, and prompts you to enter the hostname and password of the Unified Communications Manager publisher node.

When installing an IM and Presence Service server, perform the following using Cisco Unified Communications Manager Administration:

1. Pre-installation: Add the IM and Presence Service server to the Cisco Unified Communications Manager Administration GUI using **System** > **Server**.
2. Post-installation:

   You can add the installed server to an appropriate presence redundancy group that is configured for high availability using Cisco Unified Communications Manager Administration **System** > **Presence Redundancy Group**.

   Assign users to the server using either **System** > **Server** or **User Management** > **Assign Presence Users for IM and Presence Service**.

Upgrade

This section contains information about upgrading Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) software.

Upgrade Paths

The following tables list the range of upgrade paths that are supported for Unified Communications Manager. For more detailed information about supported upgrade paths, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Table 1: Cisco Unified Communications Manager Upgrade Paths

From	To	Upgrade Type
8.5(x) or older	10.0(1)	Refresh upgrade, COP file needed
8.6(x) to 9.x	10.0(1)	Refresh upgrade
10.0(1)x	10.0(1)y	Standard upgrade

For upgrades from 8.5(x) and older, you must install a COP file on all nodes before you begin the upgrade process. You can download the COP file from Cisco.com.

Table 2: IM and Presence Upgrade Paths

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) to 8.6(1)	10.0(1)	Refresh upgrade, COP file needed
8.6(4) to 9.x	10.0(1)	Refresh upgrade
10.0.1.x	10.0.1.y	Standard upgrade

For upgrades from Cisco Unified Presence 8.5(4) through to 8.6(1), you must install a COP file on all nodes before you begin the upgrade process. You can download the COP file from Cisco.com.

Version Restrictions

Unified Communications Manager and IM and Presence Service software versions must be compatible.

When you upgrade IM and Presence nodes, the software version must be compatible with the software version of the Unified Communications Manager. Ensure that the software versions meet the following requirements:

- The software version of the first IM and Presence node that you upgrade must match the first two numbers of the software version that is installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2.

- The software version of the subsequent IM and Presence nodes that you upgrade must match five numbers of the software version that is installed on the first IM and Presence node.

Note You cannot upgrade IM and Presence unless the upgraded release of Unified Communications Manager is already installed on the active or inactive partition. You must upgrade Unified Communications Manager before you can upgrade IM and Presence to the matching version.

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications applications from the perspective of migration, fresh installs, upgrades, switching versions, rebooting clusters, and changing IP addresses or hostnames. For more information, see the Cisco Prime Collaboration Deployment section under New Features.

Migration

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications applications from the perspective of migration, fresh installs, upgrades, switching versions, rebooting clusters, and changing IP addresses or hostnames. For more information, see the Cisco Prime Collaboration Deployment section under New Features.

Deployment

In Release 10.0(1) and later, Cisco only supports virtualized deployments of Cisco Unified Communications Manager (Unified Communications Manager) on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration. In Release 10.0(1) and later, Cisco does not support deployments of Unified Communications Manager on Cisco Media Convergence Server servers.

Tape device is not supported in virtualized deployments. Upgrade to 10.0(1) and later removes the devices/schedules configured with tape device. Ensure to add the network device(if it does not exists) and re-configure the schedule for backup/restore post upgrade.

For more information about the deployment of Unified Communications Manager in a virtualized environment, see:

http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

CHAPTER 3

New Features

This chapter contains information about new features for Cisco Unified Communications Manager, Release 10.0(1).

2048 Bits Certificate Support and SHA-256 Algorithm Support

Cisco Unified Communications Manager supports generation of certificates in 2048 bits and/or SHA-256. The OS Administrator creates certificate signing requests(CSR) and generates new certificates for 1024/2048 bit and SHA1/SHA-256 algorithm. Default is 1024 bit and SHA1.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

The certificate generation and certificate signing requests procedures have changes.

Serviceability Considerations

No changes.

Procedure Changes

Regenerate Certificate

You can regenerate certificates from the Cisco Unified Communications Operating System as an operating system security function. For more information about regenerating certificates, see the *Cisco Unified Communications Manager Security Guide*.

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate including a third party signed certificate if one was uploaded.

Note Certificate regeneration or upload a of third party signed certificates should be performed during maintenance.

The following table describes the system security certificates you can regenerate from the Cisco Unified Communications Operating System and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide*.

Table 3: Certificate Names and Descriptions

Name	Description	Related Services
tomcat	This self-signed root certificate is generated during installation for the HTTPS node.	tomcat
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.	Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master
CallManager	This self-signed root certificate is installed automatically when you install Cisco Unified Communications Manager. This certificate provides node identification, including the node name and the Global Unique Identifier (GUID).	CallManager and CAPF
CAPF	The system copies this root certificate to your node or to all nodes in the cluster after you complete the Cisco client configuration.	CallManager and CAPF
TVS	This is a self-signed root certificate.	TVS

If you regenerated the certificate for Cisco Certificate Authority Proxy Function (CAPF) or Cisco Unified Communications Manager and a CTL client is configured, rerun the CTL client.

After you regenerate certificates in the Cisco Unified Communications Operating System, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register with Cisco Unified Communications Manager. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Generate New**.
The Generate Certificate dialog box opens.

Step 3 From the Certificate Name drop-down list, choose a certificate name .
For details about certificate names, see the Certificate Names and Descriptions table.

Step 4 From the Key Length drop-down list, choose 1024 or 2048.

Step 5 From the Hash Algorithm drop-down list, choose SHA1 or SHA256.

Step 6 Click **Generate New**.

What to Do Next

Restart all services that are affected by the regenerated certificate as listed in the Certificate Names and Descriptions table.

Rerun the CTL client (if configured) after you regenerate the CAPF or CallManager certificates.

Perform a system backup to capture the newly regenerated certificates. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Generate Certificate Signing Request

To generate a CSR, follow these steps:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Generate CSR**.
The Generate Certificate Signing Request dialog box opens.

Step 3 From the Certificate Name drop-down list, choose a certificate name.
For details about certificate names, see the Certificate Names and Descriptions table.

Step 4 From the Key Length drop-down list, choose 1024 or 2048.

Step 5 From the Hash Algorithm drop-down list, choose SHA1 or SHA256.

Step 6 Click **Generate CSR**.

Note Generating CSR overwrites any existing CSR.

Acknowledgment in AuditLog

You can set up a warning message when an administrator attempts to sign in to any of the following Cisco Unified Communications Manager interfaces:

- Cisco Unified Reporting
- Cisco Unified Communications Manager Administration
- Disaster Recovery System
- Cisco Unified Serviceability
- Cisco Unified Operating System Administration

The administrator can sign in only after acknowledging the warning message. The acknowledgment is recorded in the audit logs along with the username of the administrator.

Note You can enable the acknowledgment by checking the Require User Acknowledgment checkbox in the Customized Logon Message window (**Software Upgrades** > **Customized Logon Message**) in the Cisco Unified Operating System Administrative interface.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

AuditLog Viewer

Cisco Unified Communications Manager, Release 10.0(1) provides an AuditLog Viewer in Cisco Unified Real Time Monitoring Tool (RTMT). You can display the following messages in AuditLog Viewer:

- AuditApp Logs - To monitor actions of one or more users.
- Vos Logs - To monitor activities of a specific terminal, port, or network address of the system.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

The following table describes the AuditLog Viewer settings (**Tools** > **AuditLog Viewer**)

Table 4: AuditLog Viewer Settings

Setting	Description
Refresh	Updates the contents of the current log on the AuditLog viewer. **Tip** You can configure the AuditLog viewer to automatically update the current log file every 5 seconds by checking the **Auto Refresh** check box.
Clear	Clears the display of the current log.
Filter	For AuditApp logs, it limits the logs displayed based on the UserID that you select. For Vos logs, it limits the logs displayed based on the set of options (Address, Terminal, and Type) that you select. **Tip** You can display the logs other than the set of options you selected by checking the **Filter Inverse** check box.
Clear Filter	Removes the filter that limits the type of logs that display.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your system.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Display AuditApp Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**.

Step 2 From the Select a Node drop-down list, choose the server on which the logs that you want to view are stored.

Step 3 Double-click the **AuditApp Logs** folder.

Step 4 Click the **.log** file located outside the Archive folder to view the current logs. The AuditApp Logs for the selected node are displayed in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The auditlog message for that particular entry appears in a new window.

Tip You can filter the auditlog message display results by choosing an option in the Filter By drop-down list box. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Display Cisco Unified OS Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**

Step 2 From the **Select a Node** drop-down list, choose the node where the logs that you want to view are stored.

Step 3 Double-click the **Cisco Unified OS Logs** folder.

Step 4 Click the **vos-audit.log** file located outside the Archive folder to view the current logs. The Cisco Unified OS Logs for the selected node appear in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The Cisco Unified OS log message for that particular entry is displayed in a new window.

Tip You can filter the Cisco Unified OS log message display results by choosing the set of options in a pop up window that appears after you click **Filter**. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Call Dusting

Call Dusting allows you to transfer an active or hold call session from a hardware endpoint to a support bring your own device (BYOD). You can trigger this feature by pressing a MOVE softkey.

Consider the following call flow:

1. When the BYOD and hardware endpoint are within proximity of each other, you press a move softkey which triggers Unified Communications Manager to ring all shared-line devices with the same user ID.
2. After the BYOD answers, Unified Communications Manager seamlessly switches the call from the endpoint to the answering device (BYOD).

The move softkey rings all shared-line devices, whether they are configured as a mobile phone or Remote Destination.

For a dual-mode device that uses single registration, the call rings on the preferred side (Wi-Fi or cellular) which is indicated in the REGISTER message. For other dual-mode clients, the call rings through Wi-Fi first. If the device is not registered to Wi-Fi, the call routes through the cellular network.

Note

- When the call is on hold, you can still move the call to BYOD by pressing the move softkey. When the call is dusted to BYOD, the call is active after it is answered.
- This feature applies only to supported SIP phones.
- Call dusting has higher priority than Time-of-Day Routing, Access List, and Do Not Disturb.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Call Home Configuration

The Call Home feature allows to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

Installation procedures for Cisco Unified Communications Manager and Cisco Unified Serviceability Administration contain the following changes:

In Cisco Unified Serviceability, choose **Call Home** > **Call Home Configuration**.

The Call Home Configuration window appears.

Note You can also configure the Cisco Smart Call Home while installing the Cisco Unified Communications Manager. During installation, the user can select one of the following options:

- Enabled (Smart Call Home)
- Enabled (Anonymous Call Home)
- None
- Disabled

The following table describes the settings to configure the Unified Communications Manager Call Home.

Table 5: Call Home Configuration Settings

Field Name	Description
Call Home Message Schedule	Displays the date and time of the last Call Home messages that were sent and the next message that is scheduled.

Field Name	Description
Call Home*	From the drop-down list, select one of the following options: • **None**: Select this option if you chose the Remind Me Later option during Cisco Unified Communications Manager installation. A message displays that the Smart Call Home is not configured during your next login to the Cisco Unified Serviceability console. • **Disabled**: Select this option if you disabled the Smart Call Home functionality during installation. • **Enabled (Smart Call Home)**: Select this option if you selected Smart Call Home option during installation. By default, this option is enabled during Cisco Unified Communications Manager installation. **Note** The values specified during the installation appear in the Cisco Unified Serviceability console. • **Enabled (Anonymous Call Home)**: Select this option if you selected Anonymous Call Home option during Cisco Unified Communications Manager installation. When you select this option, Customer Contact Details is disabled and Send data section is enabled on call home page. The following are the characteristics of Anonymous Call Home: **1** When you select Anonymous Call Home, this option sends the System configuration (hardware/VM, CPU) and Software configuration related information to Cisco Smart Call Home for information-gathering purposes and to make the product better. **2** Anonymous Call Home does not send any user related information (for example, registered devices, upgrade history). **3** Anonymous Call Home does not require any registration or entitlement for the Smart Call Home feature with Cisco. **4** The Unified Communications Manager does not send any diagnostic and configuration information to the Smart Call Home back end. Only inventory and telemetry messages are sent. **5** The periodicity of the messages is the same as that which exists at present for Smart Call Home messages. **6** The Include Verbose Diagnostics in Smart Call Home Alerts option is disabled if the user selects Anonymous Call Home. **Note** The values specified during the installation appear in the Cisco Unified Serviceability console.
Customer Contact Details	
ESW Email Address	
Send Data	

Field Name	Description
Send Data to Cisco Technical Assistance Center (TAC) using	From the drop-down list, select one of the following options to communicate the Call Home messages securely to TAC: • **Secure Web (HTTPS)** - Select this option if you want to send the data to TAC using secure web. • **Email** - Select this option if you want to send the data to TAC using email. For email, the SMTP server must be configured. You can see the IP address of the SMTP server that is configured. **Note** An error message appears if you have not configured the SMTP server. • **Secure Web (HTTPS) through Proxy** - Select this option if you want to send the data to TAC using secure web through proxy. The following fields appear on selecting this option: ◦ **HTTPS Proxy IP/Hostname*** - Enter the proxy IP/Hostname. ◦ **HTTPS Proxy Port*** - Enter the proxy port number to communicate.
Send a copy to the following email addresses (separate multiple addresses with comma)	
Note To enable the Call Home feature, you must select **Send Data to Cisco Technical Assistance Center (TAC)** checkbox.	
Enable Log Collection & Diagnostic Information	Check this check box to activate the Cisco Unified Communications Manager to collect logs and diagnostics information. **Note** This option is active only if the Cisco Unified Communications Manager Call Home service is activated. When you select this check box, and when an alert is generated, the AML alert message contains CLI command output and trace information for debugging.

Procedure changes

Set Up Cisco Unified Communications Manager Publisher Node

Follow this procedure to configure the first server where you install Cisco Unified Communications Manager software as the publisher node for the cluster. Perform this procedure after you have completed the basic installation and configured the basic installation.

Note You can configure Smart Call Home on the publisher node only. For more information on Smart Call Home, refer to Smart call home section in the Cisco Unified Serviceability Administration Guide.

Procedure

Step 1 The **Network Time Protocol Client Configuration** window appears.
Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher node. Subscriber nodes in the cluster will get their time from the first node.

Step 2 Choose whether you want to configure an external NTP server or manually configure the system time.

- To set up an external NTP server, choose Yes and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose Proceed to continue with the installation.

  The system contacts an NTP server and automatically sets the time on the hardware clock.

  Note If the **Test** button appears, you can choose Test to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The **Database Access Security Configuration** window appears.

Step 3 Enter the Security password from Required Installation Information.

Note The Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between nodes, and you must ensure this password is identical on all nodes in the cluster.

The **SMTP Host Configuration** window appears.

Step 4 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name. If you do not want to configure the SMTP server, choose **No**, which redirects to Smart Call Home page. To go to previous page, choose **Back** and to see the information about the SMTP configuration, choose **Help**.

Note You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the platform GUI or the command line interface.

Step 5 Choose **OK**. The **Smart Call Home Enable** window appears.

Step 6 On the Smart Call Home Enable Page, perform one of the following.

a) Select **Enable Smart Call Home on System Start** to enable the Call Home, and then click **OK**. The Smart Call Home Configuration window appears.

   1 Select the method for sending data to the Cisco Technical Assistance Center.

   - Secure Web (HTTPS)
   - Secure Web (HTTPS) through Proxy

     Enter the Hostname/IP Address and port number for Proxy

     - Hostname/IP Address—Enter the IP address or the hostname of the proxy server to send the Call Home messages through an indirect network connection.

        - Port—Enter the port number on which the proxy server is enabled.

    - Email

    Note You must have configured the SMTP for Email to be sent successfully.

2. To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.
3. Enter the email address of the customer in the Customer Contact Details field.
4. Click **Continue** to proceed, or select **Back** to return to the previous menu. If you click **Continue**, a message appears as `Cisco Call Home includes reporting capabilities that allow Cisco to receive diagnostic and system information from your Unified Communications Manager cluster. Cisco may use this information for proactive debugging, product development or marketing purposes. To learn more about this feature, please visit: http://www.cisco.com/en/US/products/ps7334/serv_home.html.`

    Note If you select **Secure Web (HTTPS) through Proxy** and click **Continue**, Smart Call Home Proxy Configuration Page appears.
5. Click **Confirm** to proceeds with normal installation or select **Back** to return to the Smart Call Home Enable Page.

b) Select **Enable Anonymous Call Home on System Start** to enable the Anonymous Call Home, and then click **OK**. The Anonymous Call Home Configuration window appears.

1. Select the method for sending data to the Cisco Technical Assistance Center.
    - Secure Web (HTTPS)
    - Secure Web (HTTPS) through Proxy

      Enter the Hostname/IP Address and port number for Proxy

        - Hostname/IP Address—Enter the IP address or the hostname of the proxy server to send the Call Home messages through an indirect network connection.
        - Port—Enter the port number on which the proxy server is enabled.
    - Email

    Note You must have configured the SMTP for Email to be sent successfully.
2. To send a copy of the Call Home messages to multiple email recipients, enter the email addresses separated with a comma. You can enter up to a maximum of 1024 characters.
3. Click **Continue** to proceed, or select **Back** to return to the previous menu. If you click **Continue**, a message appears as `To help improve the Cisco Unified Communications Manger experience, click Confirm to allow Cisco Systems to securely receive usage statistics from the server. This information will be used by Cisco to help understand how customers are using our product and ultimately drive product direction. If you prefer not to participate, you may choose to opt-out.`

Note If you select **Secure Web (HTTPS) through Proxy** and click **Continue**, Anonymous Call Home Proxy Configuration Page appears.

4 Click **Confirm** to proceeds with normal installation or select **Back** to return to the Smart Call Home Enable Page.

c) Select **Remind me Later to configure Smart Call Home** to configure the Smart Call Home service after installation, using Cisco Unified Serviceability pages.
A reminder message appears in Cisco Unified CM Administration.

```
Smart Call Home is not configured. To configure Smart Call Home or
disable the reminder, please go to Cisco Unified Serviceability > Call
Home.
```

d) Select **Disable All Call Home on System Start** to disable the Smart Call Home service. However, you can activate the Smart Call Home service after installation using Cisco Unified Serviceability pages.

Note You can reconfigure the service in Cisco Unified Serviceability page after installation. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Step 7 Choose **OK**. The Application User Configuration window appears.

Step 8 Enter the Application User name and password from and confirm the password by entering it again.

Step 9 Choose **OK**. The Platform Configuration Confirmation window appears.

Step 10 To continue with the installation, choose **OK**; or to modify the platform configuration, choose **Back**.
The system installs and configures the software. The server reboots.

When the installation process completes, you are prompted to log in by using the Administrator account and password.

Call Secure Status Policy

For Unified Communications Manager, Release 10.0(1) and later, Call Secure Status Policy controls display of secure status icon on phones. The following are the policy options:

- All media except BFCP and iX application streams must be encrypted.

  This is the default value. The security status of the call is not dependent on the encryption status of BFCP and iX application streams.

- All media except iX application streams must be encrypted.

  The security status of the call is not dependent on the encryption status iX application streams.

- All media except BFCP application streams must be encrypted.

  The security status of the call is not dependent on the encryption status BFCP.

- All media in a session must be encrypted.

  The security status of the call is dependent on the encryption status of all the media streams in an established session.

- Only Audio must be encrypted.

  The security status of the call is dependent on the encryption of the audio stream.

Note Changes to the policy affects the display of the secure icon and the playing of a secure tone on the phone.

A new service parameter, Secure Call Icon Display Policy, manages the call secure status policy. It replaces the following service parameters:

- Ignore BFCP Application Line Encryption Status When Designating Call Security Status
- Override Ignore BFCP Application Line Encryption Status When Designating Call Security Status

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Caller-Specific Music On Hold

Cisco Unified Communications Manager can play a different MOH audio source for SIP calls that a phone receives over the SIP trunk, which are then put on hold, depending on the MOH stream IDs that are added to the SIP header for the call. An external application, such as the Cisco Unified Customer Voice Portal (CVP) contact center solution, adds the MOH stream IDs for user and network hold to the SIP header, and then relays that to Cisco Unified Communications Manager over the SIP trunk.

Cisco Unified Communications Manager Administration Considerations

If the incoming SIP call contains MOH audio source information in the SIP header, then Cisco Unified Communications Manager initiates the following actions:

- The MOH audio source is played for the caller when the SIP call is placed on user hold.

- The MOH audio source is played for the caller when the SIP call is placed on network hold.
- The MOH audio source is played for the caller if the call is transferred to another endpoint on the same cluster and subsequently placed on user or network hold.
- When a call is sent on a SIP trunk to another cluster, the MOH audio source information is sent along with the call.
- When a call is sent on a SIP trunk to another cluster in an SME scenario, the MOH audio source information is sent along with the call.
- When a call is transferred to another cluster over a SIP trunk, the MOH audio source information is sent along with the call.
- When a call is either forwarded or redirected to another cluster over a SIP trunk, the MOH audio source information is sent along with the call.

Limitations

- If the user and network MOH audio source identifiers are not provisioned, or if one or both values are invalid, the caller-specific MOH information in the SIP header is ignored. The call reverts to tone on hold and an invalid MOH audio source alarm is raised.
- When both the user and network MOH audio source identifiers are present in the header, any invalid value is replaced by the default value (0).
- If both values are 0, or the only value is 0, the header in the incoming INVITE is ignored.
- If only one MOH audio source identifier is provided in the SIP header, including if a comma appears before or after the MOH audio source identifier value, the same MOH ID is used for both user and network MOH. The SIP trunk populates both the user and the network MOH audio source identifiers in the SIP header so that Call Control always receive both values.
- If there are more than two MOH audio source identifier values separated by a comma in the header, then the first two values are used. Subsequent values are ignored.
- Administrators are responsible to maintain consistent caller-specific MOH configurations when multiple Cisco Unified Communications Manager clusters are involved.
- The original incoming caller to the call center cannot change during the course of the entire call.
- The music on hold information is only shared across SIP trunks.
- Caller-specific MOH is not supported when calls are received or transferred over QSIG tunneling-enabled SIP trunks.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Additional Information

Three new alarms are added for caller-specific Music On Hold:

- OutOfRangeMohAudioSource
- UnableToOpenMohAudioSource
- UnprovisionedMohAudioSource

Certificate Revocation Check

For Cisco Unified Communications Manager, Release 10.0(1), you can configure certification revocation check to be performed on a periodic basis. Certificate revocation check is performed on all certificates and trust chains associated with a established long session. The check is performed for the following sessions:

- CTI connections with JTAPI /TAPI applications
- LDAP connection between Cisco Unified Communications Manager and SunOne servers
- IPsec connections

The check terminates established sessions when the certificate or trust chain status is revoked, not trusted or expired.

The enterprise parameter **Certificate Revocation and Expiry** allows you to control the certificate validation checks. The certificate service frequently checks for long sessions between Cisco Unified Communications Manager and other services. The certificate expiry for the long sessions is not verified when the **Certificate Revocation and Expiry** parameter value is disabled.

Choosing **Enable Revocation**on the Operating System Administration of Cisco Unified Communications Manager activates the certificate revocation service for LDAP and IPsec connections. **Check Every** value determines the frequency of the check. If the **Enable Revocation** check box is unchecked then the revocation check for the certificate is not performed.

The following fields are added to the **Certificate Revocation** window (**Security** > **Certificate Revocation**) in Cisco Unified Operating System Administration interface:

Enable Revocation Check

Check this check box to perform frequent certificate revocation check.

Check Every

Enter the frequency value for the certificate revocation check.

Cisco Unified Communications Manager Administration Considerations

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Cisco AXL Web Service Enabled by Default

With Release 10.0(1), Cisco AXL Web Service is now enabled by default on all cluster nodes following installation. Cisco recommends that you always leave the service activated on the publisher node to ensure that you are able to configure products that are dependent on AXL, such as Unified Provisioning Manager.

Based on your needs, you can start or stop the service on specific subscriber nodes in Cisco Unified Serviceability under Feature Services.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

Following installation, Cisco AXL Web Service is now enabled by default on all cluster nodes.

Cisco IP Voice Media Streaming Application Service Supports IPv6 Audio Media Connections

The Media Termination Point (MTP) device, software conference bridge, annunciator, and unicast Music On Hold provided by the Cisco IP Voice Media Streaming Application service support both IPv4 and IPv6 audio media connections. The MTP device, software conference bridge, annunciator, and unicast Music On Hold are configured automatically in dual mode when the platform is configured for IPv6 and the IPv6 enterprise parameter is enabled. If the platform is not configured for IPv6, the MTP device, software conference bridge, annunciator, and unicast Music On Hold are configured automatically in IPv4 only mode.

The MTP device, software conference bridge, annunciator and Music On Hold support only IPv4 for the TCP control channel. The annunciator, Music On Hold, and MTP in pass-through mode support secure media SRTP connections to both IPv4 and IPv6 addresses.

Note Multicast Music On Hold supports only IPv4.

Note Both Cisco IOS Enhanced MTP and the software MTP provided by the Cisco IP Voice Media Streaming Application support IPv4 to IPv6 translation. Both Cisco IOS Enhanced MTP and the software MTP provided by the Cisco IP Voice Media Streaming Application support media interoperation between IPv4 and IPv6 networks and operate in dual mode. For information on how Cisco Unified Communications Manager (Unified Communications Manager) inserts MTPs into calls that require IPv4 to IPv6 translation, see *Cisco Unified Communications Manager Features and Services Guide*. For information on how to configure your Cisco IOS MTP so that the MTP can support IP translation, see *Implementing VoIP for IPv6*.

Conferences

Unified Communications Manager supports dual mode for the software conference bridge provided by the Cisco IP Voice Media Streaming Application. During a conference, if an endpoint supports IPv4 only, IPv4 media is negotiated between the endpoint and the conference bridge. Whereas, if the endpoint supports IPv6 only, IPv6 media is negotiated between the endpoint and the conference bridge. If dual mode is supported by the SCCP endpoint, the media preference configured in the enterprise parameter (IPv4 or IPv6) is negotiated between the endpoint and the conference bridge. If dual mode with ANAT is supported by the SIP device, the ANAT address preference advertised by the SIP device is negotiated between the SIP device and the conference bridge. For conferences using the software conference bridge, Unified Communications Manager does not insert an MTP for IPv4 to IPv6 translation because the software conference bridge supports dual mode conferences.

If an MTP is inserted in a conference, for it to support security you must configure the MTP in pass-through mode, which means that the MTP does not transform the media payload during the call. When you configure an MTP in pass-through mode, the MTP receives the encrypted packet on one call leg and sends out the same packet on a different leg of the call. For secure conferences with secure conference bridges that do not support dual mode and encrypted devices with an IP Addressing Mode of IPv6 Only, Unified Communications Manager inserts an MTP into the conference to translate IPv4 to IPv6 (and vice versa). If you configure the MTP for pass-through mode, the encrypted IPv6 phones communicate with the conference bridge using SRTP. If you do not configure the MTP for pass-through mode, the media gets downgraded to RTP.

Music On Hold

The Cisco IP Voice Media Streaming Application, which is a component of Music On Hold, supports both IPv4 and IPv6 audio media connections for unicast Music On Hold. Multicast Music On Hold supports IPv4 only. So, devices with an IP Addressing Mode of IPv6 Only cannot support multicast Music On Hold. Under these circumstances, Unified Communications Manager plays a tone, instead of music, when the phone is on hold. However, devices with an IP Addressing Mode of IPv6 only can stream unicast Music On Hold without Unified Communications Manager inserting an MTP for IPv4 to IPv6 conversion.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications applications from the perspective of migration, fresh installs, upgrades, switching versions, rebooting clusters, and changing IP addresses or hostnames. Cisco Prime Collaboration Deployment replaces the Platform Administrative Web Services Interface Management (PAWS-M) application introduced in Release 9.0(1).

Cisco Prime Collaboration Deployment has two primary, high-level functions:

- Migrate old clusters (Release 6.1 or higher) to new clusters (this may be MCS to virtual, or virtual to virtual)
- Perform operations on existing clusters (Release 8.6(1) or later). Examples of these operations include:
    - Upgrade
    - Switch Version
    - Restart

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

CLI Changes

In order to support upgrade and migration, the Refresh Upgrade framework is being used for export the data from the old system and import the data to the new virtual system. In a system where export operation is not supported by default, the user needs to install a Cisco Options Package (COP) file which will install required files and make changes to the command-line interface (CLI).

Three CLI commands are added when the COP file is installed:

- utils system dataexport initiate
- utils system dataexport cancel
- utils system dataexport status

The utils system dataexport initiate command can be used for initiating the export operation. The user is prompted for the SFTP server details. After the export starts, the command is executed in the back end and the CLI returns.

Cisco Prime Collaboration Deployment simplifies the hostname and IP address change procedures. Hostname change refers to the changing of a server network hostname identity, an IP address, or both. Historically, changing a server hostname involved a series of steps that required the use of the CLI and web graphical user interface (GUI). It also required the user to reboot single servers and whole clusters after the event.

All the existing steps in the procedure “Changing the IP Address and Hostname for Cisco Unified Communications Manager” are automated into a single step using the CLI or GUI. The single-step includes a readiness and post-task list for user verification.

Also new as part of Cisco Prime Collaboration Deployment is the enhancement of the "set network hostname" CLI command. The interface now prompts the user for an IP, mask, and gateway value.

Procedure Changes

- Procedures for “Changing the IP Address and Hostname for Cisco Unified Communications Manager” are affected (see CLI changes above). Cisco Prime Collaboration Deployment is used to simplify and automate IP address and hostname changes across the cluster as part of a software upgrade, server migration, or re-numbering on a Release 10.0 (or higher) system.
- New procedures have been created for migrating data from an existing Cisco Unified Communications Manager node to a new machine. This operation was previously done using the Bridge Upgrade procedure. These steps can be done automatically, using the Cisco Prime Collaboration Deployment application (a new document, *Cisco Prime Collaboration Deployment Administration Guide*, will be delivered for Release 10.0(1)).

Cisco Prime License Manager

As of Release 10.0(1),Cisco Prime License Manager replaces Enterprise License Manager.Cisco Prime License Manager provides simplified, enterprise-wide management of user-based licensing, including license fulfillment. Cisco Prime License Manager handles licensing fulfillment, supports allocation and reconciliation of licenses across supported products, and provides enterprise-level reporting of usage and entitlement.

Important Cisco Prime License Manager is not installable as a standalone option from the Unified Communications operating system ISO. Co-resident installation from the Unified Communications operating system ISO is still an option.

Note You have the ability to define how to manage licensing of your enterprise. You can have one Cisco Prime License Manager for the entire enterprise, or you can have several Cisco Prime License Managers and divide the enterprise in a manner that best suits your needs.

Cisco Prime License Manager runs on a virtual machine or may co-reside on a product's virtual machine if that product supports co-resident deployment.

For more information on Cisco Prime License Manager, see the *Cisco Prime License Manager User Guide, Release 10.0(1).*

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

CLI changes

license management service

This command activates or deactivates a given service on the Cisco Prime License Manager server.

license management service {**activate**| **deactivate**}

Syntax Description

Parameters	Description
activate	Activates a given service on the Cisco Prime License Manager server.

Parameters	Description
deactivate	Deactivates a given service on the Cisco Prime License Manager server.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Enterprise License Manager, Cisco Prime License Manager

license management show system

This command lists the administrative users.

license management show system

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Enterprise License Manager, Cisco Prime License Manager

Cisco TelePresence Video Conferencing Resources

Cisco Unified Communications Manager supports new video conference bridge resources and changes to the setup as follows:

1. Cisco TelePresence Conductor
2. Conference bridge resource setup changes:
    - Configure and assign a SIP trunk.
    - Assign the encryption interworking script to SIP trunks that are used for Cisco TelePresence Conductor if encryption is used.

Cisco Unified Communications Manager Administration Considerations

See Additional Information section for details.

Bulk Administration Considerations

Unavailable.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Additional Information

Cisco TelePresence MCU Settings

Cisco TelePresence MCU refers to a set of hardware conference bridges for Cisco Unified Communications Manager.

The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full trans-coding, and is ideal for mixed HD endpoint environments.

The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.

Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco TelePresence MCU configuration settings.

The following table describes the Cisco TelePresence MCU configuration settings.

Table 6: Cisco TelePresence MCU Configuration Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge

Field	Description
Destination Address	Enter the IP Address of the Cisco TelePresence MCU conference bridge
Description	Enter a description for your conference bridge
Device Pool	Choose a device pool or choose Default.
Common Device Configuration	Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.
Location	Use location to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list box, choose the appropriate location for this conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the **System** > **Location** menu option. For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Field	Description
Use Trusted Relay Point	From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates. • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
SIP Interface Info	
MCU Conference Bridge SIP Port	This is the SIP listening port of the Cisco TelePresence MCU Conference Bridge. The default value is 5060.
SIP Profile	From the drop-down list box, choose **Standard SIP Profile for TelePresence Conferencing**.

Field	Description
SIP Trunk Security Profile	From the drop-down list box, choose the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks. Cisco Unified Communications Manager provides a default nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. To identify the settings that each profile contains, choose **System** > **Security Profile** > **SIP Trunk Security Profile**. If you are using SRTP with Cisco TelePresence MCU, the SIP trunk security profile must use the following settings: • Device Security Mode must be Encrypted • Incoming Transport Type and Outgoing Transport Type must be TLS • X.509 Subject Name must be set to the defined Common Name used in the Cisco TelePresence MCU certificates For information on how to configure security profiles, see the Cisco Unified Communications Manager Security Guide.
SRTP Allowed	Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls with Cisco TelePresence MCU. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the Cisco TelePresence MCU and uses RTP instead. For more information on encryption, see the *Cisco Unified Communications Manager Security Guide*. **Note** When this check box is checked, the vcs-interop script is selected by default in the Script drop-down list box and the Enable Trace check box is checked. **Note** If you check this check box, you must configure TLS so that you do not expose keys and other security-related information during call negotiations.
Normalization Script info	
Script	From the drop-down list box, choose the script that you want to apply to the Cisco TelePresence MCU. To import another script, go to the SIP Normalization Script Configuration window (**Device** > **Device Settings** > **SIP Normalization Script**), and import a new script file.
Enable Trace	Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces an SDI trace. **Note** Cisco recommends that you enable tracing only while debugging a script. Tracing has an impact on performance and should not be enabled under normal operating conditions.

Field	Description

Parameter Name/Parameter Value	Optionally, enter parameter names and parameter values. Valid values include all characters except equal signs (=), semicolons (;), and nonprintable characters, such as tabs. You can enter a parameter name with no value.
	`Example`
	`Parameter Name Parameter Value`
	`CCA-ID 11223344`
	`pbx`
	`location RTP`
	You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values.
	To add another parameter line, click the + (Plus) button. To delete a parameter line, click the – (Minus) button.

HTTP Interface Info	
Username	Enter the Cisco TelePresence MCU administrator username.
Password	Enter the Cisco TelePresence MCU administrator password.
Confirm Password	Enter the Cisco TelePresence MCU administrator password
HTTP Port	Enter the Cisco TelePresence MCU HTTP port. The default port is 80.
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU. The default HTTPS port is 443. For information on how to create a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU, see the Set up a TLS connection with Cisco TelePresence MCU section.

Note The HTTP configuration must match what is configured on the Cisco TelePresence MCU. This information allows Cisco Unified Communications Manager to invoke the remote management API on the Cisco TelePresence MCU.

Cisco TelePresence Conductor Settings

Cisco TelePresence Conductor provides intelligent conference administrative controls and is scalable, supporting device clustering for load balancing across MCUs and multiple device availability. Administrators can implement the Cisco TelePresence Conductor as either an appliance or a virtualized application on VMware with support for Cisco Unified Computing System (Cisco UCS) platforms or third-party-based platforms. Multiway conferencing, that allows for dynamic two-way to three-way conferencing, is also supported.

Cisco TelePresence Conductor supports both ad hoc and meet-me voice and video conferencing. Cisco TelePresence Conductor dynamically selects the most appropriate Cisco TelePresence resource for each new conference. Ad hoc, "MeetMe" and scheduled voice and video conferences can dynamically grow and exceed the capacity of individual MCUs. One Cisco TelePresence Conductor appliance or Cisco TelePresence Conductor cluster has a system capacity of 30 MCUs or 2400 MCU ports. Up to three Cisco TelePresence Conductor appliances or virtualized applications may be clustered to provide greater resilience.

Cisco TelePresence Conductor also provides the XML management API over HTTP, and has a built-in Web Server for complete configuration, control and monitoring of the system and conferences. For more information, see the *Cisco TelePresence Conductor Administrator Guide* and the *Cisco Unified Communications Manager System Guide*.

Note If you are using encryption with Cisco TelePresence Conductor, select cisco-telepresence-conductor-interop as the default normalization script.

The following table describes the Cisco TelePresence Conductor configuration settings.

Table 7: Cisco TelePresence Conductor Configuration Settings

Field	Description
Conference Bridge Name	Enter a name for your conference bridge.
Description	Enter a description for your conference bridge.
Conference Bridge Prefix	The Conference Bridge Prefix is used only for centralized deployments when the conference resources are deployed across a Small Medium Enterprise (SME) and the HTTP and SIP signaling are intended for different destinations. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
SIP Trunk	Select a SIP trunk to use for this conference bridge from a list of existing SIP trunks.
HTTP Interface Info	
Override SIP Trunk Destination	Check this check box to override the SIP trunk destination. Use this feature if the HTTP and SIP signaling are intended for different destination IP addresses, for example, when the device is used in a centralized deployment. Click the "+" and "-" buttons to add or remove IP addresses and hostnames. Do not set this parameter unless your video conference device supports this function. See the documentation that came with your conference bridge device for details.
Hostname/IP Address	Enter one or more hostnames or IP addresses for the HTTP signaling destination if you have selected to override the SIP trunk destination.
Username	Enter the Cisco TelePresence Conductor administrator username.

Field	Description
Password	Enter the Cisco TelePresence Conductor administrator password.
Confirm Password	Enter the Cisco TelePresence Conductor administrator password
Use HTTPS	Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence Conductor. The default HTTPS port is 443.
HTTP Port	Enter the Cisco TelePresence Conductor HTTP port. The default port is 80.

SIP Trunk Setup for Video Conference Bridge Devices

The following video conference bridge devices use SIP trunks for video conferences on Cisco Unified Communications Manager clusters:

- Cisco TelePresence MCU
- Cisco TelePresence Conductor

Set the following SIP trunk parameters for use with SIP video conference bridge devices. Use the default setting for all other SIP trunk parameters.

- Device Name
- Description
- Device Pool
- Location
- Destination Address
- Destination Port

Note Multiple IP addresses and ports can be specified.

- SIP Trunk Security Profile: You must select TelePresence Conference as the SIP trunk security profile.
- SIP Profile

Note For improved performance, use the default standard SIP profile for TelePresence conferencing that has the Options ping configured.

- Assign the encryption interworking script to SIP trunks that are used for Cisco TelePresence Conductor if encryption is used.

See topics related to setting up trunks for more details about SIP trunk configuration.

Limitations

- Media Termination Point (MTP) Required: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP trunk.
- Early Offer Support for Voice and Video calls: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls even if this is selected on the SIP profile that is associated with the SIP trunk that is linked to the conferencing resource server.
- SIP Rel1xx Option: Cisco Unified Communications Manager ignores this configuration for ad hoc conference calls even if this is enabled on the SIP profile associated with the SIP trunk that is linked to the conferencing resource server.
- RSVP over SIP: Cisco Unified Communications Manager ignores this configuration for all ad hoc conference calls if this is enabled for E2E. If this is configured for local RSVP, the configuration will be effective.

Procedure changes

Set Up TelePresence Video Conference Bridge

Use Cisco Unified Communications Manager Administration to add and configure a video conference bridge device. Each video conference bridge device must be assigned to a SIP trunk when you configure the video conference device for the node.

Before You Begin

Set up a SIP trunk before you proceed. See topics related to trunk setup and SIP trunk setup for video conference bridge devices for details.

Procedure

Step 1 Select **Media Resources** > **Conference Bridge**.
The **Find and List Conference Bridges** window displays.

Step 2 Click **Add New**. The **Conference Bridge Configuration** window displays.

Step 3 Select the type of SIP video conference bridge device from the **Conference Bridge Type** drop-down list.

Step 4 Enter a name and description for the video conference bridge device in the **Device Information** pane.

Note For field descriptions, see topics related to configuration settings for the selected video conference bridge type.

Step 5 Select a SIP trunk from the **SIP Trunk** drop-down list.

Step 6 Enter the following mandatory information HTTP interface username, password, and confirm the password in the **HTTP Interface Info** pane.

- Username
- Password
- Confirm Password
- HTTP Port

Step 7 (Optional) Check the **Use HTTPS** check box.

Step 8 Click **Save**.

Cisco User Data Services

Cisco User Data Services provides Cisco Unified IP Phones with the ability to access user data from the Cisco Unified Communications Manager database. With Release 10.0(1), Cisco Personal Directory (CCMPD) and Cisco CallManager Cisco IP Phone (CCMCIP) services are supported through Cisco User Data Services. If you disable Cisco User Data Services, the Directory button on Cisco Unified IP Phones will be disabled and your phones will not be able to use Cisco IP Phone services.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

Cisco User Data Services must be activated from Cisco Unified Serviceability. From Cisco Unified Serviceability, choose **Tools** > **Control Center - Network Services**. Under CM Services, click the **Cisco User Data Services** radio button and click **Start.**

With Release 10.0(1), Cisco User Data Services supports Cisco Personal Directory and Cisco IP Phone services. If you disable Cisco User Data Services, the Directory button on Cisco Unified IP Phones will be disabled and your phones will not be able to use Cisco IP Phone services.

CMC and FAC For Mobility Originated Calls

Mobile phones with Cisco Jabber installed support Client Matter Codes (CMC) and Forced Authorization Codes (FAC). The FAC and CMC are localized for Cisco Mobility.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Commercial Cost Avoidance

If a caller within a Cisco Unified Communications Manager (Unified Communications Manager) network calls a called party on an external number, Unified Communications Manager checks if an internal number exists for the called party in the LDAP database. If an internal number exists, the call is routed to the internal number. If the internal number is not found in the LDAP database, the call is routed to the original (external) number.

Cisco Unified Communications Manager Administration Considerations

To route the calls to the internal numbers, you must configure directory number alias for both the lookup and the sync servers. You must configure the LDAP server for Directory Number Alias Sync (sync server) to synchronize users from Unified Communications Manager database to the sync server. You must configure the LDAP server for Directory Number Alias Lookup (lookup server) to route the commercial calls to an alternate number.

In Cisco Unified Communications Manager Administration, use the submenus under the **Advanced Features** > **Directory Number Alias Lookup/Sync** menu path to configure directory number alias lookup and sync servers. .

The following table describes the Directory Number Alias Lookup/Sync settings.

Table 8: Directory Number Alias Lookup/Sync Settings

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Reenter the password that you provided in the LDAP Password field.
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.
LDAP Directory Server Usage	Specify if the LDAP directory server should be used as: • Directory Number Alias Sync and Lookup • Directory Number Alias Sync Only • Directory Number Alias Lookup Only By default, the Directory Number Alias Sync and Lookup option is selected. If you choose the *Directory Number Alias Sync and Lookup* option, you cannot add another sync or lookup server.
Directory Number Alias Server Configuration	
Keepalive Search User Distinguished Name	Enter the user ID (up to 128 characters) of the administrative user for which you need to perform the keepalive search.
Keepalive Time Interval in Minutes	Specify the time interval at which keepalive messages should be sent to lookup/sync servers to check if those servers are active or not. For example, if you specify the keepalive time interval as 10 minutes and select the LDAP directory server as *DN Alias Lookup only*, keepalive messages will be sent every 10 minutes to all the lookup servers that are configured.

Field	Description
Enable Caching of Records for Directory Number Alias Lookup	Check this check box to enable caching of records for directory number alias lookup. If you check this check box, you can specify Record Cache Size for Directory Number Lookup Alias and Record Cache Age for Directory Number Alias Lookup in Hours. **Note** If you specify the LDAP directory server as a sync server, the system disables this check box. This field is enabled only if the Lookup server or both (Lookup and Sync) the servers are used as LDAP directory servers. If the Sync server is used as LDAP directory server, this field is disabled.
Record Cache Size for Directory Number Alias Lookup	Specify the number of records that should be cached. You can specify any number within a range of 3000-10000. **Note** This field is enabled only if 'Enable Caching of Records for Directory Number Alias Lookup' check box is checked.
Record Cache Age for Directory Number Alias Lookup in Hours	Specify the time for which the records should be held in the record cache. **Note** This field is enabled only if 'Enable Caching of Records for Directory Number Alias Lookup' check box is checked.
LDAP Server Information	
Host Name or IP Address for Server	Enter the hostname or IP address of the server where the data for this LDAP directory resides.

Field	Description
Port	Enter the port number on which the LDAP routing database receives the LDAP requests. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. How your LDAP routing database is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers: LDAP Port when LDAP server is not a Global Catalog server: • 389: When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.) • 636: When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) LDAP Port when LDAP server Is a Global Catalog server: • 3268: When SSL is not required. • 3269: When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) **Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.
Add Another Redundant LDAP Server	Click this button to add a redundant LDAP server.

Note To enable routing the commercial calls to the internal numbers of the called parties, ensure that Cisco Directory Number Alias Lookup Service is activated. To synchronize users from the Unified Communications Manager database to the LDAP server for Directory Number Alias Sync server, ensure that Cisco Directory Number Alias Sync Service is activated.

Note You can configure the primary and secondary lookup and sync servers to support failover. If a primary server goes down and if the secondary server is configured, lookup/sync services automatically connect to the secondary server. The failover is supported for both lookup and sync services. When the primary server is restored, the network administrator must restart the lookup/sync service so that the services can connect back to the primary server.

Note A commercial call is routed to an internal number only if Confidential Access Level (CAL) resolution succeeds on that call. If the CAL resolution fails, the call is redirected to the original destination.

Call Control Agent Profile Configuration—This menu path has been added to enable you to configure the call control agent profile settings.

The following table describes the Call Control Agent Profile settings.

Table 9: Call Control Agent Profile Settings

Field	Description
Call Control Agent Profile Configuration	
Call Control Agent Profile ID	Enter the Call Control Agent Profile ID.
Primary Softswitch ID	Enter the primary softswitch ID.
Secondary Softswitch ID	Enter the secondary softswitch ID.
Object Class	Enter the object class name to be synchronized to the external directory server.
Subscriber Type	Enter the subscriber type.
SIP Alias Suffix	Enter the SIP alias suffix. The E.164 number that you specify for the directory number is appended to this suffix.
SIP User Name Suffix	Enter the SIP user name suffix.

A new field **Call Control Agent Profile** has been added to the Directory Number Configuration window (**Call Routing** > **Directory Number**). You can select the Call Control Agent Profile to associate to the directory number.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

The following services have been added in the Control Center - Feature Services window (**Tools** > **Control Center - Feature Services**):

- Cisco Directory Number Alias Sync
- Cisco Directory Number Alias Lookup

Procedure changes

Configure Directory Number to Synchronize to LDAP Directory Server

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Call Routing** > **Directory Number**.

Step 2 Perform one of the following:

- Select **Add New** to create a new directory number.
- Open an existing directory number entry.

Step 3 Enter an E.164 mask.

Step 4 Enter an enterprise alternative number (EAN).

Step 5 Select a Call Control Agent Profile from the drop-down list box to create a new Call Control Agent Profile.

What to Do Next

Configure the LDAP server for Directory Number Alias Sync (sync server) if you need to synchronize directory numbers from the Unified Communications Manager database to the sync server.

Common Cluster Topology

IM and Presence Service administration functions have been integrated into the Cisco Unified Communications Manager Administration. Common cluster topology is one of two main areas of this integration, the other being common user management which is documented separately.

Components of the common topology integration for this release include:

- Add/edit IM and Presence Service nodes
- Add/edit presence redundancy groups and high availability
- IM and Presence Service node information and status
- IM and Presence Service user assignments and status
- Select cluster node type (Unified CM or IM and Presence)
- Unified CM Cluster overview report

Cisco Unified Communications Manager Administration Considerations

The following new functions are accessible using Cisco Unified Communications Manager Administration. For more information and detailed procedures, see the *Cisco Unified Communications Manager Administration Guide* and the *Cisco Unified Communications Manager Features and Services Guide*.

- IM and Presence Service node setup and status

Note To install the IM and Presence Service node, see *Installing Cisco Unified Communications Manager*.

- High Availability and presence redundancy group setup
- Manual failover, fallback, and recovery
- Balancing user and server assignments
- End user setup for IM and Presence Service

Bulk Administration Considerations

A new field to assign an end user to an IM and Presence Service node is added to the BAT update users and the BAT user template field descriptions tables.

Assigned Presence Server	Assign the end user to an IM and Presence Service node that is installed in the cluster if the system is non-balanced. The server you specify using the Bulk Administration Tool must be part of a Presence Redundancy Group. For clusters that have the user assignment mode for the IM and Presence Service node set to balanced or active-standby, user assignments that are made using the Bulk Administration Tool override the automatic user assignments.

CDR/CAR Considerations

The IM and Presence Cluster Overview report information is included in the Unified CM Cluster Overview report. The IM and Presence Cluster Overview report is no longer available as a separate report.

If you are prompted to re-login when you select an IM and Presence Service report, re-enter your Cisco Unified Communications Manager Administration Administration login credentials

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

IM and Presence Service Considerations

You can no longer create presence redundancy groups or add users to presence redundancy groups on IM and Presence Service using the Cisco Unified CM IM and Presence Administration GUI. Presence Topology, which was renamed from Cluster Topology, now provides a read-only view of topology settings.

CLI changes

utils ha fallback

This command initiates a manual fallback for a specified node, where the Cisco Server Recovery Manager restarts the critical services on the active node and moves users back to the active node.

utils ha fallback *node name*

Syntax Description

Parameters	Description
node name	Specifies the node on which to perform a manual fallback.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Fallback Example

```
admin: ha fallback shorty-cups
Initiate Manual fallback for Node >shorty-cups<
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Falling Back Reason: On Admin Request
Node 2 Name : shorty-cups State: Taking Back Reason: On Admin Request
```

utils ha failover

This command initiates a manual failover for a specified node, where the Cisco Server Recovery Manager stops the critical services on the failed node and moves all users to the backup node.

For IM and Presence nodes, the backup node must be another IM and Presence server. Two servers must be assigned to the same presence redundancy group before you specify the backup server. The back-up server you specify is the other server that is assigned to the presence redundancy group.

utils ha failover {**node name**}

Syntax Description

Parameters	Description
node name	Specifies the node on which to perform the manual failover.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Failover Example

```
admin: ha failover shorty-cups
Initiate Manual Failover for Node > shorty-cups
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Taking Over Reason: On Admin Request
Node 2 Name : shorty-cups State: Failover Reason: On Admin Request
```

utils ha recover

This command initiates a manual recovery of the presence redundancy group (when nodes are in a Failed state), where IM and Presence restarts the Cisco Server Recovery Manager service in that presence redundancy group.

utils ha recover *presence redundancy group name*

Syntax Description

Parameters	Description
presence redundancy group name	Specifies the presence redundancy group on which to monitor HA status. If no presence redundancy group name is provided, all cluster information is provided.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Recover Example

```
admin: ha recover Defaultcluster
Stopping services... Stopped
Starting services... Started
admin:
```

utils ha status

This command displays the HA status for a specified presence redundancy group.

utils ha status *presence redundancy group name*

Syntax Description

Parameters	Description
presence redundancy group name	Specifies the presence redundancy group for which to monitor HA status. If no presence redundancy group name is provided, all cluster information is displayed.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Status Example with HA Not Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Unknown Reason: High Availability Not Enabled
Node 2 Name : shorty-cups State: Unknown Reason: High Availability Not Enabled
```

Status Example with HA Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Normal
Node 2 Name : shorty-cups State: Normal
```

Status Example with a Critical Service Down

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Over with Critical Services not Running Reason:
Critical Service Down
Node 2 Name : shorty-cups State: Running in Backup Mode Reason: Critical Service Down
```

Status Example Failed

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Reason: Critical Service Down
Node 2 Name : shorty-cups State: Failed Reason: Critical Service Down
```

Common Serviceability

Cisco Unified Communications Manager (Unified Communications Manager), Release 10.0(1) provides a common serviceability for Unified Communications Manager and IM and Presence nodes in a mixed cluster setup. The following modules have been integrated to give you a unified administration and reporting experience:

- Cisco Unified Serviceability
- Cisco Unified Real-Time Monitoring Tool (RTMT)
- Alert Manager and Controller Service (AMC)

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

The following changes have been made in the RTMT interface:

- A new IM and Presence drawer has been added, which displays information on only IM and Presence nodes.

- The CallManager drawer has been renamed as Voice/Video. It displays information on only voice or video nodes.
- System Drawer - The System Drawer has the following changes:
    - You can view the summary for all the nodes in the extended cluster (Voice/Video or IM and Presence) on the System Summary screen.
    - You can view information for all the nodes in the extended cluster (Voice/Video or IM and Presence) for CPU and Memory, Process, and Disk Usage.
    - You can view performance information from all nodes in the extended cluster (Voice/Video or IM and Presence). The applicable counters will be displayed based on the type of node that you select.
    - You can view alerts for the system for all nodes in the extended cluster.
    - You can view real-time trace and monitor use events for all the nodes in the extended cluster.
    - You can display audit logs from all nodes in the extended cluster.

Security Considerations

No changes.

Serviceability Considerations

The following changes have been made in the Cisco Unified Serviceability interface:

- Alarm Configuration - The Alarm Configuration (**Alarm** > **Configuration**) screen allows you to configure alarms for both Cisco Unified Communication Manager and IM and Presence servers.
- Alarm Definition - The Alarm Definition (**Alarm** > **Definition**) screen allows you to view alarm definitions for Cisco Unified Communication Manager and IM and Presence servers.
- Trace Configuration - The Trace Configuration (**Trace** > **Configuration**) screen allows you to configure trace for Cisco Unified Communication Manager and IM and Presence servers.
- Troubleshooting Trace Settings - The Troubleshooting Trace Settings (**Trace** > **Troubleshooting Trace Settings**) screen allows you to troubleshoot trace settings for Cisco Unified Communication Manager and IM and Presence servers.
- Service Activation - The Service Activation (**Tools** > **Services**) screen allows you to activate, deactivate, start, and stop Cisco Unified Communications Manager and IM and Presence services.
- Feature Services - The Feature Services (**Tools** > **Control Center - Feature Services**) screen allows you to activate, deactivate, start, and stop Cisco Unified Communications Manager and IM and Presence feature services.
- Network Services - The Network Services (**Tools** > **Control Center - Network Services**) screen allows you to activate, deactivate, start, and stop Cisco Unified Communications Manager and IM and Presence network services.

Common User Management

The following user management enhancements are added for IM and Presence Service on Cisco Unified Communications Manager (Unified Communications Manager):

- End user meeting and calendar information can be included in IM and Presence Service.
- Presence Viewer allows users to view the availability of their watchers and contacts, as well as access information about their current presence server assignment.
- IM and Presence Service roles are added to Unified Communications Manager.

Cisco Unified Communications Manager Administration Considerations

Calendar and Meeting Information Inclusion

You can enable the inclusion of end user meeting and calendar information in IM and Presence Service from either the End User Configuration or the Feature Group Template Configuration windows in Unified Communications Manager Administration. The following conditions must be met to enable this feature:

- The end user must be on the home cluster and have IM and Presence Service enabled.
- An Exchange Presence Gateway must be configured on the Cisco Unified Communications Manager IM and Presence Service server.

IM and Presence Service Roles

The following IM and Presence Service roles have been added to Unified Communications Manager

Table 10: IM and Presence Service Roles

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CCMADMIN Administration	Cisco Call Manager IM and Presence Administration	Allows an administrator access to all aspects of the CCMAdmin system	
Standard CCMADMIN Read Only	Cisco Call Manager IM and Presence Administration	Allows read access to all CCMAdmin resources	
Standard CUReporting	Cisco Call Manager IM and Presence Reporting	Allows application users to generate reports from various sources	

Bulk Administration Considerations

You can enable the inclusion of end user meeting and calendar information in IM and Presence Service using the Bulk Administration Tool in the BAT user template and in the User update settings. The user must be on the home cluster and have IM and Presence Service enabled. Also ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server.

CDR/CAR Considerations

Tip When generating a new report for IM and Presence Service, reenter your Cisco Unified Communications Manager Administration login credentials if you are prompted to log in again when you select an IM and Presence Service report to view.

The following reports have been added for IM and Presence Service:

Table 11: IM and Presence Service Reports

Report	Description
Presence Configuration Report	Provides configuration information about IM and Presence Service users. • Users that are synced from Cisco Unified Communications Manager • Users that are enabled for IM and Presence Service • Users that are enabled for Microsoft remote call control • Users that are enabled for calendaring information in IM and Presence Service Click **ViewDetails** to see the list of users in sortable columns.
Presence Usage Report	Provides usage information for logged-in XMPP clients and third-party APIs. Click **ViewDetails** to see the list of XMPP clients and third-party APIs in sortable columns.
Presence Limits Warning Report	Provides information about users that have met or exceeded the configuration limits for the maximum number of contacts or watchers. Click **ViewDetails** to see the list of users in sortable columns.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Additional information

Presence Viewer for End Users

Use the Presence Viewer to view the availability status of a user in IM and Presence Service, and to view the list of contacts and watchers that are configured for that user.

Access the Presence Viewer from an end-user configuration record using Cisco Unified Communications Manager Administration when IM and Presence Service is enabled for that user. For more information, see topics related to enablingIM and Presence Service for a user.

The user must be assigned to an IM and Presence Service node for valid presence information to be available. The AXL, Presence Engine, and Proxy Service must all be running on the IM and Presence Service node for this feature to be functional.

The following table lists the fields that are displayed on the Presence Viewer for the selected end user in Cisco Unified Communications Manager Administration.

Table 12: End User Presence Viewer Fields

Configuration/Availability Information	
User Status	Identifies the availability state of the user, including: • Available • Away • Do Not Disturb • Unavailable • Custom
User ID	Identifies the selected user ID. A user photo is displayed if one is available for that user. You can click **Submit** to choose a different User ID.
View From Perspective of	Specifies a user to see the availability status from the perspective of the user. This allows you to determine how the availability status of a specified user appears to another user, known as a watcher. This functionality is useful in debugging scenarios, for example, where a user has configured privacy policies. A maximum of 128 characters is allowed.

Configuration/Availability Information	
Contacts	Displays the number of contacts in the contact list for this user. Click the arrow beside the Contacts heading in the Contacts and Watchers list area to view the availability status of a specific user contact. Click the arrow beside the group name to expand the list of contacts within that group. Contacts that are not part of a group (groupless contacts) display below the contact group list. A contact may belong to multiple groups, but will only count once against the contact list size for that user. A warning message appears if the maximum number of contacts configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum contacts setting, see the *IM and Presence Administration Online Help*.
Watchers	Displays a list of users, known as watchers, who have subscribed to see the availability status of this user in their contact list. Click the arrow beside the Watchers heading in the Contacts and Watchers list area to view the availability status of a specific watcher. Click the arrow beside the group name to expand the list of watchers within that group. A watcher may belong to multiple groups but will only count once against the watcher list size for that user. A warning message appears if the maximum number of watchers configured for end users is exceeded. For more information about IM and Presence Service configuration and the maximum watchers setting, see the *IM and Presence Administration Online Help*.
Presence Server Assignment	Identifies the IM and Presence Service server to which the user is assigned. Hyperlinks allow you to go directly to the server configuration page for details.
Enable accessible presence icons	Select this check box to enable presence accessibility icons for this end user.
Submit	Select to run the Presence Viewer. The user must be assigned to an IM and Presence node for valid presence information to be available. The AXL, Presence Engine and Proxy Service must all be running on the IM and Presence server for this action to be functional.

Procedure changes

Display Presence Viewer for End Users

Use Cisco Unified Communications Manager Administration to display the Presence Viewer for an end user.

Before You Begin

The end user must be on the home cluster and have IM and Presence enabled.

Ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server.

Procedure

Step 1 Select **User Management** > **End User** to find the end user.
The End User Configuration window displays.

Step 2 Click the **Presence Viewer for User** link in the Service Settings area.

Note The Presence Viewer for User link will display only if the Home Cluster and Enable User for Unified CM IM and Presence check boxes are checked.

The Presence Viewer displays.

Confidential Access Levels

The Confidential Access Level (CAL) feature is used for restricting calls and other supplementary features such as transfer, forward, and conferences including Meet-Me. CAL is a numeric value assigned to any of the following entities:

- Device (for example, an IP Phone)
- Line (for example, a Directory Number)
- Trunk (for example, a SIP trunk)

CAL has two main functions:

- Controls call completion based on configuration.
- Displays information on the phone that conveys additional information about the call.

Format of CAL Matrix

The Confidential Access Level (CAL) matrix is an X/Y matrix that is used to compare one CAL to another for implementing a call policy. The CAL from the originating number is selected along the X-axis of the matrix and compared against the destination number along the Y-axis of the matrix. The intersection of these two values is known as the resolved CAL. The resolved CAL determines whether the call should proceed and also the message that is displayed to the users.

A sample CAL matrix is as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
Description	CAL	1	2	3
Unrestricted	1	1	1	1
Restricted	2	1	2	2
Confidential	3	1	2	3
END	Description	Unrestricted	Restricted	Confidential

Important The matrix must be symmetrical. For example, in the sample CAL matrix above, the value at the intersection of CAL 2 and CAL 3 is same as the value at the intersection of CAL 3 and CAL 2. Thus, the resolved CAL in both the cases is 2 (Restricted). Cisco Unified Communications Manager does not validate if the imported matrix is symmetrical. So it is the responsibility of the administrator to configure a matrix that aligns with the desired calling policy.

You can configure different CALs as per the requirement. The following CALs have been configured in this sample matrix:

- 1—Unrestricted
- 2—Restricted
- 3—Confidential

The first row of the CAL matrix must contain all the valid CALs that you want to import into Cisco Unified Communications Manager. Description and CAL values are optional. The CALs in the remaining columns can be any numeric values that you want to import. The subsequent rows define the textual description, as seen in column 1, and its relationship with other CALs in column 3 and the subsequent columns. For every CAL entered in the first row, there should be a resulting row that contains a textual description for that value. In other words, column 1 must contain textual descriptions for all the CALs that are entered in the first row. The last line (END, Description) indicates the end of the CAL matrix. The CALs beyond this row are not imported.

If a call is originated from a number whose CAL is 1 (Unrestricted) to a destination number whose CAL is 2 (Restricted), the resolved CAL is 1 (the intersection of CAL 1 and CAL 2). Hence, the text corresponding to CAL 1—Unrestricted is displayed on both the phones. Similarly, if the call is between a Restricted party (with CAL 2) and a Confidential party (with CAL 3), then Restricted (corresponding to the resolved CAL 2) will be displayed on both the phones. Thus, the CAL matrix resolves to the highest common value possible between all parties of the call.

Cisco Unified Communications Manager Administration Considerations

The following new fields have been added in both Phone Configuration and Trunk Configuration windows:

- Confidential Access Level - Select the appropriate CAL value from the drop-down list box.
- Confidential Access Mode - From the drop-down list box, select one of the following options to set the CAL mode:

- ◦ Fixed - CAL level will have higher precedence over call completion.
- ◦ Variable - Call completion will have higher precedence over CAL level.

Bulk Administration Considerations

Cisco Unified Communications Manager Bulk Administration contains the following change:

- **Bulk Administration** > **Confidential Access Level** > **Import Confidential Access Level Matrix—**To import the confidential access level matrix that contains the CAL table which is an X/Y matrix used to find the resolved CAL value.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Set Up Confidential Access Level

Follow these steps to set up confidential access level:

Procedure

Step 1 Choose **Bulk Administration** > **Confidential Access Level** > **Import Confidential Access Level matrix**. The Confidentiality Access Level Matrix Upload window opens.

Step 2 Click **Browse** and select the csv file that you want to upload.

Note The csv file contains the CAL table which is an X/Y matrix used to find the resolved CAL value.

Step 3 Click **Upload.**

Note The Upload button is enabled only for the users with Standard CCM Super Users and Standard Confidential Access Level Users access groups. The users with Standard Confidential Access Level Users access group will have access only to the page **Bulk Administration** > **Confidential Access Level** > **Import Confidential Access Level matrix**.

Configurable RTP and SRTP Port Ranges

The Configurable RTP and SRTP port ranges feature allows you to configure RTP and Secure RTP port ranges used by the software based conference bridges, Media Termination Points (MTP), Music on Hold (MoH), Annunciator media resources, and SIP endpoints. Two new service parameters—Start Media Port and Number of Ports have been added to configure RTP port ranges of IPVMS devices. The configurable port range is 9051-61000. The Start Media Port and Stop Media Port fields in the SIP profile are used to configure RTP port ranges for SIP end points. The configurable port range is 2048-65535.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Configurable Set of Nonpreemptable Numbers

Cisco Unified Communications Manager (Unified Communications Manager), Release 10.0(1) allows you to configure a list of destinations that cannot be pre-empted so that the calls on these destinations are not disconnected even if a higher precedence call is attempted. You can use this feature for calls to emergency services so that the emergency calls are not disconnected.

Cisco Unified Communications Manager Administration Considerations

An MLPP Preemption Disabled check box has been added to the Calling Party Transformation Pattern settings. You must check this check box to make the numbers in a transformation pattern nonpreemptable.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Configure Phone Presence for Unified Communications Manager Outside of Cluster

You can allow phone presence from a Cisco Unified Communications Manager that is outside of the IM and Presence Service cluster. Default requests from a Cisco Unified Communications Manager that is outside of the cluster will not be accepted by IM and Presence Service. You can also configure a SIP Trunk on Cisco Unified Communications Manager.

You must configure the TLS context before you configure the TLS peer subject.

Computer Telephony Integration Support for Cluster-Wide Call Park

Cisco Unified Communications Manager now provides Computer Telephone Integration (CTI) support for both legacy and cluster-wide call park.

For cluster-wide call park, if a cluster node becomes out of service while a call is parked, the monitored line generates a Call Disconnected event from that node. If all the nodes in the cluster become out of service, the monitored line generates a LineOutOfService event. The Parked line remains in service as long as there is one active node in the cluster.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Computer Telephony Integration Video Support

Cisco Unified Communications Manager Administration Considerations

Computer Telephony Integration (CTI) provides an interface into Cisco Unified Communications Manager (Unified Communications Manager) that allows applications to control and monitor calls, devices, and features. The CTI interfaces are JTAPI and TAPI. Cisco JTAPI is a java library that resides on the same platform as the JTAPI application. TAPI is a Microsoft Windows interface that utilizes the Cisco TSP to access Cisco Unified Communications Manager. Each CTIManager encapsulates details of the cluster from applications allowing applications access to CTI functionality for the entire cluster through a single CTI connection.

CTI Video Support for TAPI

The Video Capabilities and Multi-Media Information feature allows the TAPI Application to detect the multimedia capabilities of Line Devices. This information helps the applications monitoring devices to answer or route video calls to video capable devices. It also detects a device with a built-in camera from an audio-only device.

This application can determine the video capability of the device, the number of screens on a device, and if the device supports interoperability with telepresence devices.

If the application is monitoring only calling devices, then called device multimedia capabilities are communicated after the call is answered. If the application is monitoring only called devices, then calling device multimedia capabilities are communicated before the call is answered (for example, when a call is offered).

TAPI provides video capability information for same cluster calls involved in the following features:

- Basic Call and Consult Call
- Redirect

- Call Forward
- Hold and Resume
- Hunt List
- Transfer
- Extension Mobility
- Super Provider

TAPI provides video capability information for across-cluster calls involved in the following features:

- Basic Call and Consult Call
- Redirect
- Call Forward
- Hold and Resume
- Hunt List
- Extension Mobility
- Super Provider

The multimedia capability of the device is exposed as a structure DeviceMultiMediaCapability in the DevSpecific part. This structure contains three fields:

- DeviceVideoCapability provides the type value defined in the enumeration [CiscoDeviceVideoCapabilityInfo].
- TelepresenceInfo indicates if Telepresence is enabled on the device, defined in the enumeration [CiscoDeviceTelepresenceInfo].
- ScreenCount indicates the number of screens present on the device.

Note The initial video capability is not supported for CTI Route Points and CTI Ports; however, they can receive video information.

The following table describes the video capabilities provided by Cisco TAPI for currently supported devices.

Table 13: Video Capability for IP Phones for TAPI

Phone Model	Protocol	Video Capability – Registration update to Apps	Dynamic Video Capability change Notification	Supports TIP & Screen Count	Does CTI send MultiMedia streams Notification Event to applications?
8945	SCCP	Yes	Yes	No	No
8945	SIP	Yes	Yes	No	Yes

Phone Model	Protocol	Video Capability – Registration update to Apps	Dynamic Video Capability change Notification	Supports TIP & Screen Count	Does CTI send MultiMedia streams Notification Event to applications?
6921/6941	SCCP	Yes	Yes	No	No
9971/9951	SIP	Yes	Yes	No	Yes
EX90	SIP	Yes	N/A	No	Yes
CTIPort	SCCP	Yes [Video disabled]	N/A	N/A	No
CTIRoutePoint	SCCP	Yes [Video disabled]	N/A	N/A	No
CTS 500 CTS 500-32	SIP	Yes	N/A	Yes	Yes
Jabber (CSF/softphone mode)	SIP	Yes	Yes	Screen Count-No TIP-No	Yes

CTI Video Support for JTAPI

In Unified Communications Manager, Release 10.0(1), JTAPI is exposing video capabilities for supported terminals and calls. Video capabilities for near and far-end terminals include whether they are video-enabled, inter-operability with TelePresence, and the number of screens. Video attributes for calls will also be available to JTAPI applications which would include IP/port address, codec, and other information. Using the provided video terminal and call information, JTAPI applications will be able to better handle calls like routing incoming video-capable calls to agents with video-enabled terminals.

Exposing MultiMedia Capability on CiscoTerminal: Cisco JTAPI provides a new API, getCiscoMultiMediaCapabilityInfo() on Cisco Terminal to expose the multimedia capabilities of the terminal. These capabilities are exposed on a new interface CiscoMultiMediaCapabilityInfo, which will have the following APIs to expose these capabilities:

- getVideoCapability()
- getTelepresenceInfo()
- getScreenCount()

Exposing changes in MultiMedia Capability via a new provider event: Any change in video capability of the terminal will be notified to the application by a new JTAPI event (CiscoProvTerminalMultiMediaCapabilityChangedEv). Video capability can be changed only from the Admin Device Configuration pages. Plugging in or out a Cisco Camera does not affect the video capability status, hence the new event is not triggered in this case. This event is a JTAPI provider event, and will be delivered only if the application has added provider observers. The terminal has to be in the registered state as a pre-condition for receiving this event.

Note A change in Multimedia Capability through CiscoProvTerminalMultiMediaCapabilityChangedEv will not be delivered to applications when the video capability of an SCCP Phone changes. In this case, the terminal will unregister and register back; therefore the application needs to update the video capability after the terminal is registered.

Exposing MultiMedia Capability on a CiscoCall: An application can detect if the far-end Party for an incoming call is video capable prior to media setup. Consider a scenario where A calls B, the multimedia capabilities of the calling and called party will be exposed on the CiscoCall on terminal B after the call is offered to terminal B. The Cisco JTAPI provides the getCallingTerminalMultiMediaCapabilityInfo () and getCalledTerminalMultiMediaCapabilityInfo() APIs on the CiscoCall to expose the multimedia capabilities of the calling and called party in a call.

The same APIs can be used to determine the multimedia capabilities for an outgoing call, but note that the video capability will be known only after the call is answered. Consider a scenario where A calls B, B answers the call, the multimedia capabilities of the calling and called party will be exposed on the CiscoCall on terminal A after the call is answered by terminal B. The APIs getCallingTerminalMultiMediaCapabilityInfo() and getCalledTerminalMultiMediaCapabilityInfo() return CiscoMultiMediaCapabilityInfo.

Exposing MultiMedia Streams Information on Cisco Terminal: The new JTAPI terminal event CiscoMultiMediaStreamsInfoEv will be delivered to a terminal observer to indicate multimedia streams information of a call. The multimedia streams information is exposed on the interface CiscoMultiMediaProperties, via the API getProperties() on CiscoMultiMediaStreamsInfoEv. The Cisco JTAPI provides the multimedia streams information of the terminal after a call is connected. A MultiMedia Stream may include a video stream, a presentation stream, or both.

A video capable device is a device that can perform any of the following functions:

- Receive video (Video capability enabled in Admin Device Configuration pages and Cisco Camera not plugged in)
- Send video (Video capability enabled in Admin Device Configuration pages and Cisco Camera plugged in)
- Both send and receive video (Video capability enabled on Admin Device Configuration pages and Cisco Camera plugged in)

JTAPI will provide video capability information for same cluster calls involved in the following features:

- Originating Call and Consult Call
- Redirect
- Call Forward
- Hold and Resume
- Hunt List
- Transfer
- Extension Mobility
- Super Provider

JTAPI will provide video capability information for across-cluster calls involved in the following features:

- Basic Call and Consult Call
- Redirect
- Call Forward
- Hold and Resume
- Hunt List
- Extension Mobility
- Super Provider

The following table describes the video capabilities provided by Cisco JTAPI for currently supported devices.

Table 14: Video Capability for IP Phones for JTAPI

Phone Model	Protocol	Support Initial Device Multimedia Capability on Cisco Terminal	Supports Multimedia Capabilities on Cisco Call	Supports Multimedia Streams Information	Dynamic Video Capability Change
8945	SCCP	Yes	Yes	No	Yes
8945	SIP	Yes	Yes	Yes	Yes
9951/9971	SIP	Yes	Yes	Yes	Yes
EX60/90	SIP	Yes	Yes	Yes	N/A
CTIPort	SCCP	N/A	Yes	No	N/A
CTIRoutePoint	SCCP	N/A	Yes	No	N/A
CTS 500-32	SIP	Yes	Yes	Yes	N/A
Jabber (CSF/softphone mode)	SIP	Yes	Yes	Yes	No

Limitations for TAPI and JTAPI

The following are the limitations of the Video Capabilities and Multi-Media Information feature for TAPI.

- Remote in Use - CiscoTSP does not provide correct calling and called party multimedia capabilities on a call that is in inactive state or is in Remote InUse state.
- MultiMedia Capability Information:

    - Calling and called party multimedia capabilities will be UKNOWN on the calling side until the called party answers the call.
    - If an outbound call is initiated over SIP Trunk configured with Early Offer then the called party will just respond back with the capabilities it was offered during the initial offer and not its complete capabilities.
    - Only video capability information will be known for calls over H323 trunk, Screen count and telepresence interoperability information will be unknown.

- MultiMediaStreams Information - CiscoTSP does not provide multimedia streams information if the device is a SCCP phone; therefore, CiscoTSP will not deliver SLDSMT_MULTIMEDIA_STREAMSDATA and TSPI_LineGetCallInfo() API will not provide multimedia streams information in VideoStreamInfo structure.
- Change in called party - In scenarios like Shared Lines or redirect, where the called party changes, the application will be notified of the new called party capability only if they configure the called party with unique display names.

The following are the limitations of the Video Capabilities and Multi-Media Information feature for JTAPI.

- Outgoing call - Applications observing only calling party will have calling and called party multimedia capabilities as UKNOWN until the called party answers the call.
- Shared Line - Incoming call - calling and called party multimedia capabilities only if at least one of the terminal connections on the cisco call is not in passive state.
- Shared Line - Incoming Call - Called party multimedia capabilities will not have correct multimedia capabilities when more than one terminal connection is in ringing state.
- MultiMedia Streams Information - Cisco JTAPI will not deliver CiscoMultiMediaStreamsInfoEv on a CiscoTerminal which is a SCCP phone.
- Incoming Call - If an outbound call is initiated over SIP Trunk configured with Early Offer then the called party will just respond back with the capabilities it was offered during the initial offer and not its complete capabilities.
- Change in called party - In scenarios like Shared Lines or redirect, where the called party changes, the application will be notified of the new called party capability only if they configure the called party with unique display names.
- HuntList - Cisco JTAPI will not deliver correct multimedia capabilities for calls involving huntlist in broadcast mode.

Bulk Administration Considerations

No Changes.

CDR/CAR Considerations

No Changes.

IP Phones Considerations

No Changes.

RTMT Considerations

No Changes.

Security Considerations

No Changes.

Serviceability Considerations

No Changes.

Dial-Via-Office Reverse Voicemail Policy

This feature configures how dual mode device users answer Dial-via-Office Reverse (DVO-R) calls that terminate on the Mobile Identity (MI). This feature provides users with a single enterprise voicemail box for their enterprise mobility if the RD call reaches an external voice mail system. Available options are as follows:

- Use System Default
- Timer Control
- User Control

Cisco Unified Communications Manager Administration Considerations

On the **Remote Destination** settings window, the following drop-down list box has been added: Dial-via-Office Reverse Voicemail Policy.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Enhanced Location Call Admission Control Support for Cisco Extension Mobility Cross Cluster

This feature enables Location-based Call Admission Control (CAC) for Cisco Extension Mobility Cross Cluster (EMCC) calls to be based on the usual location configuration of the EMCC phone for the Enhanced Location Call Admission Control feature.

Prior to release 10.0(1), when an EMCC phone was involved in a call after it registered with the home cluster, Cisco Unified Communication Manager (Unified Communications Manager), used the local EMCC location configured with the roaming device pool on the home cluster Unified Communications Manager for both RSVP and static Location-based CAC.

With release 10.0(1), when an EMCC phone registers with the home cluster Unified Communications Manager , the location configuration for the physical phone on the visiting cluster is passed to the home cluster. If the home cluster supports the Enhanced Location CAC feature and participates in replication with the visiting cluster Location Bandwidth Manager (LBM) service, the home cluster uses the visiting cluster location for the location CAC calculation for the EMCC phone. RSVP CAC keeps using the home cluster roaming device pool location since RSVP policy can only be configured on intra-cluster location pairs. If the LBM on the home cluster does not connect to an LBM on the visiting cluster (Enhanced Location CAC is not enabled, or Enhanced Location CAC replication is not setup between the home cluster and the visiting cluster), the home cluster roaming device pool location is used to keep the existing pre-10.0(1) Unified Communications Manager behavior.

When a Cisco CallManager service connects with an LBM service, the LBM service sends the list of all the remote LBM clusters in the same LBM replication network to the Cisco CallManager service. LBM service also sends the update to Cisco CallManager service if the LBM replication network has any change. When an end user from home cluster logs into the EMCC phone on a visiting cluster, extension mobility service on the visiting cluster sends the location configuration for the EMCC phone and the visiting cluster's ID to extension mobility service on home cluster to save into the database on home cluster. When the EMCC phone registers with the Cisco CallManager service on the home cluster after login succeeds, Cisco CallManager service checks whether the visiting cluster ID for the EMCC phone is in the LBM replication network. If yes, the Cisco CallManager service uses the location configuration from the visiting cluster for the EMCC phone. Otherwise, the Cisco CallManager service uses the home cluster roaming device pool location for the EMCC phone.

EMCC with Different Releases of a Cisco Unified Communication Manager

The EMCC feature was introduced with Unified Communications Manager Release 8.0 and the Enhanced Location CAC feature was introduced with Unified Communications Manager Release 9.0. The EMCC feature can be configured between the Unified Communications Manager clusters with the same or different releases.

The following table lists the EMCC behavior with different releases of Unified Communications Manager.

Table 15: EMCC Behavior with Different Releases

Home Cluster	Visiting Cluster	Enhanced Location CAC Enabled Between Clusters	EMCC phone location in home cluster behavior
9.0 or earlier release	9.0 or earlier release	Not Supported	Uses default home cluster roaming device pool location

Home Cluster	Visiting Cluster	Enhanced Location CAC Enabled Between Clusters	EMCC phone location in home cluster behavior
9.0 or earlier release	10.0 or later release	Not Supported	Uses default home cluster roaming device pool location
10.0 or later release	9.0 or earlier release	Not Supported	Uses default home cluster roaming device pool location
10.0 or later release	10.0 or later release	Yes	Uses visiting cluster location configured for device
10.0 or later release	10.0 or later release	No	Uses default home cluster roaming device pool location

Restrictions and Interactions

If the visiting cluster administrator changes the location assigned to the EMCC device after the EMCC device on visiting cluster is logged in by a remote user from the home cluster, the change does not affect the EMCC device location in the home cluster until the user logs out and the same or another user logs in the EMCC device.

If the administrator changes the name of the location used by the EMCC device after the EMCC device on the visiting cluster is logged in by a remote user from the home cluster, LBM on the home cluster gets the name change propagation from the visiting cluster while Cisco CallManager service on the home cluster still has the old location name for the EMCC device. When the EMCC device makes a call, the bandwidth reservation will fail with no path error until the user logs out and the same or another user logs in the EMCC device.

If the LBM services communication is lost between the home cluster and the visiting cluster and LBM service on the home cluster does not recognize the remote location from the visiting cluster after EMCC device is logged in, the call reservation will follow the Unified Communications Manager Release 9.0 Enhanced Location CAC error condition behavior.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Flexible DSCP Marking and Video Promotion

Devices and applications use Differentiated Services Code Point (DSCP) markings to indicate the Quality of Service (QoS) treatment of IP communications. For example, desktop video endpoints may use multimedia conferencing AF41 marking for video media streams, while high-definition video room systems may use real-time interactive CS4 marking. When an application sends and receives IP communications to and from the same type of application, the DSCP markings are symmetric, and the QoS treatments of the IP communications that each application sends and receives are the same. However, when an application sends and receives media to and from a different type of application, the DSCP markings may be asymmetric, and the QoS treatments of the IP communications that each application sends and receives may be inconsistent. For example, the QoS treatment of the video media stream that a video room system receives from a desktop video endpoint may be inadequate to support the expected quality of the video room system.

Devices and applications are subjected to Call Admission Control (CAC) to ensure that adequate bandwidth is available for the duration of established sessions. The bandwidth that is utilized by established sessions is updated as the sessions begin and end. Attempts to establish new sessions that would exceed the available bandwidth are blocked. The amount of bandwidth available may be tracked independently for devices and applications of different types. For example, independent tracking of bandwidth may be available for desktop video endpoints and high-definition video room systems to send and receive video media streams.

When devices and applications of the same type send and receive communications to and from each other, the same type of bandwidth deductions are made in each direction. However, when devices and applications of different types send and receive communications to and from each other, different types of bandwidth deductions must be made in each direction. Moreover, the bandwidth deductions are usually symmetric in amount, by design, to reflect the usual behavior of an IP network. As a result, when devices and applications of different types send and receive communications to and from each other, the total bandwidth deductions may be up to double the amount of network bandwidth that is actually utilized. This inconsistency in bandwidth accounting may cause attempts to establish new sessions to be blocked unnecessarily. For example, when a desktop video endpoint and a Cisco TelePresence immersive video endpoint are in a call, in Release 9.x Unified Communications Manager CAC design deducts the same amount of bandwidth in both the video bandwidth pool and in the immersive bandwidth pool, because these two video endpoints are marking DSCP differently and the media packets can potentially traverse in different queues. This behavior unnecessarily deducts double the bandwidth that is required and potentially blocks new video calls.

In Unified Communications Manager Release 10.0(1) and later releases, the system administrator can configure a Video Promotion policy that reconciles the inconsistency in bandwidth accounting in favor of the application that receives more favorable CAC and QoS treatment. For example, if a session between a desktop video endpoint and a high-definition video room system is reconciled in favor of the video room system, then the reconciliation is deemed a promotion for the desktop video endpoint.

When reconciliation is in effect between devices and applications of different types, bandwidth is deducted only for the type of application that is favored by reconciliation. If sufficient bandwidth is available for a session of this type to be admitted, the device or application of the type that is not favored by reconciliation is instructed to change the DSCP markings that it uses to those that are used by the device or application of the type that is favored by reconciliation.

For example, if a desktop video endpoint is promoted in a session with a high-definition video room system, bandwidth accounting takes place as if the desktop video endpoint were an application of the same type as the video room system. The desktop video endpoint is instructed to change its DSCP markings to those that are used by the video room system. The QoS treatment is consistent in both directions, bandwidth is deducted for a session between devices and applications of the same type as the video room system, and bandwidth is not deducted for a session between devices and applications of the same type as the desktop video endpoint.

To activate the Flexible DSCP Marking and Video Promotion feature, in the Service Parameter Configuration window set the Use Video BandwidthPool for Immersive Video Calls service parameter to False and set the Video Call QoS Marking Policy service parameter to Promote to Immersive. When the Flexible DSCP Marking and Video Promotion feature is activated, Unified Communications Manager dynamically signals desktop video devices a Traffic Class Label that is indicative of the DSCP marking for each negotiated media stream.

Traffic Class Label

The Flexible DSCP and Video Promotion feature uses the Traffic Class Label (TCL) to instruct the SIP endpoint dynamically to mark its DSCP on a per call basis, based on the Video Promotion policy that is defined by the system administrator. Because TCL is a SIP Session Description Protocol (SDP) attribute that is defined per media line, the TCL and its associated DSCP markings can be different for the audio media line and the video media line of a video call. The system administrator can choose different DSCP markings for the audio stream and the video stream of the video call.

Interactions and Restrictions

The following interactions and restrictions apply to the Flexible DSCP Marking and Video Promotion feature:

- The Flexible DSCP Marking and Video Promotion feature is supported over SIP intercluster trunks.
- The Flexible DSCP Marking and Video Promotion feature is not supported over H.323 trunks and Media Gateway Control Protocol (MGCP) gateways.
- The Flexible DSCP Marking and Video Promotion feature is supported for Skinny Client Control Protocol (SCCP) devices.
- The Flexible DSCP Marking and Video Promotion feature is dependent on desktop SIP video endpoint support. At the time of the initial release of Unified Communications Manager Release 10.0(1), only Cisco DX650 series SIP phones provide the required endpoint support.
- If pass-through MTPs are inserted in a call, Unified Communications Manager signals the MTP to mark the packets with the DSCP marking that is expected from the endpoint device that originally emitted the packet for the video stream. If the two endpoints on a call use different DSCP markings (for example, a Cisco TelePresence immersive video endpoint and a desktop video endpoint without Video Promotion), the MTPs preserve the DSCP marking in each stream direction.
- Cisco recommends that you do not use the Flexible DSCP Marking and Video Promotion feature with Multilevel Precedence and Preemption (MLPP) service calls. When you need MLPP service functionality, Cisco recommends that you set the Video Call QoS Marking Policy and Use Video BandwidthPool for Immersive Video Calls service parameters to their default values. With default values for the Video Call QoS Marking Policy and Use Video BandwidthPool for Immersive Video Calls service parameters, Unified Communications Manager and endpoints use MLPP DSCP markings for the media packets.

Service Parameters for Flexible DSCP Marking and Video Promotion

Unified Communications Manager Release 10.0(1), and later releases, provides the following clusterwide service parameters to configure the Flexible DSCP Marking and Video Promotion feature:

- Video Call QoS Marking Policy. This parameter allows the administrator to configure a Promote to Immersive policy that reconciles bandwidth allocation inconsistencies between a desktop video endpoint and a Cisco TelePresence immersive video endpoint in favor of the immersive endpoint. When promotion is performed, the audio and video bandwidth are reserved from the immersive bandwidth pool allocation. The policy of Promote to Immersive takes effect only for calls between an immersive video device and a desktop video device that supports flexible DSCP marking.

  To configure a Promote to Immersive policy, in the Service Parameter Configuration window set the Use Video BandwidthPool for Immersive Video Calls parameter to False and set the Video Call QoS Marking Policy parameter to Promote to Immersive.

- Use Video BandwidthPool for Immersive Video Calls. This parameter specifies whether Unified Communications Manager reserves bandwidth from the desktop video bandwidth pool for immersive video calls.

- DSCP for Video Calls. This parameter specifies the DSCP value for the video stream of video calls.

- DSCP for Audio Portion of Video Calls. This parameter specifies the DSCP value for the audio stream of video calls.

- DSCP for TelePresence Calls. This parameter specifies the DSCP value for the video stream of Cisco TelePresence video calls.

- DSCP for Audio Portion of TelePresence Calls. This parameter specifies the DSCP value for the audio stream of Cisco TelePresence video calls.

- Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio). This parameter specifies the default maximum total bit rate for each immersive video call within a particular region, when the Use System Default option is selected as the Max Immersive Video Call Bit Rate in the Region Configuration window for the relationship of the region with itself. For more information about choosing the options in the Region Configuration window, see the *Cisco Unified Communications Manager Administration Guide*.

- Default Interregion Max Immersive Video Call Bit Rate (Includes Audio). This parameter specifies the default maximum total bit rate for each immersive video call between a particular region and another region, when the Use System Default option is selected as the Max Immersive Video Call Bit Rate in the Region Configuration window for the relationship of the region with the other region. For more information about choosing the options in the Region Configuration window, see the *Cisco Unified Communications Manager Administration Guide*.

Additional Information

Unified Communications Manager Release 10.0(1), and later releases, provides eight clusterwide service parameters to configure the Flexible DSCP Marking and Video Promotion feature. The following five new parameters were introduced in Release 10.0(1):

- DSCP for Audio Portion of Video Calls

- DSCP for Audio Portion of TelePresence Calls

- Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio)
- Default Interregion Max Immersive Video Call Bit Rate (Includes Audio)
- Video Call QoS Marking Policy

The following three parameters, which are also required to configure the Flexible DSCP Marking and Video Promotion feature, were introduced prior to Release 10.0(1):

- DSCP for Video Calls
- DSCP for TelePresence Calls
- Use Video BandwidthPool for Immersive Video Calls

Cisco Unified Communications Manager Administration Considerations

The following table describes two new fields that have been added to the **Region Configuration** window for the Flexible DSCP Marking and Video Promotion feature.

Table 16: Region Configuration Settings

Field	Description
Region Relationships	
Maximum Session Bit Rate for Immersive Video Calls	The entries in this column specify the maximum immersive video bit rate (including audio) between the region that you are configuring and the region that displays in the corresponding row.
Modify Relationship to other Regions	

Field	Description
Maximum Session Bit Rate for Immersive Video Calls	For each region that is specified in the Regions window pane, click one radio button in this column as specified: • Keep Current Setting—Click this button to use the current setting for the immersive video call bandwidth. • Use System Default—Click this button to use the default value. The default value normally specifies 2000000000 kbps, unless the default value has been set to a different value in the Service Parameters Configuration window. • None—Click this radio button if no immersive video call bit rate is allotted between this region and the specified region. If you choose this option, the system does not allow immersive video calls. • kbps—Click this button to set the maximum immersive video call bitrate between the region that you are configuring and the specified region. Enter the bit rate that is available for each immersive video call between these two regions; remember that the audio bit rate is included. Valid values range from 1 to 2147483647.

Procedure changes

Configure Flexible DSCP Marking and Video Promotion Service Parameters

To configure the Flexible DSCP Marking and Video Promotion service parameters, perform the following procedure.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.
The **Service Parameter Configuration** window displays.

Step 2 From the Server drop-down list, choose the server where you want to configure the parameters.

Step 3 From the Service drop-down list, choose the **Cisco CallManager (Active)** service.
If the service does not display as active, ensure that the service is activated in Cisco Unified Serviceability.

Step 4 To configure the parameters, scroll to the appropriate area of the **Service Parameter Configuration** window and update the parameter values.

Note To configure a Video Promotion policy that promotes desktop video endpoints to immersive video endpoints, set the Use Video BandwidthPool for Immersive Video Calls parameter to **False** and set the Video Call QoS Marking Policy parameter to **Promote to Immersive**.

Scroll to ...	To configure service parameter ...
Clusterwide Parameters (System - QOS) area	DSCP for Video Calls DSCP for Audio Portion of Video Calls DSCP for TelePresence Calls DSCP for Audio Portion of TelePresence Calls
Clusterwide Parameters (System - Location and Region) area	Default Intraregion Max Immersive Video Call Bit Rate (Includes Audio) Default Interregion Max Immersive Video Call Bit Rate (Includes Audio) Use Video BandwidthPool for Immersive Video Calls
Clusterwide Parameters (Call Admission Control) area	Video Call QoS Marking Policy

Tip For information on the service parameters, click the parameter name or click the question mark (?) icon that displays in the **Service Parameter Configuration** window.

Step 5 Click **Save**.

Gateway Recording and Media Forking

For Cisco Unified Communications Manager (Unified Communications Manager), Release 10.0(1) and later, the gateway recording and media forking feature performs the following functions:

- Records unencrypted external calls using ingress/egress voice gateways as media anchoring points to fork media.
- Configures preferred media anchoring point.
- Starts and stops media forking for calls routed by Session Manager in the UCM Leaf Cluster.
- Has a transparent record of the gateway and phone-based recording in the recording server.
- Provides recording meta data in SIP header to allow Cisco MediaSense recording server to follow the call.
- Provides CTI application as the recording party data.
- Supports existing recording call flow and automatically choose recording modes.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Global Dial Plan Replication

Global Dial Plan Replication allows you to create a global dial plan that spans across an ILS network and which includes intercluster dialing of directory URIs and alternate numbers. When Global Dial Plan Replication is enabled, the Intercluster Lookup Service (ILS) advertises global dial plan data, including locally configured and any data that was learned from other clusters, to the ILS network. Global dial plan data includes the following:

- Directory URIs
- Alternate Numbers
- Advertised Patterns
- PSTN Failover
- Route String
- Learned Global Dial Plan Data
- Imported Global Dial Plan Data

Directory URIs

ILS replicates the full catalog of locally configured directory URIs where the Advertise Globally via ILS option has been selected. The “URI dialing” chapter in the *Cisco Unified Communications Manager Features and Services Guide* contains details on how to set up URI dialing.

Alternate Numbers

Alternate numbers can be configured as aliases of directory numbers. Alternate numbers allow you to configure globally routable numbers that can be dialed from anywhere within an ILS network. Cisco Unified Communications Manager (Unified Communications Manager) allows you to create two types of alternate numbers:

- Enterprise alternate numbers
- +E.164 alternate numbers

In Cisco Unified Communications Manager Administration, you can create an enterprise alternate number and an +E.164 alternate number and associate both alternate numbers to a directory number. When you associate an alternate number to a directory number, the alternate number can act as an alias of that directory number so that when you dial the alternate number, the phone that is registered to the associated directory number rings.

Each alternate number that you set up must associate to a single directory number. However, that directory number can associate to both an enterprise alternate number and an +E.164 alternate number at the same time. You can also choose one of the alternate numbers as the PSTN failover number for all alternate numbers and directory URIs that are associated to that directory number.

Advertised Patterns

Advertised patterns allow you to create summarized routing instructions for a range of enterprise alternate numbers or +E.164 alternate numbers and replicate that pattern throughout an ILS network such that all clusters within the ILS network know the pattern. Advertised patterns save you from having to configure routing information for each alternate number on an individual basis. Advertised patterns are never used by the local cluster on which they are configured; they are only used by remote clusters that learn the pattern through ILS.

For example, if Cluster A has a range of enterprise alternate numbers between 80001-89999 and you want to replicate those alternate numbers throughout the ILS network, you can create a pattern of 8XXXX and advertise that pattern to the ILS network. When a remote cluster receives an outgoing call for which the dial string matches the learned pattern (for example, 82211), the remote cluster uses the route string that is associated with the pattern to route the call.

PSTN Failover

When Global Dial Plan Replication is enabled, ILS can be configured to replicate a PSTN failover rule for learned directory URIs, learned numbers, and learned patterns. If the dial string for an outgoing call matches a learned pattern, learned alternate number, or learned directory URI, and Unified Communications Manager is unable to route the call over a SIP trunk, Unified Communications Manager uses the calling party's AAR CSS to reroute the call to the associated PSTN failover number.

Unified Communications Manager uses the PSTN failover for routing only for calls placed to learned patterns, learned alternate numbers, or learned directory URIs. Unified Communications Manager does not route calls to the PSTN failover number for calls that are placed to patterns, alternate numbers, or directory URIs that were configured in the local cluster.

Route Strings

To configure Global Dial Plan Replication, you must assign a distinct route string for each cluster in the ILS network. Route strings can be up to 250 alphanumeric characters, including dots (.) and dashes(-). Although route strings are used with domain-based routing, route strings do not have to match a specific domain; you can assign whatever route strings you want.

When you assign a route string to a cluster, ILS associates that route string to all the global dial plan data that is local to that cluster (including locally configured directory URIs, alternate numbers, advertised patterns, and PSTN failover information). If Global Dial Plan Replication is enabled, ILS advertises the local route string and the rest of the global dial plan data to the ILS network.

To configure remote Unified Communications Manager clusters to route to the route string, for each cluster in the ILS network, you must configure SIP route patterns that match the route strings in the ILS network and route calls that are destined for those route strings to SIP trunks that lead to the next-hop clusters in your ILS network.

When a user in a remote cluster dials a directory URI or alternate number that was learned via ILS, Unified Communications Manager pulls the associated route string, matches that route string to a SIP route pattern, and routes the call to the trunk that is specified by the SIP route pattern.

Learned Global Dial Plan Data

In addition to locally configured global dial plan data, ILS advertises all global dial plan data that the local cluster has learned from other clusters in the ILS network. This ensures that all advertised data reaches each cluster in the ILS network. Learned global dial plan data includes learned directory URIs, learned alternate numbers, learned patterns, learned PSTN failover rules, and learned route strings.

Imported Global Dial Plan Data

ILS also advertises global dial plan data that has been imported from a CSV file into any hub cluster in the ILS network. Imported global dial plan data includes directory URI catalogs, +E.164 patterns, and PSTN failover numbers for a call control system that does not run ILS, such as a Cisco TelePresence Video Communication Server, or a third-party call control system.

Cisco Unified Communications Manager Administration Considerations

Cisco Unified Communications Manager Administration contains the following changes:

- **Call Routing** > **Directory Number**: The Directory Number Configuration window has the following updates:
    - An Enterprise Alternate Number section has been added that allows you to create an enterprise alternate number as an alias of the directory number and advertise that alternate number to the ILS network.
    - An +E.164 Alternate Number section has been added with the same fields and capability as with Enterprise Alternate Numbers.
    - The Directory URIs section has been updated with a check box that you must check for ILS to replicate the directory URI to remote clusters.
    - A PSTN failover option has been added where you can choose one of the alternate numbers as a PSTN failover for all the alternate numbers and directory URIs that are associated to this directory number.
- **Call Routing** > **Route Plan Report**: The Route Plan Report window now supports directory URIs and learned patterns.
- **Call Routing** > **Global Dial Plan Replication**: This menu path is new. The Global Dial Plan Replication menu path replaces the Intercluster Directory URI menu path from the last release.

- **Call Routing** > **Global Dial Plan Replication** > **Advertised Patterns**: This is a new menu item that allows you to create an alternate number pattern that ILS advertises to the ILS network. Advertised patterns allow you to create a single number pattern that summarizes a range of alternate numbers.
- **Call Routing** > **Global Dial Plan Replication** > **Block Learned Numbers and Patterns**: This is a new menu item that allows you to create a blocking rule for alternate numbers or patterns that have been learned with ILS.
- **Call Routing** > **Global Dial Plan Replication** > **Partitions for Learned Numbers and Patterns**: This is a new menu item that allows you to assign alternate numbers and alternate number patterns that have been learned with ILS to a partition on the local cluster.
- **Call Routing** > **Global Dial Plan Replication** > **Learned Numbers**: This is a new menu item that allows you to view all of the alternate numbers that the local cluster has learned with ILS.
- **Call Routing** > **Global Dial Plan Replication** > **Learned Patterns**: This is a new menu item that allows you to view all of the number patterns that the local cluster has learned with ILS.
- **Call Routing** > **Global Dial Plan Replication** > **Learned Directory URIs**: This is a new menu item that allows you to view all of the directory URIs that the local cluster has learned with ILS.
- **Advanced Features** > **ILS Configuration**:The ILS Configuration window has been updated with the Enable Global Dial Plan Replication check box and the Advertised Route String text box. In addition, the ILS Clusters and Directory URI Imported Catalogs view has been updated.
- **Device** > **Device Settings** > **SIP Profile**: The Send ILS Learned Destination Route String check box has been added.

Bulk Administration Considerations

The following menu items have been changed:

- **Bulk Administration** > **Directory URIs and Patterns**: This menu path is new. The Global Dial Plan Replication menu path replaces the Imported Directory URIs menu path from the last release.
- **Bulk Administration** > **Directory URIs and Patterns** > **Export Local Directory URIs and Patterns**: This is a new menu item that allows you to export directory URIs, +E.164 advertised patterns, and PSTN failover rules to a CSV file.

The following line fields have been added to the *bat.xlt* import spreadsheet:

- Enterprise Is Urgent
- Enterprise Add to Local Route Partition
- Enterprise Advertise Via Globally
- Enterprise Number Mask
- Enterprise Route Partition
- E.164 Is Urgent
- E.164 Add to Local Route Partition
- E.164 Advertise Via Globally
- E.164 Number Mask
- E.164 Route Partition

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Set Up Global Dial Plan Replication

This procedure describes how to set up Global Dial Plan Replication in the ILS network. See the Related Topics for more detailed information on how to perform some of the high-level steps in this procedure.

Before You Begin

Global Dial Plan Replication runs on an ILS network. Follow the procedure to set up an ILS network in the “Intercluster Lookup Service” chapter before you configure Global Dial Plan Replication.

Procedure

Step 1 Enable ILS support for Global Dial Plan Replication in the local cluster:

a) Log in to the Unified Communications Manager publisher node.
b) In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **ILS Configuration**.
c) Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.
d) In the **Advertised Route String** text box, enter a route string for the local cluster.
e) Click **Save**.

Step 2 (Optional) If you want to be able to dial directory URIs across clusters, set up URI dialing in the local cluster. For details, see the “URI dialing” chapter.

Step 3 (Optional) If you want to set up alternate numbers that you can dial between clusters, set up alternate number replication by doing the following:

a) Assign enterprise alternate numbers or +E.164 alternate numbers to the directory numbers in your network.

b) For each alternate number, check the **Advertise Globally via ILS** check box.

Step 4 (Optional) If you want to set up a PSTN failover number for specific directory URIs or alternate numbers, assign an alternate number as the PSTN failover number for all the directory URIs and alternate numbers that are associated to a specific directory number.

Step 5 (Optional) If you want to summarize your alternate numbers with a pattern, set up an advertised pattern, and assign a PSTN failover rule for the pattern.

Step 6 In the **Partitions for Learned Numbers and Patterns** configuration window, assign route partitions to the alternate numbers and patterns that the local cluster learns through ILS.

Step 7 Set up SIP route patterns to route calls to the remote clusters in your ILS network by doing the following:

a) Create SIP route patterns that match the route strings for the remote clusters in the ILS network.

b) Point those SIP route patterns to SIP trunks or route lists that route calls to the next-hop clusters in the ILS network.

Step 8 If your network includes a Cisco Unified Border Element, do the following for the SIP profiles in your network:

a) In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

b) Check the **Send ILS Learned Destination Route String** check box and click **Save**.

Step 9 Set an upper limit for the number of learned objects that ILS can write to the local database by setting a value for the ILS Max Number of Learned Objects service parameter. The default value is 100,000.

Step 10 Repeat the previous steps for each cluster in your ILS network.

Step 11 (Optional) If you want your ILS network to interoperate with a Cisco TelePresence Video Communication Server or third-party call control system, import directory URI catalogs from a CSV file for the other system into any hub cluster in the ILS network.

Related Topics

Set Up Alternate Number, on page 83

Set Up an Advertised Pattern for Alternate Numbers, on page 85

Set Up PSTN Failover for Directory URIs and Alternate Numbers, on page 84

Set Up Alternate Number

This procedure describes how to assign an enterprise alternate number or +E.164 alternate number to an existing directory number and configure that alternate number for local or intercluster calls.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.

Step 2 Find and select the directory number to which you want to associate the alternate number.

Step 3 Click either **Add Enterprise Alternate Number** or **Add +E.164 Alternate Number** depending on which type of alternate number you want to assign.

Step 4 In the **Number Mask** field, enter the number mask that you want to apply to the directory number. The **Alternate Number** field displays how the alternate number appears after Cisco Unified Communications Manager applies the number mask.

Step 5 (Optional) If you want to enable local routing for the alternate number, do the following:

a) Check the **Add to Local Route Partition** check box.
b) From the **Route Partition** drop-down list box, choose a route partition that is assigned to a local calling search space.

Step 6 (Optional) If you want to use a number pattern to set up intercluster routing for this alternate number, click **Save** and end the procedure. See the Related Topics section for a procedure on how to advertise an alternate number pattern to the ILS network.

Step 7 (Optional) If you want to set up intercluster routing for this alternate number, check the **Advertise Globally via ILS** check box for this alternate number.

Step 8 (Optional) If you want to assign a PSTN failover number to this alternate number, from the **PSTN failover** drop-down list box, assign a number as the PSTN failover.

Step 9 Click **Save**.

What to Do Next

If you want to enable intercluster routing for the alternate number you must also set up Global Dial Plan Replication within your ILS network. ILS will not advertise the alternate number unless Global Dial Plan Replication is enabled.

Related Topics

Set Up an Advertised Pattern for Alternate Numbers, on page 85

Set Up PSTN Failover for Directory URIs and Alternate Numbers

This procedure describes how to assign a PSTN failover number for directory URIs or alternate numbers and advertise that PSTN failover number to the ILS network. Remote clusters can use the PSTN failover number for calls to learned directory URIs or learned alternate numbers.

Note For alternate numbers, you can also assign a PSTN failover rule to an advertised pattern that summarizes a range of alternate numbers. To assign a PSTN failover rule to an advertised pattern, see Set Up an Advertised Pattern for Alternate Numbers, on page 85.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Directory Number**.

Step 2 Find and select the directory number that is associated to the directory URI or alternate number for which you want to assign a PSTN failover number.

Step 3 If the alternate number that you want to use as the PSTN failover does not exist, create either an enterprise alternate number or a +E.164 alternate number for the directory number.

Step 4 In the PSTN Failover drop-down list box, choose the alternate number that you want to use as the PSTN failover.

Step 5 Click **Save**.

Cisco Unified Communications Manager associates that PSTN failover number to that directory number. Global Dial Plan Replication advertises that number to the ILS network as the PSTN failover number for all the directory URIs and alternate numbers that are associated to that directory number.

What to Do Next

In order for a remote cluster to route calls to the PSTN failover number, you must set up the AAR CSS and configure route patterns in the remote cluster that route the PSTN failover number to a PSTN gateway.

Set Up an Advertised Pattern for Alternate Numbers

Follow this procedure to create a pattern that summarizes a range of alternate numbers and advertise the pattern to the ILS network.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Advertised Patterns**.

Step 2 In the **Description** field, enter a description for the pattern.

Step 3 In the **Pattern** field, enter the pattern that you want to advertise to the ILS network.

Step 4 Use the **Pattern Type** radio buttons to choose whether you want to apply the pattern to a range of enterprise alternate numbers or +E.164 alternate numbers.

Step 5 Complete the remaining fields in the **Advertised Patterns Configuration** window to configure a PSTN failover rule for the pattern.

Step 6 Click **Save.**
If Global Dial Plan Replication is enabled, ILS advertises the pattern to remote clusters in the ILS network.

What to Do Next

For remote clusters to be able to route calls to the PSTN failover number, in the remote cluster you must set up AAR and create route patterns that route the PSTN failover digits to a PSTN gateway.

Block a Learned Pattern

If you want to prevent a local Cisco Unified Communications Manager cluster from routing calls to a learned alternate number or learned alternate number pattern, you can configure a local blocking rule on that cluster. Before routing a call to a learned number or learned pattern, ILS checks to see if a local blocking rule matches the dial string. If the blocking rule matches, Cisco Unified Communications Manager does not route the call.

Some additional characteristics of blocking rules:

- Blocking rules are applied only on the local cluster on which you configure them—ILS does not advertise blocking rules.
- Blocking rules are applied only to learned alternate numbers and learned patterns—Cisco Unified Communications Manager does not apply blocking rules to locally configured numbers or route patterns.

To set up a blocking rule for a learned alternate number or learned alternate number pattern, perform the following steps:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Global Dial Plan Replication** > **Block Learned Numbers and Patterns**.

Step 2 Enter a description for the blocking rule.

Step 3 In the Blocked Pattern section, complete the fields that you want to use as conditions for the blocking rule. If you do not want to use a specific field as a blocking condition, you can leave that field blank. For example:

- If you want to block all calls to ABC_cluster1 regardless of the other call parameters, enter ABC_cluster1 in the **Cluster ID** field, click the **Any** radio button, and leave the remaining fields empty.
- If you want to block all +E.164 calls to Cluster_3 that use a prefix of 683, enter “Cluster_3” in the Cluster ID field, enter “683” in the Prefix field, click the **+E.164 Pattern** radio button, and leave the remaining fields empty.
- If you want to block a specific enterprise pattern, enter the pattern in the Pattern field and click the **Enterprise Pattern** radio button.

Step 4 In the Pattern type field, choose whether you want to apply the blocking rule to Enterprise patterns, +E.164 patterns, or both.

Step 5 Click **Save**.

IM and Presence Service Group Chat and Persistent Chat Configuration

This section describes how to configure the enhanced ad hoc and persistent chat settings. These settings are configured with default values that you can modify. You can revert all settings to their default values by clicking the **Set to Default** button.

Note To allow chat room owners to change a setting, check the **Room owners can change** check box on the server. The room owner can then configure such settings as they wish and those settings are applicable to the room they are creating. The availability of configuring these settings from the client also depends on the client implementation and whether the client is providing an interface in which to configure these settings.

Procedure changes

Configure group chat alias settings

Group chat alias settings allow users in any domain to search for specific chat rooms on specific nodes, and join in those chat rooms.

Procedure

Step 1 Check **System automatically manages primary group chat server aliases** if you want to enable the system to automatically assign chat room aliases to nodes, using the alias naming convention “conference-x-clusterid.domain.”The check box is checked by default.

Step 2 Click **Save**.

Note If you are adding, deleting, or modifying aliases you must restart the Cisco XCP Text Conference Manager on all nodes in the cluster by selecting **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

Related Topics

Group chat system administration

Cisco XCP Text Conference Manager service restart

Enable Persistent Chat

You need to configure persistent chat settings only if you use persistent chat rooms as opposed to temporary (ad hoc) chat rooms. This configuration is specific to persistent chat and has no impact on IM archiving for regulatory compliance.

Before You Begin

- To use persistent chat rooms, you must configure a unique external database instance for each node.
- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.
- Archiving all room joins and leaves is optional, because it increases traffic and consumes space on the external server.
- Before you configure the number of connections to the external database, consider the number of IMs you are writing and the overall volume of traffic that results. The number of connections that you configure will allow the system to scale. While the default settings on the UI suit most installations, you may want to adapt the parameters for your specific deployment.
- The heartbeat interval is typically used to keep connections open through firewalls. Do not set the Database Connection Heartbeat Interval value to zero without contacting Cisco support.
- You must have an external database assigned for each node.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Group Chat and Persistent Chat**.

Step 2 Check **Enable Persistent Chat**.

Step 3 (Optional) Check **Archive all room joins and exits** if you want to log all instances of users joining and leaving a room. This is a cluster-wide setting that applies to all persistent chat rooms.

Step 4 (Optional) Check **Archive all room messages** if you want to archive all the messages that are sent in the room. This is a cluster-wide setting that applies to all persistent chat rooms.

Step 5 (Optional) Check **Allow only group chat system administrators to create persistent chat rooms** if you want to ensure that persistent chat rooms are created only by group chat system administrators. This is a cluster-wide setting that applies to all persistent chat rooms.
To configure group chat system administrators, choose **Messaging** > **Group chat system administrators**.

Step 6 Enter the maximum number of persistent chat rooms that are allowed in the **Maximum number of persistent chat rooms allowed** field. The default value is set to 1500.

Note You must ensure there is sufficient space on the external database. Having a large number of chat rooms impacts resources on the external database.

Step 7 Enter the number of connections to the database that you to want to use for processing requests in the **Number of connections to the database** field. The default is set to 5. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

Step 8 Enter the number of seconds after which the database connection should refresh in the **Database connection heartbeat interval (seconds)** field. The default is set to 300. This is a cluster-wide setting that applies to all connections between chat nodes and associated databases.

Step 9 Enter the number of minutes after which the chat room should time out in the **Timeout value for persistent chat rooms (minutes)** field. The default is set to 0. The timeout is used to check whether a chat room is idle and empty. If the room is found to be idle and empty, the room is closed. With the default value set to 0, the idle check is disabled.

Step 10 Choose from the list of preconfigured external databases and assign the appropriate database to the chat node.

- If you turn on the **Archive all room joins and exits** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you turn on the **Archive all room messages** setting, Cisco recommends that you monitor the performance of each external database that is used for persistent chat. Expect an increased load on the database servers.
- If you enable persistent chat rooms but do not establish the correct connection with the external database, the chat node will fail. Under these circumstances, you will lose the functionality of all chat rooms, both temporary and persistent. If a chat node establishes a connection (even if other chat nodes fail), it will still start.
- Click the hyperlink if you need to edit the Cisco Unified Communications Manager IM and Presence Service node details in the **Cluster Topology Details** window.

Step 11 Click **Save**.

Step 12 Restart the Cisco XCP Text Conference Manager on all nodes in the cluster by selecting **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services**.

Note After you have enabled persistent chat, if you subsequently want to update any of the persistent chat settings, only the following non-dynamic settings require a Cisco XCP Text Conference Manager restart:

- Number of connections to the database
- Database connection heartbeart interval (seconds)

Set Number of Chat Rooms

Use room settings to limit the number of rooms that users can create. Limiting the number of chat rooms will help the performance of the system and allow it to scale. Limiting the number of rooms can also help mitigate any possible service-level attacks.

Procedure

Step 1 To change the maximum number of chat rooms that are allowed, enter a value in the field for **maximum number of rooms allowed**. The default is set to 16500.

Step 2 Click **Save**.

Configure Member Settings

Member settings allow system-level control over the membership in chat rooms. Such a control is useful for users to mitigate service-level attacks that can be prevented by administrative actions such as banning. Configure the member settings as required.

Procedure

Step 1 Check **Rooms are for members only by default** if you want rooms to be created as members-only rooms by default. Members-only rooms are accessible only by users on a white list configured by the room owner or administrator. The checkbox is unchecked by default.

Note The white list contains the list of members who are allowed in the room. It is created by the owner or administrator of the members-only room.

Step 2 Check **Room owners can change whether or not rooms are for members only** if you want to configure the room so that room owners are allowed to change whether or not rooms are for members only. The check box is checked by default.

Note A room owner is the user who creates the room or a user who has been designated by the room creator or owner as someone with owner status (if allowed). A room owner is allowed to change the room configuration and destroy the room, in addition to all other administrator abilities.

Step 3 Check **Only moderators can invite people to members-only rooms** if you want to configure the room so that only moderators are allowed to invite users to the room. If this check box is unchecked, members can invite other users to join the room. The check box is checked by default.

Step 4 Check **Room owners can change whether or not only moderators can invite people to members-only rooms** if you want to configure the room so that room owners can allow members to invite other users to the room. The check box is checked by default.

Step 5 Check **Users can add themselves to rooms as members** if you want to configure the room so that any user can request to join the room at any time. If this check box is checked, the room has an open membership. The check box is unchecked by default.

Step 6 Check **Room owners can change whether users can add themselves to rooms as members** if you want to configure the room so that room owners have the ability to change the setting that is listed in Step 5 at any time. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Availability Settings

Availability settings determine the visibility of a user within a room.

Procedure

Step 1 Check **Members and administrators who are not in a room are still visible in the room** if you want to keep users on the room roster even if they are currently offline. The check box is checked by default.

Step 2 Check **Room owners can change whether members and administrators who are not in a room are still visible in the room** if you want to allow room owners the ability to change the visibility of a member or administrator. The check box is checked by default.

Step 3 Check **Rooms are backwards-compatible with older clients** if you want the service to function well with older Group Chat 1.0 clients. The check box is unchecked by default.

Step 4 Check **Room owners can change whether rooms are backwards-compatible with older clients** if you want to allow room owners the ability to control backward compatibility of the chat rooms. The check box is unchecked by default.

Step 5 Check **Rooms are anonymous by default** if you want the room to display the user nickname but keep the Jabber ID private. The check box is unchecked by default.

Step 6 Check **Room owners can change whether or not rooms are anonymous** if you want to allow room owners to control the anonymity level of the user Jabber ID. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Invite Settings

Invite settings determine who can invite users to a room based on the user's role. Roles exist in a moderator-to-visitor hierarchy so, for instance, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

Procedure

Step 1 From the drop-down list for **Lowest participation level a user can have to invite others to the room**, choose one:

- **Visitor** allows visitors, participants, and moderators the ability to invite other users to the room.
- **Participant** allows participants and moderators the ability to invite other users to the room. This is the default setting.
- **Moderator** allows only moderators the ability to invite other users to the room.

Step 2 Check **Room owners can change the lowest participation level a user can have to invite others to the room** to allow room owners to change the settings for the lowest participation level that is allowed to send invitations. The check box is unchecked by default.

Step 3 Click **Save**.

Configure Occupancy Settings

Procedure

Step 1 To change the system maximum number of users that are allowed in a room, enter a value in the field for **How many users can be in a room at one time**. The default value is set to 1000.

Note The total number of users in a room should not exceed the value that you set. The total number of users in a room includes both normal users and hidden users.

Step 2 To change the number of hidden users that are allowed in a room, enter a value in the field for **How many hidden users can be in a room at one time**. Hidden users are not visible to others, cannot send a message to the room, and do not send presence updates. Hidden users can see all messages in the room and receive presence updates from others. The default value is 1000.

Step 3 To change the default maximum number of users that are allowed in a room, enter a value in the field for **Default maximum occupancy for a room**. The default value is set to 50 and cannot be any higher than the value that is set in Step 1.

Step 4 Check **Room owners can change default maximum occupancy for a room** if you want to allow room owners to change the default maximum room occupancy. The check box is checked by default.

Step 5 Click **Save**.

Configure Chat Message Settings

Use Chat Message settings to give privileges to users based on their role. For the most part, roles exist in a visitor-to-moderator hierarchy. For example, a participant can do anything a visitor can do, and a moderator can do anything a participant can do.

Procedure

Step 1 From the drop-down list for **Lowest participation level a user can have to send a private message from within the room**, choose one:

- **Visitor** allows visitors, participants, and moderators to send a private message to other users in the room. This is the default setting.
- **Participant** allows participants and moderators to send a private message to other users in the room.
- **Moderator** allows only moderators to send a private message to other users in the room.

Step 2 Check **Room owners can change the lowest participation level a user can have to send a private message from within the room** if you want to allow room owners to change the minimum participation level for private messages. The check box is checked by default.

Step 3 From the drop-down list for **Lowest participation level a user can have to change a room's subject**, choose one:

a) **Participant** allows participants and moderators to change the room's subject. This is the default setting.
b) **Moderator** allows only moderators to change the room's subject.

Visitors are not permitted to change the room subject.

Step 4 Check **Room owners can change the lowest participation level a user can have to change a room's subject** if you want to allow room owners to change the minimum participation level for updating a room's subject. The check box is checked by default.

Step 5 Check **Remove all XHTML formatting from messages** if you want to remove all Extensible Hypertext Markup Language (XHTML) from messages. The check box is unchecked by default.

Step 6 Check **Room owners can change XHTML formatting setting** if you want to allow room owners to change the XHTML formatting setting. The check box is unchecked by default.

Step 7 Click **Save**.

Configure Moderated Room Settings

Moderated rooms provide the ability for moderators to grant and revoke the voice privilege within a room (in the context of Group Chat, voice refers to the ability to send chat messages to the room). Visitors cannot send instant messages in moderated rooms.

Procedure

Step 1 Check **Rooms are moderated by default** if you want to enforce the role of moderator in a room. The check box is unchecked by default.

Step 2 Check **Room owners can change whether rooms are moderated by default** if you want to allow room owners the ability to change whether rooms are moderated. The check box is checked by default.

Step 3 Click **Save**.

Configure History Settings

Use History settings to set the default and maximum values of messages that are retrieved and displayed in the rooms, and to control the number of messages that can be retrieved through a history query. When a user joins a room, the user is sent the message history of the room. History settings determine the number of previous messages that the user receives.

Procedure

Step 1 To change the maximum number of messages that users can retrieve from the archive, enter a value in the field for **Maximum number of messages that can be retrieved from the archive**. The default value is set to 100. It serves as a limit for the next setting.

Step 2 To change the number of previous messages displayed when a user joins a chat room, enter a value in the field for **Number of messages in chat history displayed by default**. The default value is set to 15 and cannot be any higher than the value that is set in Step 1.

Step 3 Check **Room owners can change the number of messages displayed in chat history** if you want to allow room owners to change the number of previous messages displayed when a user joins a chat room. The check box is unchecked by default.

Step 4 Click **Save**.

IM and Presence Service Group Chat System Administration

This section describes how to configure group chat system administration.

Note Jabber does not currently support the persistent chat feature. The availability of the functionality depends on client implementation.

Group chat system administrators can do the following:

- Configure a room
- Join a password-protected room without supplying the password
- Change a room's subject
- Join any room (including members-only rooms)
- Moderate a room
- Join a room when the maximum occupancy is reached
- Destroy a room
- Browse a room for the list of participants
- Query a room and its items
- Remain in a room if the room changes to be members-only, or if their affiliation changes to "none" in a members-only room

- Change the affiliation of other users in a room
- Invite other users to a members-only room (even when members invite is not allowed).

Procedure changes

Configure Group Chat System Administration

Procedure

Step 1 Choose **Messaging** > **Group Chat System Administrators**.

Step 2 Check **Enable Group Chat System Administrators**.
You must restart the Cisco XCP Router when the setting is enabled or disabled. Once the System Administrator setting is enabled, you can add system administrators dynamically.

Step 3 Click **Add New**.

Step 4 Enter an IM address.

Example:
The IM address must be in the format of name@domain .

Step 5 Enter a nickname.

Step 6 Enter a description.

Step 7 Click **Save**.

IM and Presence Service IM Addressing for Multiple Domains

The IM and Presence Service supports two IM addressing schemes:

- *UserID@Default_Domain* is the default IM address scheme when you install the IM and Presence Service.
- Directory URI IM address scheme supports multiple domains, alignment with the user's email address, and alignment with Microsoft SIP URI.

Note The chosen IM address scheme must be consistent across all IM and Presence Service clusters.

The default domain is a cluster-wide setting that is used as part of the IM address when using the *UserID@Default_Domain* IM address scheme.

The Directory URI IM address scheme provides the following IM addressing features:

- Multiple domain support. IM addresses do not need to use a single IM and Presence Service domain.

- Alignment with the user's email address. The Cisco Unified Communications Manager Directory URI can be configured to align with a user's email address to provide a consistent identity for email, IM, voice and video communications.
- Alignment with Microsoft SIP URI. The Cisco Unified Communications Manager Directory URI can be configured to align with the Microsoft SIP URI to ensure that the user's identity is maintained when migrating from Microsoft OCS/Lync to IM and Presence Service.

You set the Directory URI using Cisco Unified CM IM and Presence Administration GUI in one of two ways:

- Synchronize the Directory URI from the LDAP directory source.

  If you add an LDAP directory source in Cisco Unified Communications Manager, you can set a value for the Directory URI. Cisco Unified Communications Manager then populates the Directory URI when you synchronize user data from the directory source.

  Note If LDAP Directory Sync is enabled in Cisco Unified Communications Manager, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).

- Manually specify the Directory URI value in Cisco Unified Communications Manager.

  If you do not add an LDAP directory source in Cisco Unified Communications Manager, you can manually enter the Directory URI as a free-form URI.

See the *Cisco Unified Communications Manager Administration Guide* for more information about setting up the LDAP directory for Directory URI.

IM and Presence Service supports IM addressing across multiple IM address domains and automatically lists all domains in the system. Use the Cisco Unified CM IM and Presence Administration GUI to manually add, update, and delete local administrator-managed domains, as well as view all local and system managed domains.

For more information, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

The following alerts were added:

- DuplicateDirectoryURI
- InvalidDirectoryURI
- DuplicateUserid

Security Considerations

No changes.

Serviceability Considerations

No changes.

IM and Presence Service Considerations

Use the Cisco Unified CM IM and Presence Administration GUI to set up IM addressing and multiple domain support for your deployment:

- Directory URI IM addressing scheme support and configuration
- IM and Presence Service default domain changes
- Multiple domain setup and management
- Multiple domain support for Partitioned Intradomain Federation
- End user management and duplicate or invalid user entry troubleshooting

For details to configure the IM addressing scheme, integrate and mange multiple domains, and manage end users for your deployment, see the following guides:

- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*
- *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*
- *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*

Note If the Directory URI IM address scheme is used anywhere in the deployment, your client software must support Directory URI.

For multiple domain support with intercluster deployments, IM and Presence Service clusters and client devices are no longer required to have matching DNS domains. As well, the IM and Presence Service default domain no longer has to match the DNS domain. For more information, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.

For information about setting or changing the domain name for the IM and Presence Service node, see *Installing the Cisco Unified Communications Manager* and *Changing the Hostname and IP Address for Cisco Unified Communications Manager and IM and Presence Service*.

For multiple domain support with partitioned intradomain federation, identical domains must be configured on both the IM and Presence Service node and the supported Microsoft servers. For more information, see *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.

Procedure Changes

See the related IM and Presence Service guides for all the latest procedures.

Additional Information

UserID@Default_Domain IM Address Interactions and Restrictions

The following restrictions apply to the *UserID@Default_Domain* IM address scheme:

- All IM addresses are part of the IM and Presence default domain, therefore, multiple domains are not supported.
- The IM address scheme must be consistent across all IM and Presence Service clusters.
- The default domain value must be consistent across all clusters.
- If *UserID* is mapped to an LDAP field on Cisco Unified Communications Manager, that LDAP mapping must be consistent across all clusters.

Directory URI IM Address Interactions and Restrictions

To support multiple domain configurations, you must set Directory URI as the IM address scheme for IM and Presence Service.

Caution If you configure the node to use Directory URI as the IM address scheme, Cisco recommends that you deploy only clients that support Directory URI. Any client that does not support Directory URI will not work if the Directory URI IM address scheme is enabled. Cisco recommends that you use the *UserID@Default_Domain* IM address scheme and not the Directory URI IM address scheme if you have any deployed clients that do not support Directory URI.

Observe the following restrictions and interactions when using the Directory URI IM address scheme:

- All users have a valid Directory URI value configured on Cisco Unified Communications Manager.
- All deployed clients must support Directory URI as the IM address and use EDI-based directory integration.
- UDS-based directory integration is not supported.
- The IM address scheme must be consistent across all IM and Presence Service clusters.
- All clusters must be running a version of Cisco Unified Communications Manager that supports the Directory URI addressing scheme.
- If LDAP Sync is disabled, you can set the Directory URI as a free-form URI. If LDAP Directory Sync is enabled, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).

- The Directory URI IM address settings are global and apply to all users in the cluster. You cannot set a different Directory URI IM address for individual users in the cluster.
- Your Cisco Jabber client must support Directory URI. See the documentation that came with your Cisco Jabber client to determine compatibility.
- The Cisco Jabber client must be configured to align with the IM address scheme and the Directory URI configuration on IM and Presence Service. By default, Cisco Jabber assumes the default IM address scheme *UserID@Default_Domain*. If Directory URI is used, then additional configuration is required on the Cisco Jabber client to ensure that directory searches align with the Directory URI value.

  For example, if the IM address scheme is Directory URI and that is mapped to mail in Active Directory, then Jabber for windows directory searches against Active Directory must be configured to ensure that the mail field is used as the IM address when adding a contact. See the installation and configuration guide for your verison of Cisco Jabber for Windows for details.

  Note To configure the Directory URI IM address scheme for the Cisco Jabber client, you must manually edit a configuration file in xml format. The xml configuration file must be valid before you upload the file to the TFTP server. The Cisco Jabber client ignores invalid configuration files.

CLI changes

utils users validate

This command checks user records across all nodes and clusters in the deployment to identify duplicate or invalid userid or directory URI values.

utils users validate {**all**| **userid**| **uri**}

Syntax Description

Parameters	Description
all	Validate the userid and directory URI values for all users in the nodes and clusters.
userid	Validate the userid value for all users in the nodes and clusters.
uri	Validate the directory URI value for all users in the nodes and clusters.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence Service on Unified Communications Manager

IM and Presence Service Oracle Database Support

You can configure Oracle 11G, 10G and 9G as an external database to store information synchronized from the Cisco Unified Communications Manager IM and Presence Service.

Procedures

Install Oracle Database

Before You Begin

Read the security recommendations for the Oracle database in your Oracle documentation.

IM and Presence Service supports Oracle 11G, 10G and 9G.

Note Cisco recommends that an Oracle DBA install the Oracle server.

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

To install the Oracle database, refer to your Oracle documentation.

To create tablespace and a database user, connect to the Oracle database as sysdba:

```
sqlplus / as sysdba
```

Procedure

Step 1 Create tablespace.

Note The `DATAFILE` keyword of the `CREATE TABLESPACE` command tells Oracle where to put the tablespace's datafile.

a) Enter the following command:

```
CREATE TABLESPACE tablespace_name DATAFILE
'absolute_path_to_oracle_installation\oradata\database_name\datafile.dbf' SIZE 100M
AUTOEXTEND ON NEXT 1M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE
MANAGEMENT AUTO
```

- Replace *tablespace_name* with the tablespace name.
- Replace *absolute_path_to_oracle_installation* with the absolute path to where Oracle is installed. The entire path, including *datafile*.dbf, is enclosed in single quotation marks.
- Replace *database_name* with the name of your database folder.
- The *datafile*.dbf must be created in a folder under **`\oradata\`**, in this case the *database_name* folder.

- Replace *datafile*.dbf with the datafile name you want to create.

Step 2 Create a database user.

```
CREATE USER user_name IDENTIFIED BY "********" DEFAULT TABLESPACE tablespace_name TEMPORARY
TABLESPACE "TEMP" QUOTA UNLIMITED ON tablespace_name ACCOUNT UNLOCK
```

Step 3 Grant permissions to the database user.
The following example grants all permissions to a database user:

```
GRANT DBA TO user_name
```

The following examples grant limited permissions to the database user:

- `GRANT CREATE ANY VIEW TO user_name`
- `GRANT "CONNECT" TO user_name`
- `GRANT "RESOURCE" TO user_name`

Related Topics

Oracle Documentation

Prerequisite Configuration Tasks for Oracle

Before you configure IM compliance, make sure that you have performed the following tasks:

- Install the IM and Presence servers as described in the *Installing Cisco Unified Communications Manager*.
- Configure the IM and Presence servers as described in the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* .
- Set up the external database as described in the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* .

Support for Oracle

- In compliance with XMPP specifications, the IM and Presence server uses UTF8 character encoding. This allows the server to operate using many languages simultaneously and to display special language characters correctly in the client interface. If you want to use Oracle with the server, you must configure it to support UTF8.
- The value of the **NLS_LENGTH_SEMANTIC** parameter should be set to **BYTE**.
- To determine the tablespace available for your Oracle database, execute the following query as sysdba:

  SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USERNAME';

Set Up Oracle Database Entry

Perform this configuration on the publisher node of your IM and Presence Service cluster.

Before You Begin

- Install and configure the external database.
- Obtain the hostname or IP address of the external database.
- Retrieve the tablespace value. To determine the tablespace available for your Oracle database, execute the following query as sysdba:
  SELECT DEFAULT_TABLESPACE FROM DBA_USERS WHERE USERNAME = 'UPPER_CASE_USERNAME';

Procedure

Step 1 Select **Cisco Unified CM IM and Presence Administration** > **Messaging** > **External Server Setup** > **External Databases**.

Step 2 Select **Add New**.

Step 3 Enter the name of the database that you defined at external database installation, for example "tcmadb."

Step 4 Enter the tablespace value.

Step 5 Enter the username for the database user (owner) that you defined at external database installation, for example "tcuser."

Step 6 Enter and confirm the password for the database user, for example "mypassword."

Step 7 Enter the hostname or IP address for the external database.

Step 8 Enter a port number for the external database.
The default port number for Oracle (1521) will be pre-populated in the Port Number field. You can choose to enter a different port number if required.

Step 9 Select **Save**.

IM and Presence Service Support for Microsoft Lync Server 2013

IM and Presence Service supports Microsoft Lync Server 2013. When entering the Microsoft server type during federation configuration, you can enter either Microsoft Lync Server 2010 or 2013. For more information about Lync server support, see the *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager* and *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Feature Group Template Support for the User Synced From Directory

Cisco Unified Communications Manager, Release 10.0(1) provides Feature Group Template and Access Control Groups support for new users. The administrator can select both the Feature Group Template and Access Control Groups and integrate them with the new users that are synchronized from the LDAP directory.

Cisco Unified Communications Manager Administration Considerations

LDAP directory settings

The following table describes the LDAP directory settings.

Table 17: LDAP Directory Settings

Field		Description
Work Number	(drop-down list box)	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right. For the LDAP User field, choose one of the following values: • telephoneNumber • ipPhone
Title	title	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.

Field		Description
Mobile Number	mobile	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Home Number	homePhone	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Pager Number	pager	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Group Information		
Access Control Groups		Use this option to manage the Access Control Group to configure different levels of access for new users that were synchronized from the LDAP directory. Click the **Add to Access Control Group** button to open the Find and List Access Control Groups window. From the list, select one or more Access Control Groups for a user. Click the **Add Selected** button. The Find and List Access Control Groups window closes, and the Update Users Configuration window now shows the selected groups in the list box. To delete an existing Access Control Group, select the relevant Access Control Group from the list box. Click the **Remove from Access Control** button to complete the process. To add a new Access Control Group to the Find and List Access Control Groups window, use the following menu path: **User Management** > **User Settings** > **Access Control Group**
Feature Group Template		From the drop-down list box, select the Feature Group template to be associated with the new users that are synchronized from the LDAP directory. To create a Feature Group template that includes features such as mobility and IM and Presence, use the following menu path:**User Management** > **User/Phone Add** > **Feature Group Template** If you do not select a feature group template, a warning message displays as mentioned below: **Warning** If no template is selected, the new line features below will not be active. If you select a custom feature group template with no user profile, a warning message displays as mentioned below: **Warning** The selected Feature Group Template does not have a Universal Line Template configured. The new line features below will not be active.

End user settings

The following table describes the end user settings.

Table 18: End User Settings

Field	Description
Title	Enter the end user title.
Work Number	Enter the end user work number. You may use the following special characters: (,), and -.
Mobile Number	Enter the end user mobile number. You may use the following special characters: (,), and -.
Home Number	Enter the end user home number. You may use the following special characters: (,), and -.
Pager Number	Enter the end user pager number. You may use the following special characters: (,), and -.

Bulk Administration Considerations

User Update Settings

The following table provides descriptions for all possible fields when you update users with the Query option.

Table 19: Field Descriptions for Update Users

Field	Description
User Information	
Manager User ID	Enter manager user ID, up to 128 characters, for the user of this phone.
Department	Enter the department number, up to 64 characters, for the user of this phone.
Associated PC	This field, which is required for Cisco SoftPhone and Cisco Unified Communications Manager Attendant Console users, displays after you add the user.
User Locale	Choose the language and country set that you want to associate with this user from the drop-down list. Your choice determines which cultural-dependent attributes exist for this user and which language displays in the Cisco Unified Communications Manager user windows and phones.

Field	Description
Digest Credentials	When you configure digest authentication for phones that are running, Cisco Unified Communications Manager challenges the identity of the phone every time the phone sends a SIP request to Cisco Unified Communications Manager. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. Enter a string of up to 128 alphanumeric characters. For more information on digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, reenter the credentials in this field.
Service Setting	
UC Service Profile	Select a UC service profile from the drop-down list box to associate with end users. **Note** Use the **User Management** > **User Settings** > **Service Profile** menu to set up service profiles for end users.
Include meeting information in Presence	Check this check box to enable the end user to include meeting and calendar information in IM and Presence Service. The end user must be on the home cluster and have IM and Presence enabled. Also ensure that an Exchange Presence Gateway is configured on the Cisco Unified Communications Manager IM and Presence Service server.
Include Meeting Information in Presence (Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)	Check this check box to create a sync between CUCM IM and Presence server so that it can include the meeting information under the Presence feature. **Note** You can only access this field if Home Cluster and Enable User for Unified CM IM and Presence is enabled.
Extension Mobility	
BLF Presence Group	From the drop-down list, choose the BLF presence group that watches the status of the directory number, the presence entity. For information on the BLF Presence feature, see the *Cisco Unified Communications Manager Features and Services Guide*.

Field	Description
SUBSCRIBE Calling Search Space	All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. The SUBSCRIBE Calling Search Space determines how Cisco Unified Communications Manager routes the Presence subscription requests that come from the end user. Use the **Call Routing** > **Class Control** > **Calling Search Space** menu to configure a calling search space specifically for this purpose . For information on how to configure a calling search space, see the *Cisco Unified Communications Manager Administration Guide.*
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be checked as long as at least one associated device specifies a combination of device type and protocol that CTI supports.
Enable Extension Mobility Cross Cluster	Check this check box to enable the Extension Mobility Cross Cluster CSS setting that gets used as the device CSS of the remote phone when the user selects this device profile during EMCC login.
Mobility Information	
Enable Mobility	Check this check box to activate Mobile Connect, which allows the user to manage calls by using a single phone number and to pick up and manage calls on the desk phone and mobile phone.
Enable Mobile Voice Access	Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities.
Maximum Wait Time for Desk Pickup	Enter the maximum wait time, up to 5 numerals, for this user. This indicates the maximum time that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desk phone.
Remote Destination Limit	Enter the maximum number of phones, up to 2 numerals, to which the user is permitted to transfer calls from the desk phone.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Update User Information in Cisco Unified Communications Manager Directory

You can update a group of user records in the Cisco Unified Communications Manager directory.

Before You Begin

You must have a .csv data file with updated user information.

Procedure

Step 1 Choose **Bulk Administration** > **Users** > **Update Users** > **Custom File**.
The **User Update Configuration** window appears.

Step 2 From the **File Name** drop-down list box, choose the .csv data file that you created for this bulk transaction.

Note Click **View File** to view the uploaded .csv data file.

Click **View Sample File** to view a sample .csv data file.

Step 3 From the **User Template Name** drop-down list box, choose the user template that you created for this bulk transaction.

Step 4 In the **Value for fields to be ignored** field, enter the symbol that you want to tell Unified CM Bulk Administration Tool to retain the value that was previously stored in the DC directory.

Note The value that you enter in the .csv file for updating users overrides the values that are provided in the user template.

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Choose a method to update user records. Do one of the following:

- Select **Run Immediately** to update user records immediately.
- Select **Run Later** to insert the user records at a later time.

Step 7 To create a job for updating the user records, click **Submit**.
To schedule or activate this job, use the Job Scheduler option in the Bulk Administration main menu.

IPMA and Softkey Template Support

For Unified Communications Manager, Release 10.0(1) and later, the IP Manager Assistant feature is managed by application on the phone. This is not modified by user information and updates to user settings.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

A list of phones supporting this feature is available in the *Cisco Unified Communications Manager Assistant User Guide*.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

IPv6 Enterprise Parameters

The following new IPV6 enterprise parameters have been added (**System** > **Enterprise Parameter Configuration**):

- Allow Duplicate Address Detection
- Accept Redirect Messages
- Reply Multicast Echo Request

Cisco Unified Communications Manager (Unified Communications Manager) also provides an option to configure these parameters in the Common Device Configuration window.

Cisco Unified Communications Manager Administration Considerations

The following fields have been added to the Common Device Configuration window (**Device** > **Device Settings** > **Common Device Configuration**):

- Allow Duplicate Address Detection: Select On, Off, or Default from the drop-down list box.
- Accept Redirect Messages: Select On, Off, or Default from the drop-down list box.
- Reply Multicast Echo Request: Select On, Off, or Default from the drop-down list box.

If you set these parameters as 'Default', the configuration file of IP Phones will pick up the values of these parameters from the enterprise parameters. If you set these parameters as 'On' or 'Off', the configuration file will consider these values.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

IPv6: Mobility Support

Cisco Unified Communications Manager (Unified Communications Manager), Release 10.0(1) supports IPv6 addressing from mobile phones. Cisco Unified Mobility does not support IPv6 for mobile clients that use Cisco Unified Mobility Advantage to connect to Unified Communications Manager for Dial via Office or midcall features because Cisco Unified Mobility Advantage does not support IPv6 addresses.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

IPv6-Only and Dual Stack SIP Endpoints

Cisco Unified Communications Manager Administration Considerations

Administrators can configure IPv6-only or dual stack addressing for SIP endpoints.

IP Phones or other endpoints that use Session Initiation Protocol (SIP) can register with Cisco Unified Communications Manager (Unified Communications Manager) using an IPv6 address. After these phones have registered with Unified Communications Manager, they can operate in IPv6 mode, IPv4 mode, or in dual stack mode. Administrators can specify the order of address preference for these phones by using the IP Addressing Mode Preference for Signaling setting, which is located on the Common Device Configuration panel.

This feature also adds support for all media types, including audio and video, for calls originating from and terminating on IPv6 SIP line devices located in the same cluster, or in different clusters connected by SIP trunks.

You can use the ANAT Enabled checkbox, which is selected by default, to enable or disable this feature. The checkbox was previously located on the SIP Profile panel, and is now located on the SIP Trunks configuration panel.

The following phones support IPv6 and dual stack addressing:

- Cisco Unified SIP Phone 3905
- Cisco Unified IP Phone 7821
- Cisco Unified IP Phone 7841
- Cisco Unified IP Phone 7845
- Cisco Unified IP Phone 7861
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

The following SIP Telepresence endpoints support IPv6 and dual stack addressing:

- C-series (C90, C60, C40, C20)

- Profile-series
- SX-series (SX20)
- MX-series (MX200, MX300)
- EX-series (EX60, EX90)

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

iX Channel MTP Transparency

iX channel over MTP/RSVP provides a simple, reliable and secure channel for multiplexing multiple application layer protocols. The transport used for iX channel is User Datagram Protocol (UDP). To provide a reliable channel, iX channel over MTP/RSVP uses UDP Based Data Transfer Protocol (UDT) over UDP. To provide security, Transportation Layer Security (TLS) is run over the reliable transport provided by UDT. iX channel over MTP/RSVP provides a multiplexer, which uses a simple type-length-value scheme that enables the channel to support application layer protocols of many types, including XML and binary protocols.

iX channel over MTP/RSVP can be negotiated and set up using the Session Description Protocol (SDP) and the Offer/Answer model. An iX channel extends SDP to support new attribute mapping for the protocols to be multiplexed.

In this release of Unified Communications Manager, the iX channel over MTP/RSVP feature supports Media Termination Point (MTP) cases. MTP is needed for Early Offer (EO) trunk, Trusted Relay Point (TRP) configuration, Dual tone multi frequency (DTMF) or IP address translations, and RSVP feature calls.

To support iX channels in MTP cases, Unified Communications Manager must be configured to invoke MTPs that are allocated from the IOS router, which must be running version 15.2T or above.

Note Unified Communications Manager will only support iX channel negotiation when a video channel has been established.

For RSVP and E2E RSVP calls, Unified Communications Manager supports iX channel negotiation and allows iX channels to pass through the RSVP agents. Unified Communications Manager does not need to reserve any bandwidth for iX channels in RSVP agents. RSVP will continue to reserve the bandwidth for audio and the primary video channel only.

Cisco Unified Communications Manager Administration Considerations

To enable the feature on a SIP trunk device, choose **Device > Device Settings > SIP Profile**. Select the **Allow iX Application Media** checkbox.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Locale Installer Modifications to Package New Locale Prompts with TAPS Plugin

For Cisco Unified Communications Manager, Release 10.0(1) and later, the Tool for Auto-Registered Phones Support (TAPS) automatically transfers the user-locale prompts from Cisco Unified Communications Manager to Cisco Unified Contact Center Express.

You can only transfer a maximum of 20 languages as user-locale prompts in Cisco Unified Communications Manager.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Mobility Billing

The following call detail record (CDR) fields have been added for the 10.0(1) release for calls that invoke a mobility feature. If the call does not invoke a mobility feature, these fields remain empty:

- MobileCallingPartyNumber
- FinalMobileCalledPartyNumber
- OrigMobileDeviceName
- DestMobileDeviceName
- OrigMobileCallDuration
- DestMobileCallDuration
- MobileCallType

MobileCallType Values

The MobileCallType CDR field has been added to identify the mobility feature that is invoked.

The following table displays the field values for the MobilityCallType CDR field. If a single call invokes more than one mobility feature, the value of the MobileCallType field will represent the integer values added together. For example, if a call uses the Mobile Connect feature and then invokes Hand-Out, the mobile call type will be 132 (8 + 128).

Table 20: MobilityCallType CDR Field Values

Mobility Feature	MobileCallType Value
Nonmobility call	0
Dial via Office Reverse Callback	1
Dial via Office Forward	2
Reroute Remote Destination Call to Enterprise Network	4
Mobile Connect	8
Interactive Voice Response	16
Enterprise Feature Access	32
Hand-In	64
Hand-Out	128
Redial	256
Least Cost Routing with Dial via Office Reverse Callback	512
Least Cost Routing with Dial via Office Forward	130
Send Call to Mobile	2048
Session Handoff	4096

Last Redirect Reason

In legacy deployments prior to 10.0(1), CAR uses the LastRedirectReason field to identify the mobility call type.

The following table shows the Mobility values for LastRedirectReason.

Table 21: Mobility Values for the LastRedirectReason Field

Mobility Feature	LastRedirectReason Value
Hand-In	303
Hand-Out	319
Mobile Connect	335
Redial	351

Mobility Feature	LastRedirectReason Value
Interactive Voice Response	399
Dial via Office Reverse Callback	401
Enterprise Feature Access	402
Session Handoff	403
Least Cost Routing with Dial via Office Forward	404
Least Cost Routing with Dial via Office Reverse Callback	405
Send Call to Mobile	415
Reroute Remote Destination Call to Enterprise Network	783

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

For examples of CDRs that are produced for calls that invoke specific mobility features, see the "CDR Examples" chapter of the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Multiple Codecs in SDP Answer

This option applies when incoming SIP signals do not indicate support for multiple codec negotiation and Cisco Unified Communications Manager can finalize the negotiated codec.

When this check box is checked, the endpoint behind the trunk is capable of handling multiple codecs in the answer SDP.

For example, an endpoint that supports multiple codec negotiation calls the SIP trunk and Cisco Unified Communications Manager sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation.

In this case, Cisco Unified Communications Manager identifies the trunk as capable of multiple codec negotiation and sends SIP response messages back to both endpoints with multiple common codecs.

When this check box is left unchecked, Cisco Unified Communications Manager identifies the endpoint behind the trunk as incapable of multiple codec negotiation, unless indicated otherwise by SIP contact header URI. Cisco Unified Communications Manager continues the call with single codec negotiation.

Cisco Unified Communications Manager Administration Considerations

The following check box has been added to the **SIP Profile** settings window: **Allow Multiple Codecs in Answer SDP**.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Non-SRTP Call Blocking

The Non-SRTP Call Blocking feature enables you to block unencrypted (non-SRTP) calls. The calls are blocked if either the called party or the calling party is not encrypted. A new service parameter Block Unencrypted Calls has been added to enable this feature. By default, this service parameter is set to False.

You must set this service parameter to True for blocking non-SRTP calls. When this service parameter is set to True and any one or each of the endpoints is unencrypted, the calls are blocked and Reorder tone is played on the endpoints. A perform counter gets incremented for each blocked call. An alarm is also raised for all the blocked calls so that the administrator can take appropriate action.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Plug and Play Feature

Cisco Unified Communications Manager Administration Considerations

Currently, all the IP phones are automatically registered with Cisco Unified Communications Manager. With the help of LDAP Sync and Bulk administration tool, a number of IP phones can be assigned to the users on the Cisco Unified Communications Manager. This feature provides an easy way to assign the auto-registered IP phones to the users.

A new menu item is added to Cisco Unified Communications Manager Administration under the User Management menu; choose **User Management** > **Self-Provisioning**.

For Auto-Registration settings, the options **Partition** and **External Phone number Mask** are replaced by **Universal device Template** and **Universal Line Template**.

Note When you upgrade a previous release Cisco Unified Communications Manager to Release 10.0, the Cisco Unified Communications Manager will create a Universal Device Template and a Universal Line Template which will retain the previous configurations for Auto-Registration settings (Partition and External Phone Number Mask). After the upgrade, the Cisco Unified Communications Manager populates the Cisco Unified Communications Manager name for the Universal Device Template and a Universal Line Template and configures the same values for Auto-Registration settings.

For LDAP Directory settings, the following new fields are introduced.

Field	Description
Apply mask to synced telephone numbers to create a new line for inserted users	Check the check box to apply mask to the synced telephone number of the user. Enter a mask value in the **Mask** text box. The **Mask** can contain one to twenty four characters including numbers (0-9), X, and x. It must include at least one x or X. For example, if you set the mask as 11XX for the user with a telephone number 8889945, after the mask is applied, 1145 becomes the primary extension of the user.
Assign new line from the pool list if one was not created based on a synced LDAP telephone number	Check the check box to assign a new line from the DN pool list.
Next Candidate DN	Displays the next probable DN that will be assigned to the user. The DN from the next DN pool is displayed only after all the DNs from the first DN pool are assigned. **Note** The **Next Candidate DN** displays only when you check the **Assign new line from the pool list if one was not created based on a synced LDAP telephone number** check box.
Add DN Pool	By default, only one DN pool is available. Click this option to add more DNs to the DN pool. The **DN Pool Start** and **DN Pool End** values must conform to the following requirements: • Must be a number and can contain one to twenty characters • **DN Pool End** must be greater than **DN Pool Start** • **DN Pool Start** and **DN Pool End** must not be null • DN range must be less than 10,000,000 Enter the **DN Pool Start** and **DN Pool End** values in the text box. You can reorder the DN pool to prioritize the DNs that you want to assign. If the length of the start and end DN pools are different, an error message displays: `The DNs length must be identical.` You can create only three DN pools.

Bulk Administration Considerations

The Import/Export support is extended to Self-Provisioning, where the administrators can export Self-Service User ID that is generated when a user is assigned an IP phone. The BAT spreadsheet now includes the Self-Service User ID for User Data option.

CDR/CAR Considerations

No Changes.

IP Phones Considerations

All phone models that support Auto-Registration supports Self-Provisioning. The Self-Provisioning process for desk phones, such as Jabber and Zydeco phones are different, compared to Self-Provisioning for IP phones. Self-Provisioning is also supported on analog phones.

RTMT Considerations

No Changes.

Security Considerations

No Changes.

Serviceability Considerations

This feature introduces a new Self-Provisioning Interactive Voice Response (IVR). When you dial the CTI RP DN, that is configured on the Self-Provisioning page, from an extension of a user that uses the IVR service, the phone connects to the Self-Provisioning IVR application and prompts you to provide the Self-Service credentials. Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phones to the users.

You can activate, deactivate, or restart the Self-Provisioning IVR service from the Serviceability page. By default, this service is deactivated. You can still configure Self-Provisioning on the Administration page even if the service is deactivated, but you cannot assign IP phones to users using the IVR service.

To enable Self-Provisioning IVR service, you must also enable Cisco CTI Manager service.

Remote Lock/Wipe

Cisco Unified Communications Manager Administration Considerations

Remote Lock

In Unified Communications Manager, some phones can be locked remotely. When a remote lock is performed on a phone, the phone cannot be used until it is unlocked.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

Remote Wipe

In Unified Communications Manager, some phones can be wiped remotely. When a remote wipe is performed on a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the Remote Wipe feature, a **Wipe** button appears in the top right hand corner.

Phone Wipe/Lock Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped.

Bulk Administration Considerations

- **Wipe or Lock Phones Using Query**

  You can create a query to locate phones that you want to wipe and/or lock.

- **Wipe or Lock Phones Using Custom File**

  You can create a custom file of phones that you want to wipe and/or lock using a text editor.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedures

Remotely Lock a Phone

Follow these steps to remotely lock a phone.

Procedure

Step 1 Choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 Enter search criteria and click **Find** to locate a specific phone.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote lock.

The **Phone Configuration** window displays.

Step 4 Click **Lock**.
If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**. A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

Remotely Wipe a Phone

Follow these steps to remotely wipe a phone.

⚠ **Caution** This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

Procedure

Step 1 Choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 Enter search criteria and click **Find** to locate a specific phone.
A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote wipe.
The **Phone Configuration** window displays.

Step 4 Click **Wipe**.
If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**. A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

Display Phone Wipe/Lock Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

Procedure

Step 1 Choose **Device** > **Phone**.
The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select the Phone Lock/Wipe Report from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Lock and Wipe Devices window displays.

Step 3 To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.
To filter or search records

a) From the first drop-down list box, select the device operation type(s) to search.
b) From the second drop-down list box, select a search parameter.
c) From the third drop-down list box, select a search pattern.
d) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 Click **Find**.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Wipe or Lock Phones Using Query

Caution The wipe operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

Procedure

Step 1 Choose **Bulk Administration** > **Phones** > **Wipe and Lock Phones** > **Query**.
The **Wipe and Lock Phones Configuration** window displays.

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

- Device Name
- Description
- Directory Number
- Calling Search Space
- Device Pool
- Device Type
- Call Pickup Group
- LSC Status

- Authentication String
- Device Protocol
- Security Profile
- Common Device Configuration

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

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

Step 3 Specify the appropriate search text, if applicable.

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

Step 4 To further define your query, you can choose AND or OR to add multiple filters and repeat Step 2 and Step 3.

Step 5 Click **Find**.
A list of discovered templates displays by

- Device Name
- Description
- Device Pool
- Device Protocol
- Status
- IP Address

Step 6 From the list of records, click the device name that matches your search criteria.

Step 7 Click one of the following options:

- Lock—To lock the phones
- Wipe—To wipe the phones
- Wipe and Lock—To wipe and lock the phones

Note If a phone does not support the functionality you have chosen, the transaction will fail for that phone. It will also fail if the functionality has already been requested for the phone.

Step 8 In the Job Information area, enter the Job description.

Step 9 Choose an insert method. Do one of the following:

a) Click **Run Immediately** to wipe or lock phones immediately.

b) Click **Run Later** to wipe or lock phones at a later time.

Step 10 To create a job for locking and/or wiping the phones, click **Submit**.
To schedule and/or activate this job, use the **Job Configuration** window.

Wipe or Lock Phones Using Custom File

You can create a custom file of phones that you want to wipe and/or lock using a text editor. You can use either device names or directory numbers in the custom file.

Before You Begin

Caution The wipe operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

1 Create a text file that lists one of these details for the phones that you want to wipe and/or lock:

- Device names
- Description
- Directory numbers

Note Put each item on a separate line in the text file.

2 Upload the file to the first node of Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Bulk Administration** > **Phones** > **Wipe and Lock Phones** > **Custom File**.
The **Wipe and Lock Phones Configuration** window displays.

Step 2 In the **Update Phones where** drop-down list box, choose the type of custom file that you have created from one of the following criteria:

- Device Name
- Directory Number
- Description

Step 3 In the list of custom files, choose the filename of the custom file for this update and then click **Find**.
Caution If no information is entered into the query text box, the system wipes or locks all phones.

Step 4 Click one of the following:

- Lock—To lock the phones

- Wipe—To wipe the phones
- Wipe and Lock—To wipe and lock the phones

Note If a phone does not support the functionality you have chosen, the transaction will fail for that phone. It will also fail if the functionality has already been requested for the phone.

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Choose an insert method. Do one of the following:

a) Click **Run Immediately** to wipe or lock phones immediately.
b) Click **Run Later** to wipe or lock phones at a later time.

Step 7 To create a job for locking and/or wiping the phones, click **Submit**.
To schedule and/or activate this job, use the **Job Configuration** window.

Removal of ASCII Fields

Cisco Unified Communications Manager Administration Considerations

The following ASCII fields have been removed from the Unified Communications Manager interface:

- ASCII Label
- ASCII Display Name
- ASCII Service Name

Bulk Administration Considerations

The following ASCII fields have been removed from the Bulk Administration Tool (BAT) interface:

- ASCII Label
- ASCII Line Text Label

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Routing Enhancements

Cisco Unified Communications Manager Administration Considerations

Directory number settings

The following table describes the fields that are available in the Directory Number Configuration window.

Table 22: Directory Number Settings

Field	Description
Directory Number Information	
Urgent Priority	If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call to the device associated with the directory number until the interdigit timer expires (even if the directory number is a better match for the sequence of digits dialed as compared to the overlapping pattern). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately to the device associated with the directory number. By default, the Urgent Priority check box is unchecked.

Translation pattern settings

The following table describes the available fields in the Translation Pattern Configuration window.

Table 23: Translation Pattern Settings

Field	Description
Pattern Definition	

Field	Description
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call, check the Use Originator's Calling Search Space check box. When you check this check box, it disables the Calling Search Space drop-down list box. When you save the page, the Calling Search Space box is grayed out and set to <None>. If the originating device is a phone, the originator's calling search space results from the device calling search space (configured on the Phone Configuration window) and line calling search space (configured on the Directory Number Configuration window). Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you check the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you uncheck the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used.
Do Not Wait For Interdigit Timeout On Subsequent Hops	When you check this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches. Whenever you check the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops unchecked.

Call Control Discovery feature parameters

To access the feature parameters that support the call control discovery feature, choose **Call Routing** > **Call Control Discovery** > **Feature Configuration**. For additional information, you can click the question mark help in the Feature Configuration window.

The following table describes the feature parameters for the call control discovery feature.

Table 24: Call Control Discovery Feature Parameters

Feature Parameter	Description
Set Urgent Priority for Fixed-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern (when the fixed-length learned pattern is a better match for the sequence of digits dialed as compared to the overlapping route pattern configured). If the parameter is set to True, Cisco Unified Communications Manager does not wait for the interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager learns the pattern +44987XXX for routing the calls to another Cisco Unified Communications Manager and there is also a route pattern configured as \+44! for routing the calls to the PSTN destination. If this parameter is set to False and +44987127 is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager (this interdigit timer allows user to dial more digits after +44987127 to reach the PSTN destination). If this parameter is set to True and +44987127 is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

Feature Parameter	Description
Set Urgent Priority for Variable-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to True, Cisco Unified Communications Manager does not wait for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager has translation pattern 9011.!# configured. This translation pattern strips predot digits and the trailing # character and adds the prefix +55 to the dialed digits. Cisco Unified Communications Manager also learns pattern \+55.! for routing the calls to another Cisco Unified Communications Manager. If this parameter is set to False and 9011234567# (resultant digits = +55234567) is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager. If this parameter is set to True and 9011234567# (resultant digits = +55234567) is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

The following table describes the settings for SIP trunks.

Table 25: SIP Trunk Settings

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete the prefix for unknown number type for the called party, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for the Prefix field for unknown number type, click Default Prefix Settings.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device.

Field	Description
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.
Outbound Calls	
Called Party Transformation CSS	This settings allows you to send the transformed called party number in INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This settings allows you to send the transformed calling party number in INVITE message for outgoing calls made over SIP Trunk. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number that is sent from Cisco Unified Communications Manager side in outgoing reINVITE / UPDATE messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table describes the trunk settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

Table 26: H.225 and Intercluster Trunks Settings

Field	Description
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table lists configuration settings for H.323 gateways.

Table 27: H.323 Gateway Configuration Settings

Field	Description
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Call Routing Information - Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Note** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table provides detailed descriptions for Digital Access PRI port configuration settings.

Table 28: Digital Access PRI Port Settings

Field	Description
Call Routing Information - Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. [For PRI DMS - 100 and DMS - 200]. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number sent from Cisco Unified Communications Manager in another format, such as a DID or E.164 number. **Note** You can configure a Connected Party Transformation CSS only when you select one of the following protocols that support Connected Number Information Element: • For T1 PRI : ◦ PRI DMS - 100 ◦ PRI DMS - 250 ◦ PRI ISO QSIG T1 • For E1 PRI : ◦ PRI ISO QSIG E1 For other protocol types, Connected Party Transformation CSS is grayed out. Using this setting, Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of CONNECT message for basic call. For PRI DMS - 100 and DMS - 250 protocols , Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of NOTIFY message for inbound calls after redirection. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

The following table provides detailed descriptions for BRI port configuration settings.

Table 29: BRI Port Configuration Settings

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation

Field	Description
	pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Add Route Groups to Route List

Note When you configure the Local Route Group feature, add the route groups to the route list by selecting those local route group names that are appended with the Local Route Group tag that appears in the drop-down list box.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Local Route Group Names Setup

About Local Route Group Names Setup

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Route/Hunt** > **Local Route Group Names** menu path to configure local route group names.

A local route group name is a unique name that you assign to a local route group in the Local Route Group Names window. The Local Route Group Names window allows you to add and configure multiple local route group names that you can customize and associate with route groups for a given device pool.

Note From Cisco Unified Communications Manager Release 10.0(1), a given device pool supports multiple local route groups.

Local Route Group Names Settings

The following table describes the available fields and buttons in the Local Route Group Names window.

Table 30: Local Route Group Names Settings

Field or Button	Description
Name	Enter a unique local route group name in this required field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscores (_). **Note** The Standard Local Route Group entry in the Name field is a default entry. It is populated from pre-10.0(1) release input. This field is editable. It allows you to change the name to a name of your choice. **Note** The Device Pool Configuration window under **System** > **Device Pool** displays the local route group name entries as labels under Local Route Group Settings.
Description	(Optional) Enter a description that will help you to distinguish between local route group names. You can change the description if required. The description can comprise up to 100 alphanumeric characters except the following characters: ampersand (&), double quotation marks ("), angle brackets (<>), and percent (%).
Add Row	Click this button to add new local route group names. This button adds an empty row below the previous row entry. Enter the name and description of the local route group that you want to add to this row. To delete an existing local route group name, click the **Minus Sign (-)** button at the right corner of the relevant row. Click **Save** to confirm the process. **Note** By default, the **Minus Sign (-)** button in the first row is inactive. **Note** You can delete an existing local route group name only if it does not have any dependency on any device pool or route list. To delete an existing local route group, you must first find the associated device pools as well as the route lists from the dependency record, disassociate them, and then delete the local route group name.
Save	Click this button to save the local route group name entries.

SAML Single Sign On

The Security Assertion Markup Language (SAML) Single Sign On feature allows end users to log into a Windows client machine and then access certain Cisco Unified Communications Manager applications without logging in again.

After you enable SAML Single Sign On (SSO), users are able to access the following web applications without logging in again:

- Cisco Unified Communications Manager Administration
- Cisco Unified Reporting
- Cisco Unified Serviceability

If the Windows desktop authentication for SSO is configured for an end user, the end user is able to access all the above web applications without logging in again. However, if the Windows desktop SSO authentication is not configured, when the end users attempt to log into a SAML-enabled web application, they are redirected to their configured Identity Provider (IdP) to enter the authentication details. After successful authentication by the IdP, the web browser redirects the users to the web application that they were trying to access.

Note Local end users and applications users cannot access SAML SSO-enabled web applications.

Cisco Unified Communications Manager Administration Considerations

For this feature, the following new GUI path has been added that allows you to enable SAML SSO:

System > **SAML Single Sign On**

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure

Enable SAML SSO

Note The Cisco CallManager Admin, Cisco Unified CM IM and Presence Administration, Cisco CallManager Serviceability, and Cisco Unified IM and Presence Serviceability services are restarted after enabling or disabling SAML SSO.

Perform the following steps to enable SAML SSO:

Before You Begin

Ensure that the following prerequisites are met before proceeding with the steps:

- The end-user data is synchronized to the Cisco Unified Communications Manager database.
- Verify that the Cisco Unified CM IM and Presence Cisco Sync Agent service has completed data synchronization successfully. Check the status of this test by choosing **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**. The "Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)" test indicates a "Test Passed" outcome if data synchronization has completed successfully.
- At least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified Administration.

  Note For more information about synchronizing end-user data and adding LDAP-synchronized users to a group, see the "System setup" and "End user setup" sections in the *Cisco Unified Communications Manager Administration Guide*.

- OpenAM SSO (**Cisco Unified OS Administration** > **Security** > **Single Sign On** or **Cisco Unified IM and Presence OS Administration** > **Security** > **Single Sign On**) is disabled on all the nodes. For information about OpenAM SSO, see Single Sign-On and the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, click **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO**.
A warning message is displayed to notify you that all server connections will be restarted.

Step 3 Click **Continue**.
A dialog box that allows you to import IdP metadata displays. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.
After you install the server metadata on the IdP server, you must run an SSO test to ensure that the metadata files are correctly configured.

Step 9 Click **Next** to continue.

Step 10 Select an LDAP-synced user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.
The IdP login window displays.

Note You cannot enable SAML SSO until the Run Test succeeds.

Step 12 Enter a valid username and password.
After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails or takes more than 60 seconds to authenticate, a "Login Failed" message is displayed on the IdP login window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, repeat Steps 11 and 12.

Step 13 Click **Finish** to complete the SAML SSO setup.
SAML SSO is enabled and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.

Security-By-Default Enhancements

Security-by-Default (SBD) is a feature that allows Cisco Unified Communications Manager users to benefit from security features out of the box without the user having to perform configuration tasks.

SBD leverages the ITL file, which is a digitally signed file that contains all Unified Communications Manager node certificates (including TVS) that endpoints can trust.

The SBD enhancements address the issues and gaps that can lead to phones getting locked and customers not having to delete the ITL file either manually from the phones or by using third party developed tools.

In Unified Communications Manager 10.0(1), a new ITL reset private key called ITLRecovery is regenerated and is accessible from the Certificate Management interface.

The ITL reset certificate is pushed into the database with SAST role, which allows TFTP nodes to find this certificate when they build the ITL file. TFTP nodes then include this record in the ITL file.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

When phones are in a locked state and they are not accepting any ITL or configuration changes from their Unified Communications manager cluster, a new CLI command **utils ITL reset** can be used to create a special ITL Recovery ITL file. This process takes the existing ITL file from the publisher node, strips the signature of the ITL file and signs the contents of the ITL file again with the unlocked reset ITL Recovery private key.

The new ITL file is served to the TFTP directories on all the active TFTP nodes in the cluster. TFTP services are restarted. After this command is run successfully, the administrator must manually restart all the phones from the GUI. See "Perform bulk reset of ITL file."

Note For the bulk ITL file reset to work, the ITL Recovery certificate and key need to be available. You must back up this file.

Serviceability Considerations

No changes.

Procedure changes

Perform Bulk Reset of ITL File

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a bulk reset of the Identity Trust List (ITL) file with the CLI command **utils itl reset**. This command generates a new ITL recovery file.

Tip Whenever you perform a fresh installation of Unified Communications Manager, export the ITL key as soon as possible and perform a backup through the Disaster Recovery System.

The CLI command to export the ITL recovery pair is as follows:

file get tftp *ITLRecovery.p12*
You will be prompted to enter the SFTP server (where the key will be exported) and password.

Before You Begin

Make sure you perform this procedure on the Cisco Unified Communications Manager publisher.

If needed, export the key from the publisher.

Procedure

Step 1 Perform one of the following steps:

- Run **utils itl reset localkey**.
- Run **utils itl reset remotekey**.

For **utils itl reset localkey**, the local key resides on the publisher. This step generates a new ITL file by taking the existing file on the system and replacing the signature of that file with the recovery key signature. The key is then copied to the TFTP servers in the cluster.

Step 2 Run **show itl** to verify that the reset was successful.

Step 3 From Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**

Step 4 Select **Reset**.
The devices restart. They are ready to download the ITL file that is signed by the ITLRecovery key and accept configuration files.

Step 5 Restart the TFTP service and restart all devices.
The devices download the ITL file that is signed with the TFTP key and register correctly to Unified Communications Manager again.

CLI changes

utils itl reset

This command is used when endpoints are unable to validate their configuration files.

utils itl reset {**localkey|** **remotekey**}

Syntax Description

localkey	Generates a new ITL file by taking the existing ITL file on the publisher. The command replaces the signature of that ITL file and signs the new ITL file with the ITL recovery key.
remotekey	Generates a new ITL file after importing the PKCS 12 bag that contains the recovery certificate key pair from the remote location. It then signs the newly generated ITL file with the recovery private key. **remotekey** has the following parameters: • IP address or hostname • User ID • ITLRecovery.p12

Command Modes

Administrator (admin:)

Usage Guidelines

Note You must run this command on the Unified Communications Manager publisher node.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example

```
admin:utils itl reset

Name is None


Generating the reset ITL file.....

The reset ITL file was generated successfully

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

====================

se032c-94-42

=====================

Number of Active TFTP servers in the cluster : 1

Transferring new reset ITL file to the TFTP server nodes in the cluster.........
```

```
Successfully transferred reset ITL to node se032c-94-42
```

Additional information

Proxy TFTP and Security

Endpoints in a Cisco Unified Communications Manager cluster are configured with Proxy TFTP (for example, through Dynamic Host Configuration Protocol, or DHCP). Proxy TFTP can find the target cluster of the endpoint.

Note Cisco recommends that you keep the Proxy TFTP on the current release while you upgrade the rest of the clusters, as well as have a combination of nonsecure and mixed-mode clusters.

The Proxy TFTP server does not have to be on the highest Unified Communications Manager release, and clusters in a Proxy TFTP deployment can be either nonsecure or in mixed-mode.

Proxy TFTP can find the target cluster of endpoints because the MAC address of the endpoints is part of the filename in the TFTP GET request (for example, `SEP001956A3A472.cnf.xml.sgn`). Proxy TFTP discovers the target in the following way:

1. Proxy TFTP polls all the clusters that it controls for the requested file, starting from its own database.
2. The cluster where the endpoint is configured returns the file.
3. The locale and ring list file requests do not contain a MAC address, so Proxy TFTP returns its own copies of these files.

Note The locale and ring list files are backward compatible for Unified Communications Manager releases.

When Security-by-Default (SBD) was introduced for Unified Communications Manager, Proxy TFTP (and TFTP servers in general) served both signed and nonsigned requests.

If the home cluster of an endpoint does not accept the ITL file request, the endpoint requests a default ITL file which the Proxy TFTP serves. After the endpoint receives the configuration file from its home cluster, the endpoint cannot validate the signature, because the endpoint has the ITL file from the Proxy TFTP and not its home cluster.

To address this issue, the TFTP service returns a *file not found* message when the default ITL file is requested.

10.0(1) Proxy TFTPs perform the following steps for signing files and serving them to endpoints:

- Automatically discover the cluster in the deployment that is on the highest release
- Get the locale and ring list files from the cluster
- Strip the signature of the locale or ring list file
- Sign the files with their own TFTP private key before serving them to endpoints that are requesting the files

Self Care User Options

Unified Communications Self Care Portal is a new web-based user interface that phone users can access to set up user settings for their Cisco Unified IP Phones. Unified Communications Self Care Portal replaces the Cisco Unified CM User Options interface from the last release.

For details, see the *Cisco Unified Communications Self Care Portal User Guide*.

Cisco Unified Communications Manager Administration Considerations

As with Cisco Unified CM User Options from the last release, administrators can set enterprise parameters in Cisco Unified Communications Manager that control which settings are available for users to configure in the Self Care interface. These enterprise parameters appear in the Enterprise Parameter Configuration window under the User Options Parameters heading.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Self-Provisioning

Self-Provisioning for End Users and Administrators

The Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.

This feature enhances the out-of-box experience for end users by allowing them to directly add their desk phone or soft client without contacting the administrator. It simplifies administrator deployments by allowing them to add desk phones on behalf of an end user. The feature lets administrators and users deploy a large number of devices without interacting directly with the Cisco Unified Communications Manager Administration GUI, but from the device itself. The feature relies on the administrator preconfiguring a number of templates and profiles, so that when the phone attempts to self-provision, the necessary information is available in the system for it to create a new device.

Note Self-provisioning is not supported for secured endpoints.

There are two levels of configuration for Self-Provisioning:

- The system level
- The user level

You can set up this feature at the system level from Cisco Unified Communications Manager Administration under the **User Management** > **Self-Provisioning** menu.

To set up this feature, you can select one of the following modes:

- **Secure Mode**
    - Administrators can provision devices on behalf of end users
    - End users can provision devices with their credentials
- **Non-Secure Mode**
    - End users/administrators can enter Self-Service ID for the device that is being provisioned.

With appropriately configured User Profiles, end users can provision their own devices. These User Profiles may be shared by a group of users that share the same characteristics. The User Profile contains the following settings:

- Universal Device Templates
- Universal Line Template
- End user Self-Provisioning settings

Note The administrator can set any User Profile as the system default.

In order to allow a user to provision a new device using Self-Provisioning, the user must meet the following criteria:

If you do not configure a UDT in the User Profile, user assignment fails and plays the following error message on the phone: `This device could not be associated to your account. Please contact the System administrator to complete provisioning.`

- Self-Provisioning must be enabled for the end user.

Note Self-Provisioning must be enabled even if the administrator performs device self-provisioning on behalf of the user.

- The user must have a primary extension.
- The user must have the appropriate universal device template linked to the User Profile.
- The total number of owned devices must be less than the Self-Provisioning limit that is specified on the associated User Profile.

Self-Provisioning IVR Service

The Self-Provisioning feature introduces a new service called Self-Provisioning IVR service. When you dial the CTI RP DN that is configured on the Self-Provisioning page, from an extension of a user that uses the IVR service, the phone connects to the Self-Provisioning IVR application and prompts you to provide the Self-Service credentials. Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phones to the users.

You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.

Note When you upgrade a previous release Cisco Unified Communications Manager to Release 10.0, the Cisco Unified Communications Manager will create a Universal Device Template and a Universal Line Template which will retain the previous configurations for Auto-Registration settings. After the upgrade, the values of **Partition** and **External Phone Number Mask** will be populated in the new Universal Line Template by Cisco Unified Communications Manager and in the Line field of the Universal Device Template respectively. And also, the Cisco Unified Communications Manager populates the Cisco Unified Communications Manager name for the Universal Device Template and a Universal Line Template and configures the same values for Auto-Registration settings.

Cisco Unified Communications Manager Administration Considerations

For this feature, the following are new GUI menu paths in Cisco Unified Communications Manager Administration that allow you to configure Self Provisioning:

User Management > Self-Provisioning

Allows you to set up Self-Provisioning for endpoints and the Self-Provisioning IVR service.

User Management > User Settings > User Profile

Allows you to create User Profiles.

Note The Universal Device Template and Universal Line Template setup fields are now available on this window.

The following GUI menu items have been updated for the Self-Provisioning feature:

User Management > User/Phone Add > Feature Group Template

A User Profile field has been added.

User Management > User/Phone Add > Quick User/Phone Add

The Feature Group Template field has been moved to the User Information section.

User Management > End User

The following fields have been added:

- Self-Service User ID
- User Profile

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Set Up Self-Provisioning for New User

Note A newly self-provisioned device may not immediately appear as Registered in Cisco Unified Communications Manager.

Procedure

Step 1 Select **User Management** > **Self Provisioning**.

Step 2 Select one of the following options:

- Requires Authentication: Allow authentication for users only
- Requires Authentication: Allow authentication for users and administrators

  Note For administrator authentication, specify the authentication code. The authentication code must be an integer ranging from 0 to 20 digits but cannot be empty (null).

Step 3 Select **User Management** > **User Settings** > **User Profile**.

Step 4 Create or choose an existing user profile.

Note Make sure the proper universal device template is associated with the user profile and self-provisioning is configured properly.

Step 5 Check the **Allow end user to provision their own phones** check box.

Step 6 Create or choose an existing Feature Group Template. Make sure the proper User Profile is associated.

Step 7 Create a user from **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

Step 8 Select a Feature Group Template.

Step 9 Specify a line extension.

Step 10 Select **Save**.
The new user is now able to perform self-provisioning on the device.

Set Up Self-Provisioning for Existing User

Note A newly self-provisioned device may not immediately appear as Registered in Cisco Unified Communications Manager.

Procedure

Step 1 Select **User Management** > **Self Provisioning**.

Step 2 Select one of the following options:

- Requires Authentication: Allow authentication for users only
- Requires Authentication: Allow authentication for users and administrators

Note For administrator authentication, specify the authentication code. The authentication code must be an integer ranging from 0 to 20 digits but cannot be empty (null).

Step 3 Find an existing user in the Unified Communications Manager database.

Step 4 Find the User Profile that is associated with the user.

Step 5 Open the User Profile.

Step 6 Check the **Allow end user to provision their own phones** check box.

Step 7 Select **Save**.
The user is now able to perform self-provisioning on the device.

Session Description Protocol Transparency

The Session Description Protocol (SDP) Transparency Profile can be configured to selectively allow declarative parameters or to allow all unrecognized parameters to pass from the ingress call leg to the egress call leg.

Session Description Protocol Transparency for Declarative Parameters

The Session Description Protocol Transparency for Declarative Parameters allows the administrator to specify declarative SDP attributes that are not natively supported by Cisco Unified Communications Manager (Unified Communications Manager) to be passed from the ingress call leg to the egress call leg. If the Unified Communications Manager receives attributes that are not explicitly identified by the administrator to send to the egress leg, Unified Communications Manager drops the attribute from the outgoing SDP similar to previous versions of Unified Communications Manager. This feature allows the administrator to identify attributes that are sent to the egress leg in multiple ways, such as configuring all property attributes with a particular name, all value attributes with a particular name, or all value attributes with a specific name and specific value to be passed through. The administrator can also configure all unrecognized attributes to be passed along in the outgoing SDP.

Note SDP Transparency for Declarative Parameters only applies to declarative attributes, not to negotiated attributes.

The Cisco Unified Communications Manager first looks at the name field of an incoming attribute. If the default "Pass all unknown SDP attributes" profile is not used, Unified Communications Manager looks for an exact match among the attributes designated to be passed through. An exact match between the name field of the attribute arriving on the ingress call leg and the name defined by the administrator occurs only if the two strings are identical (case sensitive). If an exact match is not found, then the attribute is not passed through.

The following are the three attributes that can be configured:

- Property attributes: When an administrator configures a property attribute in the SDP Transparency Profile, the attribute is passed through unless the incoming attribute has a value. If the incoming attribute has a value, Unified Communications Manager categorizes the incoming attribute as a value attribute and it is not passed through.
- Value attributes: When an administrator configures a value attribute of any value in the SDP Transparency Profile to be passed through, the attribute is passed through if it contains a value that includes at least

one non-white space character (horizontal tab or space). If the value payload consists of all white space characters, Unified Communications Manager categorizes it as a value attribute and it is not passed through.

- Value attributes configured for value from list: The attribute is passed through only if the value matches one of the five specified values identified by the administrator. If the value does not match one of the five specified values or the there is no value, then the attribute is not passed through.

Session Description Protocol Transparency for All Unrecognized Attributes

An administrator can configure the SDP Transparency Profile to pass all unrecognized SDP attributes from the ingress call leg to the egress call leg when the SDP Transparency Profile is set to "Pass all unknown SDP attributes". To prevent all unrecognized SDP attributes from passing through set the SDP Transparency Profile to "None". The SDP Transparency Profile is selected as "Pass all unrecognized SDP attributes" by default for:

- Standard SIP Profile for Cisco VCS
- Standard SIP Profile for Telepresence Conferencing
- Standard SIP Profile for Telepresence Endpoints

Limitations

Because of the nature of the existing SDP parsing infrastructure that is shared by multiple products, there are certain limitations in the ability to pass through an attribute without any changes.

This feature does not support attribute lines longer than XXXX chars inclusive of a, =, and CRLF. To avoid the limitations, it is recommended that devices passing SDP to the Unified Communications Manager in the ingress leg conform to RFC 4566 which define attribute syntax as:

- a=<name> for property attributes
- a=<name>:<value> for value attributes

Also avoid errors that can result from using non-standard attribute formatting. Even though adherence to RFC 4566 is not required to use this feature, devices following RFC 4566 are immune from the limitations discussed above.

Cisco Unified Communications Manager Administration Considerations

No changes.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Set Up Session Description Protocol Transparency Profile

Procedure

Step 1 To set up a new Session Description Protocol (SDP) Transparency Profile from Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **SDP Transparency Profile**.
The Find and List SDP Transparency Profile page lists all available SDP Transparency Profiles. You may need to click **Find** or **Clear Filter** if no SDP Transparency Profiles appear on the list. This list may also contain several SDP Transparency pre-configured profiles that come with Unified Communications Manager. These profiles may be copied and modified to suit your needs.

Step 2 Perform one of the following:

- Select **Add New** to create a new SDP Transparency Profile.
- Open an existing SDP Transparency Profile.

Note You cannot edit the Pass all unknown SDP attributes profile.

Step 3 Enter the Profile Information.
See the SDP Transparency Profile settings table.

Step 4 Enter the Attribute Information.
See the SDP Transparency Profile settings table.

Step 5 Click **Save**.
After the SDP Transparency Profile is ready, it needs to be associated with a SIP Profile.

Step 6 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **SIP Profile**.

Step 7 On the SIP Profile page, select the desired SDP Transparency Profile from the drop-down list box

Step 8 Click **Save**.
Devices using the SIP Profile must be reset for the changes to take effect.

Note The administrator can configure that all unrecognized attributes are passed to the egress leg by selecting the preconfigured SDP Transparency Profile named **Pass all unknown SDP attributes** from the SDP Transparency Profile drop-down list box. No other configuration is needed to pass through any unrecognized attribute.

Session Description Protocol Transparency Profile Settings

The following table describes the available fields in the SDP Profile window.

Table 31: SDP Transparency Profile Settings

Field	Description
Profile Information	
Name	The name of the SDP Transparency Profile **Note** The name must be unique among all SDP Transparency Profiles in the cluster.
Description	The administrator may also include an additional description about this particular profile
Attribute Information	
Name	Name of the attribute that is passed through
Type	Any Value: signifies that the attribute is passed through regardless of the value **Note** If the attribute is not a value attribute, it is not passed through.
	Property: signifies that the attribute is a property attribute and therefore does not have a value Example: a=foo In this example "foo" represents the property to be passed through.
	Value From List: signifies that attributes that only contain specified values are passed through **Note** The administrator is limited to specifying up to five different values. Example: a=foo:bar In this example foo represents the field, and bar represents one of the values that can be assigned.

Session Persistency

Session Persistency enhances the mobile user experience while roaming. Session Persistency allows mobile users with supported mobile devices to do the following:

- Roam between different networks (e.g. Wi-Fi, VPN over 3G/4G) without having to re-register with Cisco Unified Communications Manager (Unified Communications Manager).
- Maintain the SIP-based subscription status with Unified Communications Manager while roaming between different networks.
- Maintain registration with Unified Communications Manager in the case of network connectivity loss.

- Seamlessly transit both active and held calls from one network to another without call drops.

To facilitate connectivity during roaming between networks, Session Persistency allows dynamic IP address/port change via keep-alive registration to facilitate connectivity during roaming between networks. In addition, the feature includes a configurable TCP reconnect timer, which must be enabled at the product level, to allow mobile users to remain connected in case of a temporary network connectivity loss or roaming. The timer is in effect only when the mobile device tears down the original TCP connection explicitly.

To leverage the Session Persistency feature, mobile devices must comply with Cisco-defined SIP interfaces.

Cisco Unified Communications Manager Administration Considerations

If the TCP reconnect timer has been enabled at the product level, you can configure the timer by setting a value for the Time to Wait for Seamless Reconnect After TCP Drop or Roaming field. The field has a range of 0-300 seconds with a default value of five seconds. The field can be set from any of the following configuration windows:

- Phone Configuration window
- Common Phone Profile window
- Enterprise Phone Configuration window

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Session Timer With Update

Session Refresh Method

The session refresh timer allows for periodic refresh of SIP sessions, which allows the Unified Communications Manager and remote agents to determine whether the SIP session is still active. Prior to Release 10.0(1), when the Unified Communications Manager received a refresh command, it supported receiving either Invite or

Update SIP requests to refresh the session. When the Unified Communications Manager initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified Communications Manager can send both Update and Invite requests.

Cisco Unified Communications Manager Administration Considerations

The following row is added to the Session profile settings table:

Session Refresh Method	Specify whether Invite or Update should be used as the Session Refresh Method. **Invite** (default) **Note** Sending a mid-call Invite request requires that an offer SDP be specified in the request. This means that the far end must send an answer SDP in the Invite response. **Update**: Unified Communications Manager sends a SIP Update request, if support for the Update method is specified by the far end of the SIP session either in the Supported or Require headers. When sending the Update request, the Unified Communications Manager includes an SDP. This simplifies the session refresh since no SDP offer/answer exchange is required. **Note** If the Update method is not supported by the far end of the SIP session, the Unified Communications Manager continues to use the Invite method for session refresh.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Single-Step IP Address and Hostname Change

Cisco Unified Communications Manager (Unified Communications Manager) has been updated with a simplified procedure for updating the IP address or hostname of a Unified Communications Manager server. For details, see the *Changing the IP Address and Hostname in Cisco Unified Communications Manager, Release 10.0(1)*.

Cisco Unified Communications Manager Administration Considerations

The IP address and hostname of a Unified Communications Manager publisher or subscriber node can be updated from Cisco Unified Operating System Administration, or from the Command Line Interface.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Universal Line Template

The Universal Line Template (ULT) feature allows you to create templates with settings that you would normally apply to a directory number. You can create one or more ULTs to reflect your most common directory number configurations, and apply the templates when adding a new directory number on the **Quick User/Phone Add** window.

Tip To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you walk through the template setup process. Select the **Expand All** button to expand all sections.

Note The ULT sections in this window may appear in a different order than the settings table indicates. To change the order of these settings, use the **User Management** > **User/Phone Add** > **Page Layout Preference** menu.

Cisco Unified Communications Manager Administration Considerations

You can find ULT under the following GUI menu item: **User Management** > **User/Phone Add** > **Universal Line Template**

The following GUI menu items have been updated for the ULT feature:

- **User Management > User/Phone Add > Page Layout Preferences**

  A ULT link has been added, where you can customize the layout of the ULT window.

  User Management > User/Phone Add > Feature Group Template

  A ULT section has been added, which contains a drop-down list box from which you can select a ULT. You can also click View Details to display settings for the ULT that you selected.

  User Management > User/Phone Add > Quick User/Phone Add

  Under the Extensions section when you click New, you see a Line Template drop-down list box, from which you can select a ULT.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

User Agent and Server Headers

User-Agent and Server Header Information

This feature provides the option to configure, in the SIP profile, the portion of the installed build number that is sent in SIP messages. This value is used to populate the User-Agent header in SIP requests and the Server header in SIP responses.

Cisco Unified Communications Manager Administration Considerations

The following row is added to the SIP profile settings table:

User-Agent and Server header information	This feature indicates how Unified Communications Manager handles the User-Agent and Server header information in a SIP message. Choose one of the following three options: • Send Unified Communications Manager Version Information as User-Agent Header—For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified Communications Manager passes through any contact headers untouched. This is the default behavior. • Pass Through Received Information as Contact Header Parameters —If this option is selected, the User-Agent/Server header information is passed as Contact header parameters. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers. • Pass Through Received Information as User-Agent and Server Header—If this option is selected, the User-Agent/Server header information is passed as User-Agent/Server headers. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Video Codec Support

Release 10.0(1) introduces H.265 High Efficiency Video Codec (HEVC) and H.264 Scalable Video Codec (SVC). These video codecs are supported in SIP protocols only.

Unified Communications Manager maintains the offerer' s video codec ordering preference when making the answer, if possible. H.265 is the preferred video codec if available on the endpoints, otherwise, Unified Communications Manager follows the following codec preference order:

1. H.265 (HEVC): provides higher quality video using lower bandwidth.
2. H.264 (SVC): allows rendering of variable quality video from the same media stream, by disregarding a subset of the packets received.
3. H.264 (AVC) Advanced Video Coding
4. H.263
5. H.261

H. 264 SVC is a new annex to H.264-AVC video compression standard; meaning it is an enhancement on top of H.264-AVC. It provides the ability to encapsulate multiple video streams at various frame-rates and resolutions in one container.

Video on Hold

The Video on Hold feature is for video contact centers where customers that place a call are able to watch a specific video after initial consultation with the contact center agent. In this case, the agent selects the video stream that is played to the customer while the customer is on hold.

In addition to the video contact center Video on Hold can be deployed within any enterprise if the deployment requires a generic video on hold capability.

Cisco Unified Communications Manager (Unified Communications Manager) now has a new configuration "Video on Hold Server" that allows a media content server to be provisioned under the existing "Media

Resources" menu. The media content server can stream audio and video content when directed by Unified Communications Manager. The media content server is an external device that can store and stream audio and video content under Unified Communications Manager control using SIP as the signal protocol. The media content server is capable of providing hi-definition video content at 1080p, 720p, or lower resolutions such as 360p.

In addition to the video contact centre, Video on Hold can be deployed within any enterprise if the deployment requires a generic video on hold capability. The configured Default Video Content Identifier for the Video on Hold server is used to play the video stream to the user on hold.

The media content server configuration and allocation for a particular session follows the "Media Resource Group" and "Media Resource Group List" constructs in Unified Communications Manager.

Cisco MediaSense is used as the media content server.

Interaction with Enhanced Location Call Admission Control

For this feature, the Cisco MediaSense servers can be collocated in a Unified Communications Manager cluster (the Cisco MediaSense cluster is directly connected to the cluster where the holding party is registered). In that case, the Unified Communications Manager cluster is responsible for deducting the bandwidth between the location of the party on hold and the Cisco MediaSense location. Since Video on Hold interactions make use of 720p or 1080p video streams, it is important to take the bandwidth usage into account before allowing new sessions in order to maintain video quality of existing sessions.

Video on Hold Setup

Configure Unified Communications Manager with a SIP trunk to a Cisco MediaSense cluster. The SIP trunk to the Cisco MediaSense server will have the IP addresses of the Cisco MediaSense nodes configured. The Unified Communications Manager SIP trunk supports up to 16 destination IP addresses.

Note Cisco MediaSense cluster should have two or more nodes for redundancy and scalability purposes.

Two topologies are possible to set up Video on Hold:

- Cisco MediaSense is directly connected with the holding party's Unified Communications Manager cluster.

  When Video on Hold server is located on the same cluster as the Holding Party, the SIP Trunk on the Video on Hold server configuration should point to the Cisco MediaSense server and the default content identifier should point to a stream ID that exists on the MediaSense server. The content identifier can be any alphanumeric string. No additional configuration is needed.

- Cisco MediaSenseis centrally deployed with Session Management Edition (SME).

  When Video on Hold server is located off the SME, the Video on Hold Server must be configured on the leaf cluster hosting the Holding Party. The SIP trunk on this Video on Hold Server should point to the SME SIP trunk. On the SME, a SIP Trunk should be provisioned to point to the Cisco MediaSense server.

  There are three ways on how Unified Communications Manager can be configured to support this centralized deployment:

  - Content Identifier is numeric: In this case, a route pattern must be provisioned on the SME to route the INVITE to Cisco MediaSense server. Essentially, we use the left hand side of the INVITE URI sent by the leaf cluster to route the call to Cisco MediaSense server. The right hand side of the INVITE URI contains the IP address of SME node.

- Content Identifier is alpha-numeric and contains the IP address of Cisco MediaSense: In this case, the content identifier configured on the leaf cluster should contain both the stream-id and the IP address of the Cisco MediaSense server (stream-id@mediasense-ipaddress).

  On the SME cluster, a SIP route pattern must be configured that uses the IP address routing with the IP address of the MediaSense server matching the default content identifier. In this scenario, the route is based on the right hand side of the INVITE URI (IP address of MediaSense server) sent by the leaf cluster.

- Content Identifier is alpha-numeric and contains the domain name: In this case, the content identifier configured on the leaf cluster should contain both the stream-id and the domain name of the Cisco MediaSense server (stream-id@cisco.com).

  On the SME cluster, a URI catalog must be created with a SIP route pattern as a Route String. The content identifiers from the Cisco MediaSense server must be imported into this catalog using the URI infrastructure.

  Note The SIP Route Pattern must be configured to use domain routing. This SIP Route pattern should point to a SIP Trunk to Cisco MediaSense server.

Video on Hold SIP Trunk

The SIP Trunk pointing to Video on Hold server should be configured with the default configuration. The following information is needed for configuring the SIP Trunk:

- Name
- Description
- Device Pool
- Location
- Destination address and destination port (multiple IP addresses and ports can be specified)
- SIP Trunk Security Profile
- SIP Profile: A SIP profile with the option ping configured should be selected. If none exists, one should be created. This is not mandatory but will improve the user experience.

Note Other configurations on the SIP Trunk are not supported for Video on Hold.

Cisco Unified Communications Manager Administration Considerations

New configuration: Video on Hold Server under Media Resources.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

There are two performance counters that can be observed from RTMT for Video on Hold server:

- VideoOnHoldOutofResources
- VideoOnHoldResourceActive

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Set Up Video On Hold

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Media Resources** > **Video on Hold Server**.

Step 2 Click **Add New** to set up a new Video on Hold server.

Step 3 Enter the name of the Video on Hold server.

Step 4 Enter a description for the server.

Step 5 Enter the Default Video Content Identifier.

Step 6 Select the SIP Trunk to be used from the drop-down list. If a new SIP Trunk needs to be created, click the button **Create SIP Trunk**.

Step 7 Click **Save**.

Video QoS Reservation

Cisco Unified Communications Manager Administration Considerations

Note This feature is limited to use in lab environments for demonstration purposes only. Cisco Technical Assistance Center (TAC) does not provide support for this feature.

The Video Quality of Service (QoS) Reservation feature reserves bandwidth in a mobile network, through a third party HTTP service, when a mobile device makes a call. This reservation is only for VoIP calls made through Cisco Unified Communications Manager, not for other voice calls already classified by the mobile network as voice calls.

For each device with its MSISDN configured, Unified Communications Manager requests its connection type. If the connection type for the device is supported, Unified Communications Manager reserves the bandwidth with its MSISDN and the connected IP address. For a video call, there are two separate reservations, one for the audio portion and one for the video portion, both with the QoS Class Identifier (QCI) value set to 2. For an audio call, there is one reservation, with the QCI value set to 1.

This feature only supports Unified Communications Manager SIP line side devices, such as CSF client (Jabber for Tablet) and Cius.

To enable the Video QoS feature, use the **System > Service Parameters** menu path to configure the parameters for the device. In the **Clusterwide Parameters** section, configure **External QoS Enabled** to True.

To configure a MSISDN for the device, use the **Device > Phone** menu path. Enter the MSISDN in the **Mobile Subscriber ISDN(MSISDN)** field.

Use the **Call Routing > HTTP Profile** menu path to configure a HTTP profile.

The following table shows the HTTP Profile settings.

Table 32: HTTP Profile Settings

Field	Description
Name	Enter a name for the HTTP profile.
User Name	Enter a user name.
Password	Enter a password.
Request Timer	Enter an amount for the request timer in milliseconds.
Web Service Root URI	Enter the Web Service Root URI.
QoS Connection Type	Used in conjunction with Web Service Root URI to query the device's connection type.
QoS URI	Used in conjunction with Web Service Root URI to reserve bandwidth for the device.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Wireless LAN Profiles

The Wireless LAN Profile feature removes the need for users to configure Wi-Fi parameters on their phones by allowing the administrator to configure Wi-Fi profiles for them. The user devices can automatically download the Wi-Fi configuration from the Cisco Unified Communications Manager TFTP server, and the configuration is then applied to these devices.

Before you create a Wireless LAN Profile, you can configure a Network Access Profile, which contains information about VPN connectivity and HTTP proxy settings. Create a Network Access Profile from the **Device** > **Device Settings** > **Network Access Profile** menu.

After you create one or more Wireless LAN Profiles, you can add them to a Wireless LAN Profile Group, which you can configure from the **Device** > **Device Settings** > **Wireless LAN Profile Group** menu. You can also specify the enterprise-wide default group.

Note You may add up to four Wireless LAN Profiles to a Wireless LAN Profile Group.

Note The Cisco Desktop Collaboration Experience DX650 (SIP) supports Wireless LAN Profiles.

To use the Wireless LAN Profile feature, consider the following work flow:

1. (Optional) You can configure a Network Access Profile.
2. Create one or more Wireless LAN Profiles, and add a Network Access Profile if you configured one.
3. After you create one or more Wireless LAN Profiles, you can add them to a Wireless LAN Profile Group. You can also specify the enterprise-wide default group.

4 You can add a Wireless LAN Profile Group to a device pool or device-level configuration.

5 After Step 4, TFTP adds the Wireless LAN Profile Group to the existing device configuration file, which the device proceeds to download.

Cisco Unified Communications Manager Administration Considerations

For this feature, the following are new GUI menu paths in Cisco Unified Communications Manager Administration that allow you to configure Wireless LAN Profiles:

Device > Device Settings > Network Access Profile

Allows you to create Network Access Profiles.

Device > Device Settings > Wireless LAN Profile

Allows you to create Wireless LAN Profiles.

Device > Device Settings > Wireless LAN Profile Group

Allows you to create Wireless LAN Profile Groups (from Wireless LAN Profiles that you previously created).

The following GUI menu items have been updated for the Wireless LAN Profile feature:

Device > Phone

A Wireless LAN Profile Group field has been added.

System > Device Pool

A Wireless LAN Profile Group field has been added.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Procedure changes

Create Network Access Profile

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Network Access Profile**

Step 2 Click **Add New**.
The Network Access Profile settings window appears.

Step 3 Enter Network Access Profile settings.

Step 4 Click **Save**.
The Network Access Profile is created.

What to Do Next

- Create a Wireless LAN Profile
- Add this Network Access Profile to a Wireless LAN Profile

Create Wireless LAN Profile

Before You Begin

Optionally, create a Network Access Profile to associate to a Wireless LAN Profile.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wireless LAN Profile**

Step 2 Click **Add New**.
The Wireless LAN Profile settings window appears.

Step 3 Enter the Wireless LAN Profile settings.

Step 4 Click **Save**.
The Wireless LAN Profile is created.

What to Do Next

- Create another Wireless LAN Profile
- Combine Wireless LAN Profiles into a Wireless LAN Profile Group

Create Wireless LAN Profile Group

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wireless LAN Profile Group**

Step 2 Click **Add New**.
The Wireless LAN Profile Group settings window appears.

Step 3 Enter the Wireless LAN Profile Group settings.

Step 4 Click **Save**.
The Wireless LAN Profile is created.

What to Do Next

Link a Wireless LAN Profile Group to a device or Device Pool.

Link Wireless LAN Profile Group with Device

You can link a Wireless LAN Profile Group at the device or device pool level.

Note If you link a Wireless LAN Profile Group at the device and device pool level, Cisco Unified Communications Manager uses the device pool level.

Before You Begin

Create a Wireless LAN Profile Group.

Procedure

Step 1 Perform one of the following actions:

- Select **Device** > **Phone**.
- Select **System** > **Device Pool**

Step 2 Perform one of the following actions:

- Find an existing device or create a new device.

- Find an existing device pool or create a new device pool.

Step 3 Select a Wireless LAN Profile Group from the drop-down list box.

Step 4 Select **Save**.
The Wireless LAN Profile Group is linked to the device or Device Pool.

Wi-Fi Hotspot Profile

The Wi-Fi Hotspot Profile feature allows users to use their desk phones to provide a Wi-Fi Hotspot, so that they can connect a Wi-Fi device such as a tablet or a mobile phone to the network through the desk phone. The desk phones can automatically download the Wi-Fi Hotspot configuration from the Cisco Unified Communications Manager, and the configuration is then applied to these devices.

To use the Wi-Fi Hotspot Profile feature, you must configure a Wi-Fi Hotspot Profile on the Cisco Unified Communications Manager administrative interface. After the profile is created, you must associate it with a phone. To associate a Wi-Fi Hotspot Profile to a phone, you can configure the profile at the Enterprise Parameters, Common Phone Profile, or individual phone level. Configuring a Wi-Fi Hotspot Profile on the Phone page overrides the Enterprise Parameters and Common Phone Profile settings. After the desk phones download the TFTP configuration file, the users can enable Wi-Fi Hotspot and connect the Wi-Fi devices.

By default, the Wi-Fi Hotspot Profile feature is disabled in Cisco Unified Communications Manager. If you want to enable the Wi-Fi Hotspot for a desk phone, you can enable the Wi-Fi Hotspot feature at the Enterprise Phone Configuration, Common Phone Profile or individual phone level and then apply a Wi-Fi Hotspot Profile to the Enterprise Parameters, Common Phone Profile or individual phone level. The Wi-Fi Hotspot setting on the Phone page overrides the setting on the Common Phone Profile page, which overrides the setting on the Enterprise Phone Configuration page.

Cisco Unified Communications Manager Administration Considerations

The following new GUI menu path in Cisco Unified Communications Manager Administration allows you to configure Wi-Fi Hotspot Profile:

- **Device** > **Device Settings** > **Wi-Fi Hotspot Profile**

The following GUI menu items have been updated for the Wi-Fi Hotspot Profile feature:

Device > Phone

A Wi-Fi field has been added.

Device > Phone

A Wi-Fi Hotspot field has been added.

Device > Phone

A Wi-Fi Hotspot Profile field has been added.

Device > Device Settings > Common Phone Profile

A Wi-Fi field has been added.

Device > Device Settings > Common Phone Profile

A Wi-Fi Hotspot field has been added.

System > Enterprise Phone Configuration

A Wi-Fi field has been added.

System > Enterprise Phone Configuration

A Wi-Fi Hotspot field has been added.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.

Wi-Fi Hotspot Profile Settings

The following table displays the Wi-Fi Hotspot Profile settings.

Name	Description
Wi-Fi Hotspot Profile Information	
Name	Enter a name for the Wi-Fi Hotspot Profile. The value can include 1 to 50 characters, including alphanumeric characters, dots, dashes, and underscores.
Description	Enter a description for the Wi-Fi Hotspot Profile. The description can include up to 50 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).

Name	Description
User Modifiable	Select one of the following options from the drop-down list box: **Allowed** Indicates that the user can change any profile settings. This is the default setting. **Disallowed** Indicates that the user cannot make any changes to the profile. **Restricted** Indicates that some settings (Enable/Disable, SSID Suffix, PSK Passphrase, WEP Key) can be modified, but other settings (Frequency Band, Authentication Method, Authentication Server, Port, Shared Secret) cannot be modified.
Wireless Settings	
SSID (Network Name) Prefix	Enter the Service Set Identifier (SSID) Prefix for the Wi-Fi Hotspot Profile. The SSID Prefix that you enter here is combined with the SSID suffix, which is generated automatically based on the local endpoint information, to create a unique SSID for the Wi-Fi Hotspot of the phone. The value can include 1 to 20 alphanumeric characters.

Name	Description
Frequency Band	Select one of the following frequency band settings from the drop-down list box: **Auto** The profile automatically chooses a frequency band. **2.4 GHz** The profile automatically chooses 2.4 GHz as the frequency band. **5 GHz** The profile automatically chooses 5 GHz as the frequency band. **Note** If you select the Auto option, a single channel will be used to serve clients because dual-band operation is currently not supported.
Authentication	

Name	Description
Authentication Method	

Name	Description
	Specify the authentication method that is used to secure access to the Wi-Fi Hotspot. Depending on the method you choose, a PSK Passphrase, WEP key, or password description field appears so that you can provide the credentials that are required to connect to this Wi-Fi Hotspot. The following authentication methods are available: **EAP-FAST** (Extensible Authentication Protocol - Flexible Authentication through Secure Tunneling) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **PEAP-MSCHAPV2** (Protected Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol Version 2) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **PEAP-GTC** (Protected Extensible Authentication Protocol - Generic Token Card) If you choose this method, the Wi-Fi client that is connecting to the Wi-Fi Hotspot must be configured with a valid username and password. **WPA2-PSK** (Wi-Fi Protected Access Pre-Shared Key) This method uses Advanced Encryption Standard (AES) encryption. If you select this method, you must enter a passphrase, which is an 8 to 63 ASCII character string or a 64 HEX character string. **WPA-PSK** This method uses Temporal Key Integrity

Name	Description
	Protocol (TKIP) encryption. If you select this method, you must enter a passphrase, which is an 8 to 63 ASCII character string or a 64 HEX character string. **WEP** (Wired Equivalent Privacy) WEP requires a WEP Key, which is either a 5 or 13 ASCII character string or a 10 or 26 HEX character string. **None** No authentication is required.
Server Settings	
Host Name/IP Address	Enter the DNS hostname (up to 255 characters) or IP address of the authentication server.
Port	Enter the port number. 1812 is the default port. The accepted port range is 1-65535.
Shared Secret	Enter the shared secret. The value can include 1 to 32 characters. The shared secret is used to authenticate against the authentication server. The shared secret specified in the Wi-Fi Hotspot Profile must match with the shared secret specified in the authentication server.
Note The server settings are displayed only if you select the authentication method as EAP-FAST, PEAP-MSCHAPv2, or PEAP-GTC.	

Procedure changes

Create Wi-Fi Hotspot Profile

Use the following procedure to create a new Wi-Fi Hotspot Profile. After you create a Wi-Fi Hotspot Profile, you can apply it at the Enterprise Parameters, Common Phone Profile or individual phone level.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **Device** > **Device Settings** > **Wi-Fi Hotspot Profile**.

Step 2 Click **Add New**.
The Wi-Fi Hotspot Profile settings window appears.

Step 3 Enter the Wi-Fi Hotspot Profile settings.

Step 4 Click **Save.**
The Wi-Fi Hotspot Profile is created.

Repeat this procedure for each Wi-Fi Hotspot Profile that you want to create.

CHAPTER 4

Cisco IP Phones and Cisco Desktop Collaboration Experience DX650

Cisco IP Phones

Cisco IP Phone Firmware Versions

The following table lists the latest Cisco IP Phone firmware version supported for Cisco Unified Communications Manager 10.0. Phones in this table that are identified with an asterisk (*) are new since Cisco Unified Communications Manager 9.0.

Table 33: Phone Firmware Versions

Phone family	Firmware release number
Cisco Unified SIP Phone 3905	9.4(1)
Cisco Unified IP Phones 6901 and 6911	9.3(1)SR1
Cisco Unified IP Phones 6921, 6941, 6945, and 6961	9.4(1)
* Cisco IP Phone 7800 Series	10.1(1)
Cisco Unified IP Phone 7900 Series	9.3(1)SR2
Cisco Unified Wireless IP Phone 792x Series	1.4(5)
* Cisco Unified IP Conference Phone 8831	9.3(3)

Phone family	Firmware release number
Cisco Unified IP Phones 8941 and 8945	9.3(2)SR1
Cisco Unified IP Phones 8961, 9951, and 9971	9.4(1)

Cisco Unified SIP Phone 3905 Features

The following table lists the features added to the Cisco Unified SIP Phone 3905 for firmware release 9.4(1). For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/ps7193/prod_release_notes_list.html

Feature name	Firmware release
IPv6	9.4(1)
IPv6 Ready Logo (SIP)	9.4(1)
Multiple Date Display Formats	9.4(1)
Paging Support on Cisco Unified Communications Manager	9.4(1)
Paging Support on Cisco Unified Communications Manager Express	9.4(1)
SIP MD5 Digest Authentication	9.4(1)

Cisco Unified IP Phone 6900 Series Features

The following table lists the features added to the Cisco Unified IP Phone 6900 Series for firmware releases 9.3(1)SR1, 9.3(3), 9.3(3)SR1, and 9.4(1). For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/ps10326/prod_release_notes_list.html

Feature name	Supported on Cisco Unified IP Phones 6901 and 6911	Supported on Cisco Unified IP Phones 6921, 6941, 6945, and 6961
Configurable Maximum Number of Calls and Busy Trigger	9.3(1)SR1	No
Web Access Disabled by Default	9.3(1)SR1	9.3(3)
Call Waiting Ring	No	9.3(3)

Feature name	Supported on Cisco Unified IP Phones 6901 and 6911	Supported on Cisco Unified IP Phones 6921, 6941, 6945, and 6961
Debug Phone	No	9.3(3)
HTTPS	No	9.3(3)
Show Calling ID and Calling Number	No	9.3(3)
Electronic Hookswitch	No	9.3(3)
Minimum Ring Volume	No	9.3(3)
Secure EMCC	No	9.3(3)
TVS and Security by Default	No	9.3(3)
E-SRST Service Improvements	No	9.4(1)
IPv6 Support for SIP	No	9.4(1)
Peer Firmware Sharing	No	9.4(1)
PSTN Mode	No	9.4(1)
Save Volume Change	No	9.4(1)
Serviceability for SIP Endpoints	No	9.4(1)
Show Call Duration in Call History	No	9.4(1)

Cisco IP Phone 7800 Series Features

The Cisco® IP Phone 7800 Series is a high-fidelity voice communications portfolio designed for people-centric collaboration. It combines always-on reliability and security, full-featured easy-to-use IP telephony, and wideband audio to increase productivity, with an earth-friendly design for reduced costs.

The Cisco IP Phone 7800 Series brings a higher quality standard, with full wideband audio support for handset, headset and speaker, to our voice-centric portfolio. A new ergonomic design includes support for larger grayscale, graphical backlit displays. The Cisco IP Phone 7800 Series also offers customers very low power consumption, as the phones are IEEE Class 1 devices. Combined with support for Cisco EnergyWise™, this delivers greater economies of scale in customers wiring closets as well as helping to reduce operating expenditures with energy savings. Other key differences include Electronic Hook-switch capability, for call control while using third-party headsets, encrypted communications, and a field replaceable bezel option.

For more information on the Cisco IP Phone 7800 Series, see http://www.cisco.com/en/US/products/ps13220/tsd_products_support_series_home.html

Cisco Unified IP Phone 7900 Series Features

The following table lists the features added to the Cisco Unified IP Phone 7900 Series for firmware releases 9.3(1)SR1 and 9.3(2)SR2. For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_notes_list.html

Feature name	Firmware release
Hardware Updates	9.3(1)SR1
Firmware Release 9.3(1)SR2 Security Enhancements	9.3(1)SR2

Cisco Unified Wireless IP Phone 792x Series Features

The following table lists the features added to the Cisco Unified Wireless IP Phone 792x Series for firmware releases 1.4(3), 1.4(4), and 1.4(5). For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_notes_list.html

Feature name	Firmware release
Clear Call History Confirmation	1.4(3)
7926G J2ME Memory Increase	1.4(4)
792x USB Driver Support for Microsoft Windows 7	1.4(4)
Dock Icon Support for Cisco Unified Wireless IP Phone 7925G Desktop Charger	1.4(4)
Timezone Support	1.4(4)
XSI Audio Path Control	1.4(4)
MIDlet Minimize to Background When Power On	1.4(5)

Cisco Unified IP Conference Phone 8831 Features

The Cisco Unified IP Conference Phone 8831 is a full-featured single line conference station that provides voice communication over an IP network. It functions much like a digital business phone, allowing users to place and receive calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because conference stations connect to the data network, they offer enhanced IP telephony features, including access to network information and services, and customizable features and services.

The conference phone provides a backlit LCD screen, support for up to ten speed-dial numbers, and a variety of other sophisticated functions. Optional microphone extension kits provide enhanced room coverage that can be further expanded by linking two units together.

In addition to basic call handling features, the conference phone can provide enhanced productivity features that extend call handling capabilities. Depending on configuration, the phone supports:

- Access to network data, XML applications, and web-based services.
- Online customizing of conference station features and services from the User Options web pages.

The phone supports seamless firmware upgrade. If two devices are connected in Linked Mode, firmware upgrades are pushed automatically from the primary unit to the secondary unit.

For more information on the Cisco Unified IP Conference Phone 8831, see http://www.cisco.com/en/US/products/ps12965/tsd_products_support_series_home.html.

Cisco Unified IP Phones 8941 and 8945 Features

The following table lists the features added to the Cisco Unified IP Phones 8941 and 8945 for firmware release 9.3(2). For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/ps10451/prod_release_notes_list.html

Feature name	Firmware release
Audio Only Lock Icon	9.3(2)
Enhanced Message Waiting Indicator	9.3(2)
HTTPS Support	9.3(2)
One Click to Home Screen	9.3(2)
User Experience Enhancements	9.3(2)
VPN Client Support	9.3(2)
XSI Component API Support	9.3(2)

Cisco Unified IP Phones 8961, 9951, and 9971 Features

The following table lists the features added to the Cisco Unified IP Phones 8961, 9951, and 9971 for firmware releases 9.3(2), 9.3(4), and 9.4(1). For more information, see the Release Notes at the following location:

http://www.cisco.com/en/US/products/ps10453/prod_release_notes_list.html

Feature name	Firmware release
Actionable Incoming Call Alert	9.3(2)

Feature name	Firmware release
Call History Display Enhancement for Call Window	9.3(2)
Custom Line filters	9.3(2)
New Hardware Models	9.3(2)
Prompt for Barge	9.3(2)
Audio-Only Lock Icon	9.3(2)
Configurable DF Bit	9.3(2)
CGI CallInfo and LineInfo	9.3(4)
Conference and Transfer Enhancement	9.3(4)
Configurable Font Size	9.3(4)
Hide Softkeys in Full Screen Video Mode	9.3(4)
Hold or Resume Toggle from Hard Key	9.3(4)
One Button to Access Call History	9.3(4)
Unique cBarge Call Instance ID	9.3(4)
Cisco IP Manager Assistant Support	9.3(4)
Separate Audio and Video Mute	9.3(4)
Softkey Template	9.3(4)
URI Dialing Enhancement	9.3(4)
CGI ModeInfo	9.4(1)
Confidential Access Level	9.4(1)
Configurable RTP/SRTP Port Range	9.4(1)
Configurable TLS Resumption Timer	9.4(1)
CTL and ITL Status Display and Report	9.4(1)
CTL/ITL Signature	9.4(1)
E-SRST Service Improvements	9.4(1)

Feature name	Firmware release
FIPS 140-2 Level 1 Compliance	9.4(1)
Gateway Recording For SIP	9.4(1)
Hide Wi-Fi UI Setting	9.4(1)
IPv6 Support	9.4(1)
Line State Display Enhancement	9.4(1)
RTCP Always On	9.4(1)
Separate Video and Audio Port Range configuration	9.4(1)
Serviceability for SIP Endpoints	9.4(1)
Unified Font Size Enhancement	9.4(1)

Cisco Desktop Collaboration Experience DX650

Cisco Desktop Collaboration Experience DX650 Firmware Versions

The following table lists the latest Cisco Desktop Collaboration Experience DX600 Series firmware version supported for Cisco Unified Communications Manager 10.0. Phones in this table that are marked with an asterisk (*) are new since Cisco Unified Communications Manager 9.0.

Table 34: Phone Firmware Versions

Phone family	Firmware release number
* Cisco Desktop Collaboration Experience DX650	10.1(1)

Cisco Desktop Collaboration Experience DX650 Features

The Cisco Desktop Collaboration Experience DX650 (Cisco DX650) is built to deliver integrated, always-on and secure, high-definition (HD) voice and video communications; conferencing with Cisco WebEx meeting applications; presence and instant messaging with the Cisco Jabber messaging integration platform; and on-demand access to cloud services. Cisco DX650 meets the demands of people who must collaborate effectively with experts even if separated by long distances.

The following table lists the features added to the Cisco DX650 for firmware releases 10.0(1) and 10.1(1). For more information on the Cisco DX650, see the Release Notes at the following location: http://www.cisco.com/en/US/products/ps12956/prod_release_notes_list.html

Feature name	Firmware release
+ Dialing (ITU E.164)	10.0(1)
Abbreviated dialing	10.0(1)
Adjustable ringing and volume levels	10.0(1)
Adjustable display brightness	10.0(1)
Android bundled applications and widgets	10.0(1)
Android core features	10.0(1)
Application dial rule	10.1(1)
Auto-answer	10.0(1)
Auto-detection of headset	10.0(1)
Barge (cBarge)	10.0(1)
Bluetooth Hands-Free Profile	10.1(1)
Bluetooth Phone Book Access Profile	10.1(1)
Callback	10.0(1)
Call Chaperone	10.0(1)
Call forward	10.0(1)
Call forward notification	10.0(1)
Call history lists	10.0(1)
Call park (including Directed Call Park and Assisted Directed Call Park)	10.0(1)
Call pickup	10.0(1)
Call timer	10.0(1)
Call waiting	10.0(1)
Caller ID	10.0(1)
Cisco AnyConnect Secure Mobility Client (VPN) Version 3.0	10.0(1)
Cisco Jabber IM	10.0(1)
Cisco WebEx Version 2.5	10.0(1)
Corporate directory	10.0(1)
Conference (ad hoc)	10.0(1)
Data migration	10.1(1)
Default wallpaper control	10.1(1)

Feature name	Firmware release
Direct transfer	10.0(1)
Divert (iDivert)	10.0(1)
Do Not Disturb (DND)	10.0(1)
Extension Mobility service	10.0(1)
Fast-dial service	10.0(1)
Flexible DSCP	10.1(1)
Forced access codes and client matter codes	10.0(1)
Google bundled applications	10.0(1)
Group call pickup	10.0(1)
Hold (and Resume)	10.0(1)
Intercom	10.0(1)
International call logging	10.0(1)
IP Phone Manager Assistant (IPMA)	10.1(1)
Join (ad hoc)	10.0(1)
Last-number redial (LNR)	10.0(1)
Malicious-caller ID	10.0(1)
Media Net _End of session	10.1(1)
Message-waiting indicator (MWI)	10.0(1)
Meet-me conference	10.0(1)
Mobility (Mobile Connect and Mobile Voice Access)	10.0(1)
Music on Hold (MoH)	10.0(1)
Mute (audio and video)	10.0(1)
Network profiles (automatic)	10.0(1)
On- and off-network distinctive ringing	10.0(1)
Personal directory	10.0(1)
Phone-Only Mode	10.1(1)
PickUp	10.0(1)
Predialing before sending	10.0(1)
Privacy	10.0(1)
Private Line Automated Ringdown (PLAR)	10.0(1)
Quick Contact Badge	10.0(1)

Feature name	Firmware release
Remote Wipe/Lock	10.1(1)
Remotely check CTL/ITL file	10.1(1)
Ring tone per line appearance	10.0(1)
Self-provisioning	10.1(1)
Self-View (video call)	10.0(1)
Service URL	10.0(1)
Shared line(s)	10.0(1)
SIP Gateway Recording	10.1(1)
Time and date display	10.0(1)
Transfer (ad hoc)	10.0(1)
Visual Voicemail	10.0(1)
Wireless profiles	10.1(1)

Routing Enhancements

Cisco Unified Communications Manager Administration Considerations

Directory number settings

The following table describes the fields that are available in the Directory Number Configuration window.

Table 35: Directory Number Settings

Field	Description
Directory Number Information	
Urgent Priority	If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call to the device associated with the directory number until the interdigit timer expires (even if the directory number is a better match for the sequence of digits dialed as compared to the overlapping pattern). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately to the device associated with the directory number. By default, the Urgent Priority check box is unchecked.

Translation pattern settings

The following table describes the available fields in the Translation Pattern Configuration window.

Table 36: Translation Pattern Settings

Field	Description
Pattern Definition	
Use Originator's Calling Search Space	To use the originator's calling search space for routing a call, check the Use Originator's Calling Search Space check box. When you check this check box, it disables the Calling Search Space drop-down list box. When you save the page, the Calling Search Space box is grayed out and set to <None>. If the originating device is a phone, the originator's calling search space results from the device calling search space (configured on the Phone Configuration window) and line calling search space (configured on the Directory Number Configuration window). Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you check the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you uncheck the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used.
Do Not Wait For Interdigit Timeout On Subsequent Hops	When you check this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches. Whenever you check the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns. **Note**: Cisco Unified Communications Manager does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops unchecked.

Call Control Discovery feature parameters

To access the feature parameters that support the call control discovery feature, choose **Call Routing** > **Call Control Discovery** > **Feature Configuration**. For additional information, you can click the question mark help in the Feature Configuration window.

The following table describes the feature parameters for the call control discovery feature.

Table 37: Call Control Discovery Feature Parameters

Feature Parameter	Description
Set Urgent Priority for Fixed-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern (when the fixed-length learned pattern is a better match for the sequence of digits dialed as compared to the overlapping route pattern configured). If the parameter is set to True, Cisco Unified Communications Manager does not wait for the interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the fixed-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager learns the pattern +44987XXX for routing the calls to another Cisco Unified Communications Manager and there is also a route pattern configured as \+44! for routing the calls to the PSTN destination. If this parameter is set to False and +44987127 is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager (this interdigit timer allows user to dial more digits after +44987127 to reach the PSTN destination). If this parameter is set to True and +44987127 is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

Feature Parameter	Description
Set Urgent Priority for Variable-Length CCD Learned Patterns	This parameter determines whether Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to True, Cisco Unified Communications Manager does not wait for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. If the parameter is set to False, Cisco Unified Communications Manager waits for interdigit timer before routing the call to the destination that is associated with the variable-length learned pattern. The default equals False. Example: Cisco Unified Communications Manager has translation pattern 9011.!# configured. This translation pattern strips predot digits and the trailing # character and adds the prefix +55 to the dialed digits. Cisco Unified Communications Manager also learns pattern \+55.! for routing the calls to another Cisco Unified Communications Manager. If this parameter is set to False and 9011234567# (resultant digits = +55234567) is dialed, Cisco Unified Communications Manager waits for interdigit timer before routing the call to another Cisco Unified Communications Manager. If this parameter is set to True and 9011234567# (resultant digits = +55234567) is dialed, then Cisco Unified Communications Manager immediately routes the call to another Cisco Unified Communications Manager.

The following table describes the settings for SIP trunks.

Table 38: SIP Trunk Settings

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete the prefix for unknown number type for the called party, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for the Prefix field for unknown number type, click Default Prefix Settings.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device.

Field	Description
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update/reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing.
Outbound Calls	
Called Party Transformation CSS	This settings allows you to send the transformed called party number in INVITE message for outgoing calls made over SIP Trunk. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This settings allows you to send the transformed calling party number in INVITE message for outgoing calls made over SIP Trunk. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number that is sent from Cisco Unified Communications Manager side in outgoing reINVITE / UPDATE messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table describes the trunk settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

Table 39: H.225 and Intercluster Trunks Settings

Field	Description
Connected Party Settings	
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table lists configuration settings for H.323 gateways.

Table 40: H.323 Gateway Configuration Settings

Field	Description
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number that Cisco Unified Communications Manager sends in another format, such as a DID or E.164 number. This setting is applicable while sending connected number for basic call as well as sending connected number after inbound call is redirected. Cisco Unified Communications Manager includes the transformed number in the Connected Number Information Element (IE) of CONNECT and NOTIFY messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.
Call Routing Information - Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation CSS in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Note** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

The following table provides detailed descriptions for Digital Access PRI port configuration settings.

Table 41: Digital Access PRI Port Settings

Field	Description
Call Routing Information - Outbound Calls	
Called Party Transformation CSS	This setting allows you to send transformed called party number in SETUP message for outgoing calls. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device. **Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.

Field	Description
Calling Party Transformation CSS	This setting allows you to send transformed calling party number in SETUP message for outgoing calls. Also when redirection occurs for outbound calls, this CSS will be used to transform the connected number sent from Cisco Unified Communications Manager side in outgoing NOTIFY messages. [For PRI DMS - 100 and DMS - 200]. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. **Tip** If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.
Connected Party Settings	

Field	Description
Connected Party Transformation CSS	This setting is applicable only for inbound Calls. This setting allows you to transform the connected party number sent from Cisco Unified Communications Manager in another format, such as a DID or E.164 number. **Note** You can configure a Connected Party Transformation CSS only when you select one of the following protocols that support Connected Number Information Element: • For T1 PRI : ◦ PRI DMS - 100 ◦ PRI DMS - 250 ◦ PRI ISO QSIG T1 • For E1 PRI : ◦ PRI ISO QSIG E1 For other protocol types, Connected Party Transformation CSS is grayed out. Using this setting, Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of CONNECT message for basic call. For PRI DMS - 100 and DMS - 250 protocols , Cisco Unified Communications Manager includes transformed number in Connected Number Information Element (IE) of NOTIFY message for inbound calls after redirection. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. **Note** If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Connected Party Transformation CSS in a non-null partition that is not used for routing.
Use Device Pool Connected Party Transformation CSS	To use the Connected Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager does not apply any prefix or strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

The following table provides detailed descriptions for BRI port configuration settings.

Table 42: BRI Port Configuration Settings

Field	Description
Incoming Called Party Settings	
Clear Prefix Settings	To delete all prefixes for all called party number types, click Clear Prefix Settings.
Default Prefix Settings	To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Field	Description
National Number	Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes. • Use Device Pool CSS— Check this check box to use the calling search space for the National Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
International Number	

Field	Description
	Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the International Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation

Field	Description
	pattern that you want to assign to this device.

Field	Description
Unknown Number	Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Unknown Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Field	Description
Subscriber Number	Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type. • Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. **Tip** If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that is applied to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called party prefix, which supports both the prefix and strip digit functionality. **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field. • Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes. • Use Device Pool CSS—Check this check box to use the calling search space for the Subscriber Number field that is configured in the device pool that is applied to the device. • Calling Search Space—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

Add Route Groups to Route List

Note When you configure the Local Route Group feature, add the route groups to the route list by selecting those local route group names that are appended with the Local Route Group tag that appears in the drop-down list box.

Bulk Administration Considerations

No changes.

CDR/CAR Considerations

No changes.

IP Phones Considerations

No changes.

RTMT Considerations

No changes.

Security Considerations

No changes.

Serviceability Considerations

No changes.