# New and Changed Features



# New Default Softkey Templates for Feature Hardkey Phones

The following softkey templates with new softkey layouts are introduced for Cisco Unified Communications Manager Release 10.5(1):

- Cisco Protected Phone with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys
- Cisco Feature with Feature Hardkeys
- Cisco User with Feature Hardkeys (default)
- Cisco Manager with Feature Hardkeys
- Cisco Assistant with Feature Hardkeys

- Cisco Shared Mode Manager with Feature Hardkeys

The phones with feature hardkeys have hardkeys for the Hold, Transfer, and Conference call features. The new softkey templates avoid needing both hardkeys and softkeys for these call features.

**Note** The existing Standard User template before Release 10.5(1) appears for both a fresh installation and an upgrade. This is the only built-in template that is appropriate for use on phones that use softkeys for Hold, Transfer, and Conference, such as the Cisco 7961.

7936 phones use the Standard User as the default template. In order to use the conference, hold, transfer softkeys the Default template must be changed for Standard User. From **Device** > **Device Settings** > **Softkey Templates**, choose **Standard User** and check the **Default Softkey Template** option.

**Note** The softkey templates that are added for Cisco Unified Communications Manager Release 10.5(1) support a description length of 100 characters.

**Important** For an upgrade from any version of Cisco Unified Communications Manager before Release 10.5(1), Cisco Unified Communications Manager retains the existing templates from the previous version, and in addition, adds the new softkey templates. It also retains the custom softkey templates (if any) from the previous version. The default template that was used before the upgrade also remains the default template after the upgrade.

# Cluster-wide Multiserver Certificate Support

From Cisco Unified Communications Manager Release 10.5(1), Unified Communications Manager adds support for multiserver certificates which allows the administrator to assign a single certificate for a given certificate unit (for example; Tomcat, CallManager, cup-xmpp, and cup-xmpp-s2s) across multiple servers in a cluster. In Cisco Unified Communications Manager Release 10.0(1) and earlier releases, the system uses a single certificate for each certificate unit on each server in a cluster. As a result of this, the administrator has to configure and maintain a number of security certificates across the deployment. Any application connecting to the system, including Jabber that validates the certificates to establish a secure connection to the servers, requires that the presented certificates are trusted. If the certificates are not trusted, the system displays a number of security warnings to the users. With signed multiserver certificates in Cisco Unified Communications Manager Release 10.5(1), the system removes these warnings and reduces the number of certificates which the administrator must configure and maintain.

**Note** The administrator can continue to use a single certificate for each certificate unit on each server in a cluster.

The following table describes the basic differences between single-server certificates and multiserver certificates.

***Table 1: Configuration Comparison of Certificates***

| Single-server Certificate | Multiserver Certificate |
|---|---|
| Contains a single Fully Qualified Domain Name (FQDN) or domain in either the Common Name (CN) field or Subject Alternative Name (SAN) extensions. | Contains multiple FQDNs or domains present in SAN extensions. |
| The system uses a single certificate for each server in a cluster. | A single certificate identifies multiple servers. |
| The administrator regenerates the certificate and private key on each individual server in situations such as certificate expiry, and private key compromise. | Because this certificate covers only one public and private key pair common to all servers, it requires secure transfer of same private key to all the servers in a cluster along with the certificate. If the private key is compromised on any server, the certificate and private key must be regenerated for all the servers. |
| Generation of a single-server certificate can add overhead for the administrator in a large cluster because the administrator needs to perform steps such as generate Certificate Signing Request (CSR), send CSR to CA for signing, and upload signed certificate for each of the servers in the cluster. | There is less overhead in managing multiserver certificates, because the administrator performs the steps only once on a given server, and the system distributes the associated private key and signed certificates to all the servers in the cluster. |

# Multiserver Certificate Overview

Subject Alternate Name (SAN) is a section defined under X.509 certificate extensions. SAN contains multiple Fully Qualified Domain Names (FQDN) or hostnames or other valid names. X.509 technology allows placing a trust in the identity of an entity such as an Internet website when it is digitally signed by a Certificate Authority (CA). The identity of a server that is on a network can be qualified by the FQDN and trusted by other clients connecting to this server. The system trusts the server because it presents an X.509-based certificate that is signed by a CA. The certificate allows the hostname or the FQDN to be included in either the Subject Name field of the certificate or the SAN field of the certificate, or in both the fields of the certificate.

The SAN field allows multiple FQDNs, domain names, or other approved names to be included in X.509 certificates so that a user does not need to generate a certificate for each server. Instead one certificate identifies multiple servers.

Unified Communications Manager supports a single CA signed certificate with SAN extensions across multiple servers for each of the Tomcat, CallManager, and IM and Presence Service services. The SAN fields are utilized and shared across multiple servers in a cluster for each of the Tomcat, CallManager, cup-xmpp, and cup-xmpp-s2s certificates. The administrator selects between single-server certificates and multiserver certificates with SAN extensions to generate a CSR, and then uploads the certificate or certificate chain.

## Multiserver Certificate Benefits

- Allows the administrator to configure the Common Name (CN) field of the certificate.
- Allows the administrator to generate a single CSR, sign a single certificate, and upload a single certificate for each service.

- Provides secure transfer of private key and CA signed certificate across all the servers in a cluster by using the Platform Administrative Web Services (PAWS) API.

The following table lists the certificate names and the servers where the respective private key and certificates are copied.

***Table 2: Certificate Names and Servers***

| Certificate | Server | Certificate usage |
|---|---|---|
| Tomcat | • Unified Communications Manager<br>• IM and Presence Service | Any applications, including Jabber clients accessing Cisco Tomcat service, use this certificate to verify the Unified Communications Manager server and IM and Presence Service server identity. |
| CallManager | Unified Communications Manager | Any applications, endpoints and Jabber clients accessing CallManager service use this certificate to verify the Unified Communications Manager server identity. |
| cup-xmpp | • IM and Presence Service | Jabber clients and Cisco AJAX XMPP Library (CAXL) clients use this certificate to verify the IM and Presence Service server identity. |
| cup-xmpp-s2s | • IM and Presence Service | This certificate is used to establish secure server-to-server connections for the IM and Presence Service XMPP interdomain federation feature. |

While generating the CSR, the administrator has the option of configuring the CN field or leaving the default value of CN for Tomcat, cup-xmpp, cup-xmpp-s2s, and CallManager (single-server or multiserver) certificates. However, the administrator cannot modify the CN for self-signed certificates. The CN has a default value assigned to it.

The default value of CN will be FQDN (if domain name is configured) or hostname (if domain name is not configured) of the server from which the request is generated for single-server or SAN-based multiserver CSR.

**Note** The administrator can configure the SAN field to add more FQDNs or domain names.

The following table lists the SAN entries for each of the certificate types.

*Table 3: Certificates and SAN Entries*

| Certificate | SAN Entries | |
|---|---|---|
| | CSR (Single-Server) | CSR (Multiserver) |
| Tomcat | • FQDN (or hostname)<br>• Network domain (if configured) | • FQDN of all Unified Communications Manager and IM and Presence Service servers in the cluster<br>• Network domains (if configured)<br>• Custom values |
| CallManager | • FQDN (or hostname)<br>• Network domain (if configured) | • FQDN of all Unified Communications Manager servers in the cluster<br>• Network domains (if configured)<br>• Custom values |
| cup-xmpp | • FQDN (or hostname)<br>• Presence domains | • FQDN of all IM and Presence Service servers in the cluster<br>• Presence domains:<br>Configure Presence domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Domains**.<br>• Custom values |

| Certificate | SAN Entries | |
|---|---|---|
| | CSR (Single-Server) | CSR (Multiserver) |
| cup-xmpp-s2s | • FQDN (or hostname)<br>• Presence domains<br>• Wildcarded Presence domains (if configured)<br>• Email domains<br>• Group Chat Server Alias | • FQDN of all IM and Presence Service servers in the cluster<br>• Presence domains:<br>Configure Presence domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Domains**.<br>• Wildcarded Presence domains (if configured):<br>Enable or disable this feature by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Settings** > **Standard Settings**.<br>• Email domains (if configured):<br>• Enable or disable the feature by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Settings** > **Standard Settings**.<br>• Configure Email domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Inter-Domain Federation** > **Email Federated Domains**.<br>• Group Chat Server Alias:<br>Configure Group Chat Server Aliases by using the **IM and Presence Server Administration** window, and selecting **Messaging** > **Group Chat Server Alias Mapping**.<br>• Custom values |

The following is an example of a Tomcat certificate setup:

- Network domain is *cisco.com*
- Nodes in the cluster are *cucm-node-01, cucm-node-02, cup-node-03*
- Email domain is *email.com*

The network domain and cluster server FQDNs are included in the CSR and subsequent signed certificate by default. The email domain must be manually added as a custom additional SAN entry. The SAN in the Tomcat certificate appears as follows:

```
Subject Alternative Names:
DNS: cucm-node-01.cisco.com, DNS: cucm-node-02.cisco.com,
DNS:cup-node-03.cisco.com, DNS: cisco.com, DNS: email.com
```

Depending on the system configuration, Jabber users who connect to the system can enter their user ID as *user@email.com*. Establishment of the secure connection and validation of the Tomcat X.509 certificate is dependent on the values in the SAN extension.

## Manage Certificates

The following topics describe the functions that you can perform for single-server and multiserver certificates from the Certificate Management menu.

Restart the following services after regenerating or uploading single-server certificates:

***Table 4: Services to Restart for Single-Server Certificates***

| Certificate | Services to Restart |
|---|---|
| CallManager | Cisco CallManager Service, Cisco TFTP Service, and all other relevant services that use CallManager certificate. |
| cup-xmpp | Cisco XCP Router |
| cup-xmpp-s2s | Cisco XCP XMPP Federation Connection Manager |

Restart the following services after regenerating or uploading multiserver certificates with SAN extensions:

***Table 5: Services to Restart for Multiserver Certificates with SAN Extensions***

| Certificate | Services to Restart |
|---|---|
| CallManager (Restart on each Unified Communications Manager server) | Cisco CallManager Service, Cisco TFTP Service, and all other relevant services that use CallManager certificate. |
| cup-xmpp (Restart on each IM and Presence server) | Cisco XCP Router |
| cup-xmpp-s2s (Restart on each IM and Presence server) | Cisco XCP XMPP Federation Connection Manager |
| Tomcat (Restart on each Unified Communications Manager and IM and Presence server | Cisco Tomcat on all the servers in the cluster |

**Note** A new section "Configure Multiserver Certificate" has been added to *Cisco Unified Communications Operating System Administration Guide*.

Configure Multiserver Certificate, on page 8

**Note** Cisco Unified Communications operating system generates multiserver certificates with SAN extensions for the Tomcat service, CallManager service, and IM and Presence Service.

For information on configuring multiserver certificates, see the *Cisco Unified Communications Operating System Administration Guide* that supports this release.

### IM and Presence Service Multiserver Certificates

For more information on Security Certificate management on IM and Presence Service, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(1)* and the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(1)*.

## Configure Multiserver Certificate

Cisco Unified Communications operating system generates multiserver certificates with SAN extensions for the Tomcat service, CallManager service, and IM and Presence Service.

The following procedure provides an overview of this process.

**Note** The detailed steps are explained in subsequent sections.

### Procedure

**Step 1** Log in to Cisco Unified Communications Operating System Administration on any Unified Communications Manager or IM and Presence Service server using your administrator password.

**Step 2** Generate a CSR on the server.

**Note** Cisco Unified Communications Operating System Administration allows the system administrator to select the distribution type when generating a CSR for the individual certificate purposes that supports the multiserver option. The system automatically populates the CSR with the required SAN entries and displays the default SAN entries on the screen. On generating a multiserver CSR, the system automatically distributes that CSR to all the required servers in the cluster. For details about certificate names and servers, see Table 2: Certificate Names and Servers, on page 4.

**Step 3** Download the CSR to your PC.

**Step 4** Use the CSR to obtain an application certificate from a CA and request that the CA sign the CSR.

**Note** Get information about obtaining a root certificate from your CA.

**Step 5** Obtain the root CA certificate or certificate chain to upload on the cluster.

**Note** Get information about obtaining a root certificate from your CA.

**Step 6** Upload the root CA certificate and signed CA certificate to the server.

During upload, the system automatically distributes the certificates to all the required servers in the cluster.

**Step 7** Restart the services that are affected by the new certificate.

**Tip** For all certificate types, restart the corresponding service (for example, restart the Cisco Tomcat service after regenerating the Tomcat certificate).

**Note** For details about the corresponding service names for each of the certificate types, see Table 5: Services to Restart for Multiserver Certificates with SAN Extensions, on page 7.

See the *Cisco Unified Communications Manager Serviceability Administration Guide* for information about restarting services.

## Generate Certificate Signing Request for Multiserver Certificate

**Note** If your deployment contains Cisco Unified Communications Manager and IM and Presence Service nodes that are installed on different network domains, you should generate the multiserver Tomcat certificate from the Unified Communications Manager node. This action ensures that the Unified Communications Manager network (parent) domain appears in the certificate.

You must generate a new certificate signing request when you want to renew a multiserver certificate.

### Procedure

**Step 1** Select **Security** > **Certificate Management**.
The **Certificate List** window appears.

**Step 2** Use the Find controls to filter the certificate list.

**Step 3** Click **Generate CSR**.

The **Generate Certificate Signing Request** window appears.

**Step 4** From the **Certificate Purpose** drop-down list, select the required certificate purpose.

**Step 5** From the **Distribution** drop-down list, select **Multi-server (SAN)**.

**Note** The Multi-server (SAN) option is available only when you select either Tomcat, CallManager, cup-xmpp or cup-xmpp-s2s from the **Certificate Purpose** drop-down list.

**Note** By default, the system populates the CN field with the server FQDN (or hostname). You can modify the value, if required. For self-signed certificate, the CN is not configurable.

**Step 6** From the **Key Length** drop-down list, select **1024** or **2048**.

**Step 7** From the **Hash Algorithm** drop-down list, select **SHA1** or **SHA256**.

**Step 8** Click **Generate** to generate a new CSR.

**Note** The new CSR that is generated for a specific certificate type overwrites any existing CSR for that type. The CSR is automatically distributed to all the required servers in the cluster.

See Table 2: Certificate Names and Servers, on page 4 to get the list of the certificate names and the servers where the respective private key and certificates are copied.

### Download Certificate Signing Request for Single-Server and Multiserver Certificate

**Procedure**

**Step 1** Select **Security** > **Certificate Management**.

The **Certificate List** window appears.

**Step 2** From the list, click the Common Name of the entry with the type **CSR Only** and a Distribution value matching the Common Name.

**Note** For the multiserver SAN certificate, click the Common Name of the entry with type **CSR Only** and a Distribution value of **Multi-Server (SAN)**.

The **CSR Details** window appears.

**Step 3** Click **Download CSR**.

**Step 4** After the CSR download completes, click **Close**.

# SAML Single Sign-On

The following content has been added to the "SAML Single Sign-On counters" table in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Cisco Unified Communications Manager Release 10.5(1) supports SAML-based Single Sign-On. Unified RTMT displays seven additional counters that are functional in Cisco Unified Communications Manager Release 10.5(1).

**Note** In Cisco Unified Communications Manager Release 10.0(1), SAML_REQUESTS and SAML_RESPONSES are the only two counters that are functional and are displayed in the Unified RTMT.

The following table contains information about SAML Single Sign-On counters.

*Table 6: SAML Single Sign-On Counters*

| Counter | Counter Description |
|---|---|
| SAML_FAILED_REQUESTS | This counter represents the number of failed or invalid SAML requests.<br>**Tip** For details on the exact failures, see one of the following logs:<br>• `ssosp000xx.log`<br>• `ssoApp.log` |
| SAML_FAILED_RESPONSES | This counter represents the number of failed or invalid SAML responses received from the configured Identity Provider.<br>**Tip** For details on the exact failures, see one of the following logs:<br>• `ssosp000xx.log`<br>• `ssoApp.log` |
| OAUTH_TOKENS_ISSUED | This counter represents the number of OAuth tokens that are issued by the administrator. |
| OAUTH_TOKENS_ACTIVE | This counter represents the number of OAuth tokens that are currently active in the Token store. |
| OAUTH_TOKENS_VALIDATED | This counter represents the number of times OAuth tokens are validated. |
| OAUTH_TOKENS_EXPIRED | This counter represents the number of OAuth tokens that are removed from the Token store upon expiry. |
| OAUTH_TOKENS_REVOKED | This counter represents the number of OAuth tokens that are revoked by the administrator. |

**Note** When a user requests a new token from the same client, the existing token is lost and is no longer valid. The authorization service issues a new token that replaces the previous token. The token that is lost or replaced is not registered in any of the available counters.

The following content has been added to the "SAML Single Sign-On" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

### SAML Single Sign-On

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

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

- Unified Communications Self Care Portal

### Enable SAML SSO

**Note** After you enable SAML SSO, you can log in to the following applications directly from the default page:

- Cisco Unified Reporting
- Cisco Unified Serviceability

# JTAPI Support for Single Sign-On

**Note** The following information is for JTAPI developers.

With Cisco Unified Communications Manager Release 8.5(1), JTAPI can authenticate applications using Single Sign-On (SSO) Tickets and with Unified Communications Manager Release 10.0(1), JTAPI can also authenticate applications using an SSO Cookie.

With Unified Communications Manager Release 10.5(1), JTAPI and CTI expands SSO support to include authentication using a standard based SAML OAuth token.

Single Sign-On provides the following advantages:

- Simplifies Access
- Centralizes Credential Management
- Eliminates Password Resets
- Is secure
- Integrates with Multivendor Identity Provider (IdP)
- SSO is a cluster-wide setting that can be enabled after an installation or upgrade to Release 10.5(1).
- Application user login procedure does not change. JTAPI Applications using Application accounts can only log in with username and password.
- Applications using LDAP Synchronized User accounts can log in with either username and password or Oauth token when SSO is enabled.
- Oauth token authentication is not supported for locally configured user accounts.
- JTAPI supports the use of an SSO Oauth token for both secure and non-secure connections.
- The application must provide the SSO Oauth token in the providerString for initializing and receiving the Provider object.

### Details

A JTAPI provider is established using the method getProvider(String provStr) on a JtapiPeer object. The mode of authentication is governed by the format of the provider string, which is passed as an argument to this method.

**General format**

**username/password authentication:**

serverIP;login=<userName>;passwd=<password>;

For example:

John/Cisco123

serverIP;login=John;passwd=Cisco123;

**SSO Oauth token authentication:**

For example:

token “abcde”

serverIP;ssooauthtoken=abcde;

severIP;ssooauthtoken=<oAuthToken>;

### Sample Code

```
//application gets SSOoAuthToken
String oAuthToken = tokenFetchedByApp;
//Create provider string in the required format
String providerString = ctiserverIP + ";ssooauthtoken=" + oAuthToken +";";
JtapiPeer peer = JtapiPeerFactory.getJtapiPeer ( null );
try {
         Provider provider = peer.getProvider (providerString);
} catch (Exception exp ){
//Exception handling code
}
```

## Acquire the Single Sign-On Token

Complete the following procedure to acquire the Single Sign-On (SSO) Oauth token.

### Procedure

**Step 1** Determine the SSO feature status. Applications should use the following URL to determine whether the SSO feature is enabled.

For example: https://<anyPublisherOrSubscriberIP>:8443/ssosp/ws/public/singlesignon.

The response <Status enabled="true"/> indicates if SSO is enabled. <anyPublisherOrSubscriberIP> is the IP address of any Unified Communications Manager Publisher or Subscriber node.

**Result**:

```
<SSOResult>
<ErrorCode>0</ErrorCode>
<Response>
<SingleSignOn version="10.5.0.98000-77">
<Status enabled="true"/>
```

```
<Token reuse="false"/>
<Uri>https://<anyPublisherOrSubscriberIP>:8443/ssosp/oauth/authorize</Uri>
</SingleSignOn>
</Response>
</SSOResult>
```

**Step 2** If the SSO status = true, parse the <URI> response and add the mandatory parameters:

https://<anyPublisherOrSubscriberIP>:8443/ssosp/oauth/authorize.

**Supported Parameters:**

response_type=token (mandatory) Value *must* be 'token' in Unified Communications Manager Release 10. If a client passes a value other than 'token', the request is rejected with the error 'unauthorized_client'.

client_id=C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94 (mandatory) JTAPI applications *must* pass this OAuth client_id. UC 10.0 does not support client_id registration, so all JTAPI applications will use "C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94". If an unrecognized client_id is passed, the request is rejected with the error 'unauthorized_client'.

**Example:**

https://10.10.10.10:8443/ssosp/oauth/authorize?
response_type=token&client_id=C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94
&token_type=Bearer

**Step 3** Obtain an Oauth token by issuing a request through a WebView/Browser.

Redirection to the IDP occurs automatically from the /ssosp/oauth/authorize API. Enter your password and the token is returned to the WebView/Browser.

**Result:**

Within the browser/webview, the connecting client is redirected to the redirect_uri with the OAuth access token as a parameter.

**Step 4** After successfully authenticating, parse the 'access_token' value from the response. Copy the entire value for access_token up to the '&'. This token is used in the getProvider (providerString) for the 'ssooauthtoken' parameter.

**Result:**

https://10.10.10.10:8433/ssosp/publicoauthcb#access_token=
Mjo4YFiNTJmNy1JyZRmLTRjMTQtYTNmMy1jNDgyYzQ2NjcyOGM&token_type=Bearer&expires_in=3600

Access token from the result above: Mjo4YFiNTJmNy1JyZRmLTRjMTQtYTNmMy1jNDgyYzQ2NjcyOGM

## Interface Changes for Single Sign-On Oauth Support

### Interface CiscoJtapiException

Three new fields are added in CiscoJtapiException for SSO Oauth support.

### Declaration

public interface CiscoJtapiException

### Fields

*Table 7: Fields in public static final int*

| Interface | Field | Description |
|---|---|---|
| public static final int | CTIERR_OAUTH_TOKEN_UNAUTHORIZED | This error code is returned if the Oauth token is expired and the application tries to reopen provider with same oauth token. |
| public static final int | CTIERR_INVALID_OAUTH_TOKEN | This error code is returned if the Oauth token is invalid. |
| public static final int | CTIERR_OAUTH_SERVER_NOT_REACHABLE | This error code is returned if the Oauth server is not reachable for validation. |

## Use Cases for Single Sign-On Oauth Support

*Table 8: Successful Authentication Using an SSO Oauth Token*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD>";); | ProvInServiceEv | Provider object is returned to application. |

*Table 9: Valid SSO Oauth Token with a UserId and Password*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken along with UserId and Password<br>JtapiPeer.getProvider(“ServerIP;login=<br><UserId>;passwd=<br><password>ssooauthtoken=<<br>ssoOauthTokenfromAD>”;); | ProvInServiceEv | Provider object is returned to application. But the authentication is done based on ssooauthtoken and the userid and password are ignored by JTAPI. |

*Table 10: Application Specifies Invalid Oauth Token but a Correct Userid and Password in API*

| Action | Event | Result |
|---|---|---|
| Application specifies invalid token but correct userid and password in API<br>JtapiPeer.getProvider("ServerIP;login=<br><UserId>;passwd=<br><password>ssooauthtoken=<<br>ssoOauthTokenfromAD>";); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_OAUTH_TOKEN |

*Table 11: Application Specifies an Empty Oauth Token*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an empty SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD >;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_PARAMETER |

*Table 12: Application Specifies an Invalid Token*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an empty SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>Any Invalid Token>;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_OAUTH_<br>TOKEN |

*Table 13: Application Tries to Open the Provider with Oauth Token but OauthServer Is Not Reachable by the CTI for Validation*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>Any Invalid Token>;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_OAUTH_SERVER_<br>NOT_REACHABLE |

*Table 14: Failover Scenario*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD >;");<br>CTI failover happens | ProvInServiceEv<br>ProvOutOfServiceEv<br>ProvInServiceEv | Provider object is returned to application.<br>ProvOutOfServiceEv is reported to the application for current CTI node.<br>JTAPI will connect to the next CTI node with the same SSO Oauth token as used earlier since that token has not expired.<br>If the token has expired for the next open provider then the application has to re-initialize the JTAPI with a fresh Oauth token. |

*Table 15: Successful Authentication Using an SSO Oauth Token for Secured Scenario*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken, Fully Qualified Directory Name of client certificate, and the server certificate<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<br><ssooauthtokenfromAD>;ClientCert=<FQDN client<br>certificate>;ServerCert=< FQDN servercertificate >" | ProvInServiceEv | Secured connection is set up between JTAPI and CTI node.<br>Provider object is returned to application. |

# TAPI Support for Single Sign-On

**Note** The following information is for TAPI developers.

With Cisco Unified Communications Manager Release 10.5(1), the Cisco TSP client is enhanced to support authentication using Single Sign-On (SSO).

Using Single Sign-On provides the following advantages:

- Simplifies access
- Centralizes Credential Management
- Eliminates password resets
- Is Secure
- Integrates with Multivendor Identity Provider (IdP)

The Cisco TSP client can be configured to use either a static password, as in previous releases, or to use Single Sign-On.

If the Cisco TSP client is configured to use an Application Account or a local User account, configure the password in the client.

If the Cisco TSP client is configured to use an LDAP Synchronized User Account and Single Sign-On is enabled for the Cisco Unified Communications Manager cluster, choose Single Sign-On.

When Single Sign-On is selected and the TAPI application is opened, the Cisco TSP client automatically attempts to acquire the OAuth token needed to access CTI Manager. For a first-time login and when the token expires, a browser window appears asking the user to provide Single Sign-On credentials.

### UI Enhancements for Cisco TSP-Installer

TSP Notifier is now a required component and is installed automatically during a fresh installation or upgrade regardless of SSO settings. For each desired TSP Instance, the CiscoTSP Installer UI is enhanced to allow the user to select either Single Sign-On or Username/Password as the authentication type during a fresh installation.

The default authentication type for a fresh installation is Single Sign-On.

You can select **Use the following Credentials** to change the authentication type to Username/Password from SSO.

If you want to change the authentication type after installation is complete, access the Cisco TSP Configuration-User Tab UI and select the authentication type you want to use.

During an upgrade of an older Cisco TSP client to a new Cisco TSP client, the authentication type of the end user is retained from the previous configuration of the CiscoTSP client that is being upgraded.

If you choose to add a fresh TSP instance during the upgrade, the newly added TSP instance is completely configurable and you can select the authentication type as either SSO or Username\Password.

### Silent Installation

The new parameter **AUTH** is added to the existing Silent Install Command line, to specify Authentication type during installation.

#### Examples

Customer information:

- USER ID = bob
- PASSWORD = cisco123

CTI-Manager configuration:

- CTIManager1= 1.1.1.1 (ipv4) , 1:1:1:1:1:1 (ipv6), cti-dev-94.cisco.com (hostname)
- CTI1_TYPE = Ipv4 , Ipv6 , Host

#### Authentication Type: User Credentials

Silent install for end user : bob with Authentication Type : User Credentials , Primary CTIManager IP address : 1.1.1.1 and IP addressing mode : IPV4

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1**= CTIManager address **CTI1_TYPE=IPV4"**

- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1=1.1.1.1 CTI1_TYPE=IPV4"**

Silent install for end user : bob with Authentication Type : User Credentials , Primary CTIManager IP address : 1:1:1:1:1:1 and IP addressing mode : IPV6

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1**= CTIManager address **CTI1_TYPE=IPV6"**
- Command Line for a 64-bit machine :**CiscoTSPx64.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1=1.1.1.1 CTI1_TYPE=IPV6"**

**Authentication Type: Single Sign On**

Silent install for end user : bob with Authentication Type : Single Sign On, Primary CTIManager IP address : 1.1.1.1 and IP addressing mode : IPV4

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1 CTI1_TYPE=IPV4"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1 CTI1_TYPE=IPV4"**

Silent install for end user : bob with Authentication Type : Single Sign On, Primary CTIManager IP address: 1:1:1:1:1:1 and IP addressing mode : IPV6

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1.1.1 CTI1_TYPE=IPV6"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1.1.1 CTI1_TYPE=IPV6"**

Silent install for end user : bob with Authentication Type : Single Sign On , Primary CTIManager IP address : cti-dev-94.cisco.com and IP addressing mode : Hostname

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=cti-dev-94.cisco.com CTI1_TYPE=HOST"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=cti-dev-94.cisco.com CTI1_TYPE=HOST"**

For more information about Silent Installation, see “Silent Installation of Cisco Unified CM TSP” in the *TAPI Developer Guide*.

### Limitations

Authentication using a Single Sign-On is not supported when multiple instances of TSP are configured.

Users must log out of the operating system when they switch accounts (for example, Microsoft switch user feature is not supported).

### Interface Changes

The following messages can appear in the tool tip box of CiscoTSPNotifier when failures occur:

- Unified CM TSP SSO OAUTH Authentication failed – Token Unauthorized
- Unified CM TSP SSO OAUTH Authentication failed – Invalid Token
- Unified CM TSP SSO OAUTH failed – Server is not Reachable
- Unified CM TSP SSO OAUTH Fetch failed – SSO is Disabled on Server

- Unified CM TSP SSO OAUTH Fetch failed – OAUTH Invalid message
- Unified CM TSP SSO OAUTH Fetch failed – Receive TimeOut
- Unified CM TSP SSO OAUTH Fetch failed – SSO Status
- Unified CM TSP SSO OAUTH Fetch failed – SSO Token

## TAPI Use Cases for Single Sign-On Support

The following are TAPI use cases for Single Sign-On Support.

***Table 16: Successful Authentication Using an SSO OAuth Token***

| Action | Result |
|---|---|
| **1.** The application performs LineInitialize().<br>**2.** Provide the correct user credentials in the popup window. | The dialog automatically closes and an OAuth Token is acquired. The application connects to CTI and the provider opens. |

***Table 17: Provider Opens When SSO OAuth Token Is Already Present***

| Action | Result |
|---|---|
| The application performs LineInitialize(). | Application connects to CTI and the provider opens. |

***Table 18: Change Authentication Method From Username and Password to SSO***

| Action | Result |
|---|---|
| **1.** The application performs LineInitialize().<br>**2.** Change the authentication method to SSO.<br>**3.** Provide the correct user credentials in the popup window. | The dialog automatically closes and the OAuth Token is acquired. The application connects to CTI and the provider opens. |

***Table 19: Failover Scenario***

| Action | Result |
|---|---|
| **1.** The application performs LineInitialize().<br>**2.** Provide the correct user credentials in the popup window.<br>**3.** Stop the CTI Manager of the publisher. | TSP automatically connects to the subscriber (using the SSO Oauth token already acquired).<br>Failover to the backup node occurs. |

***Table 20: Successful Authentication Using an SSO OAuth Token for a Secured Scenario***

| Action | Result |
|---|---|
| **1.** The application performs LineInitialize().<br>**2.** Provide the correct user credentials in the popup window. | The dialog automatically closes and the OAuth Token is acquired. The application connects to CTI through a secure connection and Provider opens. |

*Table 21: Provider Opens When Notifier Is Not Running*

| Action | Result |
|---|---|
| The application performs LineInitialize(). | The TSP LineInitialize() fails with proper error. (Failure is permanent.) |

*Table 22: Provider Opens Without Providing User Credentials*

| Action | Result |
|---|---|
| 1. The application performs LineInitialize().<br>2. Do not provide any credentials in the popup window and wait for some time. | TSP notifier sends an error to the TSP and then the TSP retrys the connection.<br>TSPNOTIFIER_ERR_OAUTH_TOKEN_FETCH_FAILURE (Failure is temporary.) |

*Table 23: Provider Opens with Invalid User Credentials*

| Action | Result |
|---|---|
| 1. The application performs LineInitialize().<br>2. Provide invalid user credentials in the popup window. | A new popup window appears.<br>“Invalid user credentials” error message appears. |

*Table 24: Provider Opens Using SSO on a Cisco Unified Communications Manager Where SSO Is Not Enabled*

| Action | Result |
|---|---|
| The application performs LineInitialize(). | The provider fails to open and the error message "SSO is not enabled on the CUCM" appears. |

*Table 25: SSO OAuth Token Expires After CTIManager Failover Fallback*

| Action | Result |
|---|---|
| 1. The application does a LineInitialize().<br>2. Provide the correct user credentials in the popup window.<br>3. Wait for the SSO OAuth token to expire.<br>4. Stop the CTI Manager of the publisher. | Application automatically connects to the CTI Manager of the subscriber and the popup window appears requesting credentials because the token has expired. |

# Web Dialer Single Sign-On Support

With Release 10.5(1), the Web Dialer interface supports Single Sign-On (SSO). After you activate SSO on the cluster, Web Dialer SSO is enabled along with all other web applications that support SSO. For more information about activating Single Sign-On, see the *Features and Services Guide for Cisco Unified Communications Manager*.

Applications that use Web Dialer interface are backward compatible with earlier releases of Cisco Unified Communications Manager. They may use SSO or continue to use Username and Password, independent of

SSO. For more information about using the Web Dialer interface with Single Sign-On, go to: `http://developer.cisco.com/web/webdialer`.

# SIP Best Effort Early Offer

SIP Early Offer means media negotiation is initiated in the SIP INVITE request and concluded in the 200 OK response. Delayed Offer means media negotiation is initiated in the 200 OK response and concluded in the subsequent ACK request. Although support for Delayed Offer is mandated by IETF RFC 3261, some SIP products cannot respond appropriately to Delayed Offer.

Early Offer requires a complete session description, which may not be available at the time of the INVITE request.

Cisco Unified Communications Manager Release 10.5(1) provides the following configuration options for SIP Early Offer support:

- Early Offer Mandatory—Early Offer is always sent. Accordingly, an MTP will be inserted to provide a complete session description protocol (SDP) at the time of outbound INVITE if calling-side media information is unavailable. When calling-side media information is available, an MTP will not be inserted. This configuration option is part of the existing Early Offer support for voice and video calls.
- Best Effort Early Offer—Does not insert an MTP but sends a Delayed Offer INVITE if a complete session description is not available.
- Early Offer Disabled—In this case, Delayed Offer is used exclusively.

The following table provides an overview of the interactions between the different configuration options.

***Table 26: Configuration Interactions***

| SIP Profile Early Offer Support Configuration | Calling-Side Media Information Available? | MTP Inserted? | Outbound INVITE |
|---|---|---|---|
| Early Offer Mandatory | No | Yes | Early Offer |
| Early Offer Mandatory | Yes | No | Early Offer |
| Best Effort Early Offer | No | No | Delayed Offer |
| Best Effort Early Offer | Yes | No | Early Offer |
| Early Offer Disabled | No | No | Delayed Offer |
| Early Offer Disabled | Yes | No | Delayed Offer |

The following sections include the benefits of Best Effort Early Offer, the modified SIP trunk setup procedure, and the new settings that have been added to the SIP Profile.

# SIP Best Effort Early Offer Benefits

Best Effort Early Offer on a SIP trunk allows a SIP trunk to send an Early Offer without inserting an MTP, while preserving the ability of the SIP trunk to fallback to Delayed Offer when calling-side media information is unavailable at the time of outbound INVITE. The insertion of a media termination endpoint (MTP) is avoided, in this case.

Best Effort Early Offer provides the following benefits:

- Best Effort Early Offer on a SIP ICT preserves the capability of the destination cluster to send an Early Offer without inserting an MTP. For example, if cluster A sends an Early Offer, the destination cluster of the SIP trunk (cluster B) can send an Early Offer on another SIP trunk without inserting an MTP, the same behavior as the Early Offer Mandatory configuration option. With the new Best Effort Early Offer setting, if cluster A sends a Delayed Offer on the SIP trunk, cluster B can send a Delayed Offer and not insert an MTP. In contrast, If the outbound SIP trunk on cluster B is configured as Early Offer Mandatory, cluster B is forced to insert an MTP to make an Early Offer.
- Best Effort Early Offer avoids premature MTP insertion in cases where it may not be necessary.
- Best Effort Early Offer preserves video and secure media in cases where MTP insertion is not necessary.
- Best Effort Early Offer provides the best interoperability with the least MTP usage.

# Set Up SIP Trunk

**Procedure**

**Step 1** Choose **Device** > **Device Settings** > **SIP Profile** and select an existing SIP profile.

**Step 2** Copy the SIP profile.

**Step 3** In the **Name** field, enter a new name for the profile.

**Step 4** From the **Early Offer support for voice and video calls** drop-down list, choose one of the following:

- Disabled (Default value)
- Best Effort (no MTP inserted)
- Mandatory (insert MTP if needed)

**Step 5** Click **Save**.

**Step 6** Choose **Device** > **Trunk** and choose the SIP profile you want to assign to a SIP Trunk.

**Step 7** From the **Trunk Configuration** window, click **Reset**.

# SIP Profile Settings

The following field has been added for the SIP Best Effort Early Offer feature.

| Field | Description |
|---|---|
| Early Offer support for voice and video calls | This field configures Early Offer support for voice and video calls. When enabled, Early Offer support includes a session description in the initial INVITE for outbound calls. Early Offer configuration settings on SIP profile apply only to SIP trunk calls. These configuration settings do not affect SIP line-side calls. If this profile is shared between a trunk and a line, only a SIP trunk that uses the profile is affected by these settings.<br><br>Because End to End RSVP provides an early offer, the Early Offer and End to End RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose End to End from the RSVP Over SIP drop-down list, the Early Offer support for voice and video calls drop-down list is disabled.<br><br>The Media Transfer Point (MTP) Required check box on the Trunk Configuration window, if enabled, overrides the early offer configuration on the associated SIP profile. Cisco Unified Communications Manager sends the MTP IP address and port with a single codec in the Session Description Protocol (SDP) in the initial INVITE.<br><br>From the drop-down list, select one of the following three options:<br>• Disabled (Default value)—Disable Early Offer; no SDP will be included in the initial INVITE for outbound calls.<br>• Best Effort (no MTP inserted)<br>  • Provide Early Offer for the outbound call only when the caller side media port, IP and codec information are available.<br>  • Provide Delayed Offer for the outbound call when caller side's media port, IP address, and codec information is not available. No MTP is inserted to provide Early Offer in this case.<br>• Mandatory (insert MTP if needed)—Provide Early Offer for all outbound calls and insert MTP when caller side's media port, IP and codec information is not available. |

The following fields have been changed for the SIP Best Effort Early Offer feature.

| Field | Description |
|---|---|
| Send send-receive SDP in mid-call INVITE | Check this check box to prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services.<br><br>**Note** This check box applies only to Early Offer or Best Effort Early Offer-enabled SIP trunks and has no impact on SIP line calls.<br><br>When a SIP INVITE message with a=inactive, sendonly, or recvonly in the audio media line is received on a SIP trunk and sent on a tandem SIP trunk with this check box and `either form of` Early Offer enabled, Cisco Unified Communications Manager inserts an MTP to provide an SDP with a=sendrcv in the SIP INVITE message that is sent on the tandem SIP trunk. Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of the media path by sending either a delayed INVITE or mid-call INVITE with send-recv SDP.<br><br>When you enable both **Send send-receive SDP in mid-call INVITE** and **Require SDP Inactive Exchange for Mid-Call Media Change** on the same SIP profile, the **Send send-receive SDP in Mid-Call INVITE** setting overrides the **Require SDP Inactive Exchange for Mid-Call Media Change** setting. For SIP line-side calls, the **Send send-receive SDP in mid-call INVITE** check box is not applicable; the **Require SDP Inactive Exchange for Mid-Call Media Change** check box applies when enabled.<br><br>**Note** To prevent the SDP mode from being set to Inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (**System** > **Service Parameters, Cisco CallManager**) to True. |

| Field | Description |
|---|---|
| Require SDP Inactive Exchange for Mid-Call Media Change | This feature designates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers.<br><br>If the box is checked, during mid-call codec or connection updates Cisco Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint cannot react to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls.<br><br>**Note** For Early Offer or Best Effort early offer-enabled SIP trunks, this parameter will be overridden by the Send send-receive SDP in mid-call INVITE parameter.<br><br>If the box is unchecked, Cisco Unified Communications Manager passes the mid-call SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. This is the default behavior. |

# Daylight Saving Time Rules

Unified Communications Manager supports daylight saving time (DST) changes for a time zone. DST rules describe DST start and end dates for a time zone annually.

The Unified Communications Manager server generates a new DST rules file every year with DST start and end time for all countries in accordance with the calender year.

The following conditions apply for DST rules file generation:

- If the Unified Communications Manager server is powered on, the DST rules file is generated for the current year at 00:00 hours on January 1 and the Cisco TFTP service is restarted automatically.
- If the Unified Communications Manager server is not powered on January 1, the DST rules file is generated for the current year during servers boot up and the Cisco TFTP service is restarted automatically.
- Administrators can generate the DST rules file manually by executing the command `utils update dst` using the command line interface (CLI).

# DST-CiscoSyslog Messages

The following table describes CiscoSyslog messages for DST.

| CiscoSyslog message | Description | Process | Resolution |
|---|---|---|---|
| DST rules file for the current year is created from the cron job.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if the cron job generates the DST rules file successfully. | Cron Job | Ensure phones are restarted after the file is generated. |
| An attempt was made to create the DST rules file from the cron job.<br>DST rules file already created for current year. | This message is displayed if the cron job attempts to generate a new DST rules file even when the file for the current year is already generated. | Cron Job | |
| Cron job failed to create the DST rules file for the current year.<br>Execute **'utils update dst'** to create the DST rules file. | This message is displayed if the cron job fails to generate the DST rules file successfully. | Cron Job | Enter the **utils update dst** from CLI to create the DST rules file. |
| The DST rules file for the current year is created during server reboot.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if server reboot generates the DST rules file successfully. | Bootup Script | Ensure that phones are restarted after the file is generated. |
| An attempt was made to create the DST rules file during server reboot.<br>DST rules file already created for current year. | This message is displayed if server reboot attempts to generate a new DST rules file even when the file for the current year is already generated. | Bootup Script | |
| Server reboot failed to create DST rules file for the current year.<br>Execute **'utils update dst'** to create the DST rules file. | This message is displayed if server reboot fails to generate the new DST rules file successfully. | Bootup Script | Enter the **utils update dst** from CLI to create the DST rules file. |

| CiscoSyslog message | Description | Process | Resolution |
|---|---|---|---|
| DST rules file for the current year is created from CLI.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if the CLI generates the DST rules file successfully. | CLI | Ensure that phones are restarted after the file is generated. |
| An attempt was made to create DST rules file from CLI.<br>DST rules file already created for the current year. | This message is displayed if the CLI attempts to generate a new DST rules file even when the file for the current year is already generated. | CLI | |
| CLI failed to create DST rules file for the current year. | This message is displayed if the CLI fails to generate the new DST rules file successfully. | CLI | |

# utils update dst

This command updates the daylight saving time (DST) rules for the current year.

**utils update dst**

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

This command takes a backup of the existing DST rules file and creates a new DST rules file for the current year.

**Caution** Restart the phones after you execute the command. Not restarting the phones results in wrong DST start and stop dates.

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to Unified Communications Manager and IM and Presence service.

# Directory Search in Self Care

The Directory Search option under User Options in releases before 10.0(1) has been removed from the 10.0(1) release onward. However, in the Self Care Portal, the same search capability is available under Contacts and Speed Dials, both of which a user can manually create.

# Embedded Cisco TelePresence Management Suite in Self Care Portal

You can configure Unified Communications Manager to open the Cisco TelePresence Management Suite (TMS) User Portal within the Conferencing tab of the Self Care Portal.

With this configuration, when users who are configured with TelePresence select the **Conferencing** tab and then select **Schedule a Meeting**, the TMS User Portal opens inside the application interface rather than in a separate popup window.

## Enable Embedded TelePresence for Self Care Portal

Follow this procedure to embed the TMS User Portal into the Self Care Portal interface.

### Before you begin

- Configure a Video Conference Server UC Service and a Service Profile with the Video Conferencing UC Server.
- Associate the Service Profile to the end users who will use Self Care.

### Procedure

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

**Step 2** Navigate to **Self Care Portal Parameters**.

**Step 3** From the **Show Video Conference Scheduler** drop-down list, select **Show in Conferencing tab**.

**Note** If the TMS User Portal does not appear properly in the Self Care Portal, the browser may not support this function. In this case, select **Show as Browser Popup**.

The Cisco TelePresence Management Suite conferencing status will appear in the Self Care Portal window for the end user.

# IM and Presence Service Deprecation of Microsoft Exchange Server 2003

Microsoft Exchange Server 2003 is no longer supported for Cisco Unified Communications Manager IM and Presence Service, Release 10.5 and later.

# IM and Presence Service Deprecation of WebDAV

WebDAV is being deprecated from Release 10.5 and later. All clients with WebDAV configured integrations must remove WebDAV or switch to EWS before upgrading to 10.5.

# IM and Presence Service IPv6 Support

IM and Presence Service supports Internet Protocol version 6 (IPv6), which uses packets to exchange data, voice, and video traffic over digital networks. IPv6 also increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 deployment in the IM and Presence Service network functions transparently in a dual-stack IPv4 and IPv6 environment. The default network setting is IPv4.

Outbound IPv6 traffic is allowed when IPv6 is enabled. For example, SIP S2S can be configured to use either static routes or DNS queries. When a static route is configured and IPv6 is enabled, the SIP proxy attempts to establish an IPv6 connection if IPv6 IP traffic is provided. You can use IPv6 for connections to external databases, LDAP and Exchange servers, and for federation connections on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.

If the service uses DNS requests (for example, with XMPP S2S), then after receiving the list of IP addresses as the result of the DNS query, the service attempts to connect to each IP address on the list one by one. If a listed IP address is IPv6, the server establishes an IPv6 connection. If the request to establish the IPv6 connection fails, the service moves on to the next IP address on the list.

If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

For additional information about IPv6 and for network guidelines, see the following documents:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Command Line Interface Guide for Cisco Unified Communications Solutions*
- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*
- *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*

# IPv6 Configuration

To enable IPv6 for IM and Presence Service, you must perform the following tasks:

- Configure IPv6 on Eth0 for each IM and Presence Service node in the cluster using either the Cisco Unified IM and Presence OS Administration GUI or the Command Line Interface.
- Enable the IPv6 enterprise parameter for the IM and Presence Service cluster.

You must configure IPv6 for both the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node for IPv6 to be used; otherwise, the system attempts to use IPv4 for IP traffic. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

For configuration changes to the IPv6 enterprise parameter to take affect, you must restart the following services on IM and Presence Service:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

For instructions to configure IPv6 for IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

For more information about using the Command Line Interface to configure IPv6 parameters, see the *Cisco Unified Communications Manager Administration Guide* and the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

# IPv6 Interactions and Restrictions

Observe the following interactions and restrictions when configuring IPv6 on IM and Presence Service and when interacting with external IPv6 devices and networks:

- You can use IPv6 for your external interfaces on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.
- You must configure IPv6 for the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node to use IPv6; otherwise, the system attempts to use IPv4 for IP traffic on the external interfaces. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

**Note** If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

- For federation, you must enable IM and Presence Service for IPv6 if you need to support federated links to a foreign Enterprise that is IPv6 enabled. This is true even if there is an ASA installed between the IM and Presence Service node and the federated Enterprise. The ASA is transparent to the IM and Presence Service node.
- If IPv6 is configured for any of the following items on the IM and Presence Service node, the node will not accept incoming IPv4 packets and will not automatically revert to using IPv4. To use IPv4, you must ensure that the following items are configured for IPv4 if they appear in your deployment:
  - Connection to an external database.
  - Connection to an LDAP server.
  - Connection to an Exchange server.
  - Federation deployments.

# New CLI Commands

## set network ipv6 dhcp

This command sets the DHCPv6 client on the server and enables IPv6 support. For changes to take effect, you must restart the server.

**set network ipv6 dhcp enable** | **disable** [**reboot**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **dhcp** | Sets the DHCPv6 client on the server. By default, the server does not restart after you enable the DHCPv6 client. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| **enable** | Enables IPv6 support. |
| **disable** | Disables IPv6 support. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 gateway

This command sets the IPv6 gateway for the server. For changes to take effect, you must restart the server.

**set network ipv6 gateway** *addr* [**reboot**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **gateway** | Sets the IPv6 gateway for the server. By default, the server does not restart after you set the IPv6 gateway for the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | The IPv6 gateway address. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 service

This command enables or disables the IPv6 service on the server. For changes to take effect, you must restart the server.

**set network ipv6 service enable** | **disable** [**reboot**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **service** | Sets the IPv6 service on the server. By default, the server does not restart after you enable or disable the IPv6 service on the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *enable* | Enables IPv6 service on the server. |
| *disable* | Disables IPv6 service on the server. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 static_address

This command assigns the static IPv6 address to the server. For changes to take effect, you must restart the server.

**set network ipv6 static_address** *addr mask* [**reboot**]

**Syntax Description**

| Parameters | Description |
|---|---|
| **static_address** | Assigns a static IPv6 address to the server. By default, the server does not restart after you assign the static IPv6 address. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | Specifies the static IPv6 address you assign to the server. |
| *mask* | Specifies the IPv6 network mask (0-128). |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

# IM and Presence Service Support for Encrypted External Database

### User Interface

In the **Cisco Unified CM IM and Presence Administration** user interface, under **Messaging** > **External Server Setup** > **External Databases**, an Enable SSL check box and a Certificate Name drop-down list have been added to the External Database Settings area. These become active when you choose Oracle as the Database Type.

### Certificates

- When the SSL field or the Certificate drop-down field is modified, a notification to restart the corresponding service assigned to the external database is sent. A message concerning either "Cisco XCP Message Archiver" or "Cisco XCP Text Conference Manager" will be generated.
- The certificate you need to enable SSL must be uploaded to the cup-xmpp-trust store.
- Once the certificate is uploaded to the cup-xmpp-trust store, you must wait 15 minutes for the certificate to propagate to all the nodes of the IM and Presence Service cluster. If you do not wait, the SSL connection on nodes where the certificate has not propagated fails.

### System Troubleshooter

In the **Cisco Unified CM IM and Presence Administration** user interface, the results of a troubleshooting test has been made more descriptive. The test results are shown in the **System Configuration Troubleshooter** window, External Database Troubleshooter area (under **Diagnostics** > **System Troubleshooter**). The test result is also shown in the **External Database Settings** window, External Database Status area (under **Messaging** > **External Server Setup** > **External Databases**) .

The test is:

- Verify external database server connectivity (database connection check)

### Real Time Monitoring Tool (RTMT)

If the certificate is missing or has been deleted from the cup-xmpp-trust store, an alarm 'XCPExternalDatabaseCertificateNotFound' is raised in the Cisco Unified Communications Manager RTMT.

# Support Variable Extension Length and +E.164 for LDAP Directory Numbers

### Cisco Unified Communications Administrator Guide Updates

In Cisco Unified Communications Manager, use the **System** > **LDAP** > **LDAP Directory** menu path to configure LDAP directories. The following changes are applicable to the following fields in LDAP directory settings:

| 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.<br>Enter a mask value in the **Mask** text box.<br>**Note**<br>• The mask must contain numbers (0-9), X, and x. It must include at least one x or X.<br>• The mask can have + or \+ special characters only at the start position.<br>• The applied mask length is the same as the entered telephone number, even if the number of characters that are entered for the mask is longer than the telephone number.<br>• If the mask is longer then, it is applied from right to left of the entered telephone number.<br>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.<br>The DN from the next DN pool is displayed only after all the DNs from the first DN pool are assigned.<br>**Note** The **Next Candidate DN** is displayed 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. |

| Field | Description |
|---|---|
| Add DN Pool | By default, only one DN pool is available. Click this option to add more DNs to the DN pool.<br>Enter the **DN Pool Start** and **DN Pool End** values in the text box.<br>You can reorder the DN pool to prioritize the DNs that you want to assign. The DN pool values must conform to the following requirements:<br>• **DN Pool Start** and **DN Pool End** must be numbers only.<br>• DN length in **DN Pool Start** and **DN Pool End** must be identical with a maximum length of 20 characters excluding + or \+.<br>• **DN Pool Start** and **DN Pool End** can have + or \+ special characters only at the start position.<br>• **DN Pool End** must be greater than **DN Pool Start**,<br>• **DN Pool Start** and **DN Pool End** must not be null,<br>• DN range is between 0 to 10,000,000.<br>You can create only three DN pools. |

# Voice Gateway Support

The following gateways are supported by Cisco Unified Communications Manager release 10.0 - 10.5. For this release, documentation has been added.

- Cisco Integrated Services Router 4451-X
- Cisco VG310 Analog Phone Gateway
- Cisco VG320 Analog Phone Gateway
- Cisco VG350 Analog Phone Gateway

The following sections summarize gateway support in Cisco Unified Communications Manager.

## Cisco Voice Gateways (ISR) 44XX Series

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 44XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and PRI using SIP or H.323

### Cisco ISR44XX Series Gateways

The Cisco Integrated Services Router 44XX series gateways are Integrated Services Router family gateways with multi-core capability.

The key features of the gateways are:

- Runs on BinOS in different cores.
- Provides Services Integration for Wide area application services (WAAS), Application Firewall, Video, Application Visibility, and so on in different cores.
- Provides manageability to the next level.

### Cisco Integrated Services Router 4451-X

The Cisco Integrated Services Router 4451-X is a modular router, with LAN and WAN connections, that is configured by means of interface modules, Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The router provides encryption acceleration, voice and video capable architecture, application firewall, call processing, and embedded services.

The Cisco ISR 4451-X supports different wired interfaces such as T1 CAS/PRI and E1/PRI signaling using MGCP, T1/PRI and PRI using SIP or H.323, and fiber Gigabit Ethernet.

## Cisco Voice Gateways

Cisco Unified Communications Manager supports several types of Cisco Unified Communications gateways. Gateways use call-control protocols to communicate with the PSTN and other non-IP telecommunications devices, such as private branch exchanges (PBXs), key systems, analog phones, fax machines, and modems.

Trunk interfaces specify how the gateway communicates with the PSTN or other external devices by using time-division-multiplexing (TDM) signaling. Cisco Unified Communications Manager and Cisco gateways use a variety of TDM interfaces, but supported TDM interfaces vary by gateway model.

The following list provides available interfaces that Cisco Unified Communications Manager supports with MGCP gateways:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- T1 Channel Associated Signaling (CAS) recEive and transMit or ear and mouth (E&M)
- Basic Rate Interface (BRI) Q.931
- T1 PRI-North American ISDN Primary Rate Interface (PRI)
- E1 PRI-European ISDN Primary Rate Interface (PRI)

The following list provides available interfaces that Cisco Unified Communications Manager supports with H.323 gateways:

- FXO
- FXS
- E&M
- Analog Direct Inward Dialing (DID)
- Centralized Automatic Message Accounting (CAMA)
- BRI Q.931

- BRI QSIG-Q signaling protocol that is based on ISDN standards
- T1 CAS FXS, FXO, and E&M
- T1 FGD
- T1/E1 PRI
- T1 PRI NFAS
- T1/E1 QSIG
- J1

The following list provides available interfaces that Cisco Unified Communications Manager supports with SCCP gateways:

- FXS

Cisco Unified Communications Manager can use H.323 gateways that support E1 CAS, but you must configure the E1 CAS interface on the gateway.

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 44XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and PRI using SIP or H.323
- Analog FXS, FXO and BRI using MGCP
- Analog FXS and BRI using SCCP
- Analog FXS, FXO and BRI using SIP or H.323

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 43XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and E1/PRI using SIP or H.323
- Analog FXS, FXO and BRI using mgcp
- Analog FXS and BRI using sccp
- Analog FXS, FXO and BRI using SIP or H.323

## Standalone Voice Gateways

This section describes these standalone, application-specific gateway models that are supported for use with Cisco Unified Communications Manager.

### *Cisco VG310 Analog Phone Gateway*

The Cisco VG310 is a medium-density 24-FXS port standalone Analog Voice Gateway that allows analog phones, TDM PBXs, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports OPX-Lite analog ports, T1 CAS/PRI, E1/PRI , T1/PRI, PRI and BRI interfaces using SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

*Cisco VG320 Analog Phone Gateway*

The Cisco VG320 is a medium-density 48-FXS port standalone Analog Voice Gateway that allows analog phones, TDM PBXs, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports OPX-Lite FXS analog ports, T1 CAS/PRI, E1/PRI, T1/PRI, PRI and BRI interfaces using SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

*Cisco VG350 Analog Phone Gateway*

The Cisco VG350 is a high density 144 standard FXS port and 96 OPX-Lite FXS port standalone Analog Voice Gateway. It allows analog phones, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports four EHWIC slots for additional FXS, FXO ports, SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

## Voice Gateway Model Summary

The following table summarizes Cisco voice gateways that Cisco Unified Communications Manager supports with information about the supported signaling protocols, trunk interfaces, and port types.

***Table 27: Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types***

| Gateway Model | Supported Signaling Protocols | Trunk Interfaces | Port Types | Notes |
|---|---|---|---|---|
| Cisco ISR 4451-X | MGCP | T1/CAS/PRI<br>E1/PRI | | |
| | H.323 and SIP | T1/CAS/PR<br>PRI | | |
| Cisco VG310 | MGCP | T1/CAS/PRI<br>E1/PRI | FXS/FXO | |
| | H.323 and SIP | T1/CAS/PRI<br>PRI | | |
| Cisco VG320 | MGCP | T1/CAS/PRI<br>E1/PRI | FXS/FXO | |
| | H.323 and SIP | T1/CAS/PRI<br>PRI | | |
| Cisco VG350 | MGCP | T1/CAS/PRI<br>E1/PRI | FXS/FXO | |

| Gateway Model | Supported Signaling Protocols | Trunk Interfaces | Port Types | Notes |
|---|---|---|---|---|
| | H.323 and SIP | T1/CAS/PRI<br>PRI | | |

# New CLI Commands

**Related Topics**

utils update dst, on page 28

## utils vmtools refresh

This command refreshes the currently installed VMware Tools to the latest version that is prescribed by the ESXi host for that VM.

**Note** This is applicable for native vmtools.

**utils vmtools refresh**

**Command Modes** Administrator (admin:)

**Usage Guidelines** To update the current version of the VMware Tools, select **Guest** > **Install/Upgrade VMWare Tools** > **Interactive Tools Upgrade**.

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

### Example

```
admin:utils vmtools refresh
VMware Tools match host. Upgrade allowed, though not required.

***   W A R N I N G   ***
Running this command will update your current version of VMware Tools
to the latest version prescribed by the ESXi host on which this VM is
running. The tools install will cause your system to reboot twice.
```

# Windows 8.1 and Windows Server 2012 R2 Support

With Cisco Unified Communications Manager Release 10.5(1), the following client applications support Windows 8.1 (32-bit and 64-bit) operating system and Windows Server 2012 R2 operating system:

- Cisco Unified TAPI Client
- Cisco Unified JTAPI Client
- Cisco Unified Real-time Monitoring Tool (RTMT)
- Cisco Unified Communications Manager Cisco Trust List (CTL) Client
- Cisco Unified Communications Manager Assistant Console

**Note** Windows User Account Control (UAC) must be disabled to run Cisco Unified CM Assistance Console on Windows 8.x.

# About Cross-Origin Resource Sharing

Cross-Origin Resource Sharing (CORS) is a function that allows JavaScript on a web page of one domain to make XMLHttpRequests to another domain. Such cross-domain requests would otherwise be forbidden by web browsers, based on the security policy. CORS defines a way in which the browser and Unified Communications Manager can interact using the User Data Service (UDS) interface to determine whether or not to allow the cross-origin request. This provides a method that is more useful than only allowing same-origin requests, and is more secure than only allowing all of these cross-origin requests.

CORS is particularly useful for web-based applications that use the UDS interface on Unified Communications Manager and the Unified Messaging interface (CUMI) on Cisco Unity Connection.

For example: A web application provides an end user with capabilities to manage their voice settings. This web application is hosted at https://domaina/webapps/vsettings.html and requires access to UDS, which is hosted on Unified Communications Manager servers. Due to cross-domain restrictions, the web application normally would be denied access to UDS because the web application and UDS are from different domains. With CORS, the system administrator using Unified Communications Manager Administration can give permission to applications that are hosted at https://domaina to access UDS.

CORS is also useful for developers who are integrating Jabber SDK and Unified Communications Manager directory services with web-based applications such as those that are provided by cloud services that are hosted in different domains. For example, a cloud service integration that needs to look up Unified Communications Manager contact information for people in an instant-messaging contact list would benefit from CORS in situations where the Unified Communications Manager domain differs from that of the cloud service.

When CORS is configured, Unified Communications Manager allows cross-domain requests like Get User or Put Credentials to succeed. When CORS is not configured, Unified Communications Manager rejects cross-domain requests.

# Configure Cross-Origin Resource Sharing

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose **System** > **Cross-Resource Sharing (CORS)**.
The Find and List Cross-Resource Sharing (CORS) web page.

**Step 2** Set the Preflight Response Cache Settings. The settings allow you to customize the amount of time that you want the verification information to remain live in the browser's cache.

**Step 3** To add a domain to access User Data Service (UDS), click **Add New**.

**Step 4** Enter the domain in the **Domain** field.

The protocol must be defined and wildcards are permitted as a standalone entry or after the protocol. For example: http://*.mycompanyinternalsite.com.

**Step 5** Enter a description in the **description** field.

**Step 6** Choose an access level. These access levels are intended to restrict the HTTP Methods that are allowed by UDS.

- Read-Only — Allows only the Get and Head methods, which are for obtaining information and not for changing it.
- Full-Access — Allows for Read-Only and adds the Post, Put, and Delete methods. If you intend your web applications to support full CRUD (Create, Read, Update, and Delete) operations, Full-Access.

**Step 7** Click **Save**.

# Configure LDAP Directory

Cisco Unified Communications Manager supports user synchronization and authentication with the following LDAP directories:

- Microsoft Active Directory 2003 R1/R2
- Microsoft Active Directory Application Mode (ADAM) 2003 R1/R2
- Microsoft Active Directory 2008 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Sun One 6.x
- Sun Directory Services 7.0
- Oracle Directory Services Enterprise Edition 11gR1 (v11.1.1.5.0)
- OpenLDAP 2.3.39 & 2.4.x

### Real-Time Measuring Tool Performance Counters for LDAP Directory

Cisco Unified Communications Manager Release 10.5 adds two new Real-Time Measuring Tool (RTMT) performance counters for LDAP Directory to help Administrators monitor account synchronization status.

**Performance Counters**

- Accounts Failed – The number of user accounts that failed to synchronize during the last directory synchronization operation.
- Accounts Synchronized – The number of user accounts successfully synchronized during the last directory synchronization operation.

# New RTMT Alert for Global Dial Plan Replication

The following Cisco Unified Real-Time Monitoring Tool alert has been added for Global Dial Plan Replication feature:

**ILSDuplicateURI**

This alert occurs when the Cisco Unified Communications Manager identifies that it has learned duplicate Universal Resource Identifier (URI) entries through Intercluster Lookup Service (ILS) during a call to the URI. Whenever there are duplicate entries for a URI, such as the URI user@example.com existing on two clusters, the call is always routed to the cluster from which the URI was first learned. Calls are not routed to the other duplicate entries.

**Default Configuration**

| Value | Default Configuration |
|---|---|
| Enable Alert | Selected |
| Severity | Alert |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when the following condition is met:<br>Duplicate URI is found in the remote cluster |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | Trigger alert when it occurs |
| Enable Email | Selected |
| Trigger Alert Action | Default |

# Silent Monitoring CLI Update

With release 10.5(1), Cisco Unified Communications Manager now supports the `set replication-sync monitor` CLI command for silent monitoring. This CLI command turns on the replication monitoring service. This command replaces the `set replwatcher monitor` CLI command from previous releases, which is no longer supported.

## Set replication-sync monitor

This command enables or disables replication monitoring by the Cisco Replication Watcher service. The Cisco Replication Watcher service blocks other services from starting until database replication is setup and functioning normally.

**set replication-sync monitor {enable | disable}**

**Syntax Description**

| Parameters | Description |
|---|---|
| **enable** | Turns on the replication monitoring service. |
| **disable** | Turns off the replication monitoring service |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

# Product-Specific Configuration in TelePresence Device User Interfaces

With this feature, users can set their product-specific configuration from certain Cisco TelePresence device interfaces. The information that the user enters is then sent to Unified Communications Manager so that the device settings are synchronized.

# 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 10.5.

*Table 28: Phone Firmware Versions*

| Phone family | Firmware release number |
|---|---|
| Cisco Unified SIP Phone 3905 | 9.4(1) |

| Phone family | Firmware release number |
|---|---|
| Cisco Unified IP Phones 6901 and 6911 | 9.3(1)SR1 |
| Cisco Unified IP Phones 6921, 6941, 6945, and 6961 | 9.4(1)SR1 |
| Cisco IP Phone 7800 Series | 10.1(1)SR1 |
| Cisco Unified IP Phone 7900 Series | 9.3(1)SR4 |
| Cisco Unified Wireless IP Phone 792x Series | 1.4(5) |
| Cisco Unified IP Conference Phone 8831 | 9.3(3) |
| Cisco Unified IP Phones 8941 and 8945 | 9.4(1)SR1 |
| Cisco Unified IP Phones 8961, 9951, and 9971 | 9.4(1)SR1 |

## Cisco Unified SIP Phone 3905 Features

No features have been introduced to the Cisco Unified SIP Phone 3905.

## Cisco Unified IP Phone 6900 Series Features

No features have been introduced to the Cisco Unified IP Phone 6901 and 6911.

The following table lists the features added to the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 for firmware release 9.4(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-6900-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Rate Limit for Multicast and Broadcast Traffic | 9.4(1)SR1 |

## Cisco IP Phone 7800 Series Features

The following table lists the features added to the Cisco IP Phone 7800 Series for firmware release 10.1(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Hardware Updates | 10.1(1)SR1 |

## Cisco Unified IP Phone 7900 Series Features

The following table lists the features added to the Cisco Unified IP Phone 7900 Series for firmware release 9.3(1)SR4. No new features were added for firmware release 9.3(1)SR3. For more information, see the Release Notes at the following location:

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

| Feature name | Firmware release |
|---|---|
| Control Default Wallpaper | 9.3(1)SR4 |
| Default Audio Path Support | 9.3(1)SR4 |
| DSP Audio Enhancement Support | 9.3(1)SR4 |
| Hardware Updates | 9.3(1)SR4 |

## Cisco Unified Wireless IP Phone 792x Series Features

No features have been introduced to the Cisco Unified Wireless IP Phone 792x Series.

## Cisco Unified IP Conference Phone 8831 Features

No features have been introduced to the Cisco Unified IP Conference Phone 8831.

## 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 releases 9.3(4) and 9.4(1). No new features were introduced for firmware release 9.4(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8900-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Adaptive Bandwidth Management | 9.4(1) |
| Bandwidth Management Enhancement | 9.3(4) |
| Configurable Volume Autosave | 9.4(1) |
| Electronic Hookswitch | 9.4(1) |
| E-SRST Service Improvements | 9.3(4) |
| Flexible DSCP Marking | 9.4(1) |
| Gateway Recording for SIP | 9.4(1) |
| Hold or Resume Toggle from Hard Key | 9.3(4) |
| Larger Font for Time and Date | 9.3(4) |
| Minimum Ring Volume | 9.3(4) |
| Peer Firmware Sharing | 9.4(1) |
| Remotely Check CTL and ITL File | 9.3(4) |

| Feature name | Firmware release |
|---|---|
| Report CTL and ITL Information | 9.3(4) |
| Ringtone and Wallpaper Customization API | 9.4(1) |
| RTCP Always On | 9.4(1) |
| Secondary Load Server | 9.3(4) |
| Serviceability for SIP Endpoints | 9.4(1) |
| Video Through PC | 9.3(4) |
| Video UI Enhancement | 9.3(4) |
| Visual Voicemail | 9.3(4) |
| W360p By Default | 9.3(4) |

## Cisco Unified IP Phones 8961, 9951, and 9971 Features

No features have been introduced to the Cisco Unified IP Phones 8961, 9951, and 9971.

# Cisco DX Series

## Cisco DX650 Firmware Versions

The following table lists the latest Cisco DX650 firmware version supported for Cisco Unified Communications Manager 10.5.

| Device | Firmware Release Number |
|---|---|
| Cisco DX650 | 10.1(2)SR1 |

### Cisco DX650 Features

The following table lists the features added to the Cisco DX650 for firmware release 10.1(2). For more information on the Cisco DX650, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Public Mode | 10.1(2) |
| Video Greetings | 10.1(2) |