



INTEGRATION GUIDE



Configuring Cisco Unified Presence Release 8.5 with Microsoft OCS for Microsoft Office Communicator Call Control

Revised: March 28, 2011

- 1** Requirements for this Integration
- 2** Overview of this Integration
- 3** License Requirements for this Integration
- 4** How to Configure Cisco Unified Communications Manager for Integration with Microsoft OCS
- 5** How to Configure Cisco Unified Presence for Integration with Microsoft OCS
- 6** How to Configure Microsoft Components for integration with Cisco Unified Presence
- 7** How to Configure the Normalization Rules on Microsoft Active Directory
- 8** How to Configure the Security Certificate for Cisco Unified Presence
- 9** How to Configure Security Between Cisco Unified Presence and Microsoft OCS
- 10** Setting Up Redundancy for this Integration
- 11** How to Deploy the Phone Selection Plug-in
- 12** Getting More Information

1 Requirements for this Integration

This module describes the configuration steps for integrating Cisco Unified Presence with Microsoft Office Communications Server or Microsoft Live Communications Server for Microsoft Office Communicator (MOC) call control.



Note This module describes the procedure for integrating Cisco Unified Presence with Microsoft Office Communications Server (OCS). Use this module as a guide for setting up this integration between Cisco Unified Presence and Microsoft Live Communications Server (LCS).

Software Requirements

- Cisco Unified Presence Server Release 8.0.x, 8.5.x
- Cisco Unified Communications Manager Server Release 6.x, 7.x or 8.x
- Microsoft Office Communications (OCS) 2007 or 2007 R2 Server, Standard or Enterprise
- Microsoft Live Communications (LCS) 2005 Server, Standard or Enterprise
- Microsoft Office Communicator (MOC)
- Microsoft Windows Server
- (Optional) Cisco CSS 11500 Content Services Switch

Refer to the *Hardware and Software Compatibility Information for Cisco Unified Presence* for software compatibility information with Cisco Unified Communications Manager.

For this integration it is assumed that you have the following installed and configured:

- A Cisco Unified Presence server that is set up and configured as described in the *Deployment Guide for Cisco Unified Presence*.
- The Cisco Unified Presence server must be correctly deployed with a Cisco Unified Communications Manager (CUCM) server as described in the *Deployment Guide for Cisco Unified Presence*.
- A Microsoft OCS or LCS server that is set up and configured as per the requirements defined in the Microsoft documentation.

2 Overview of this Integration

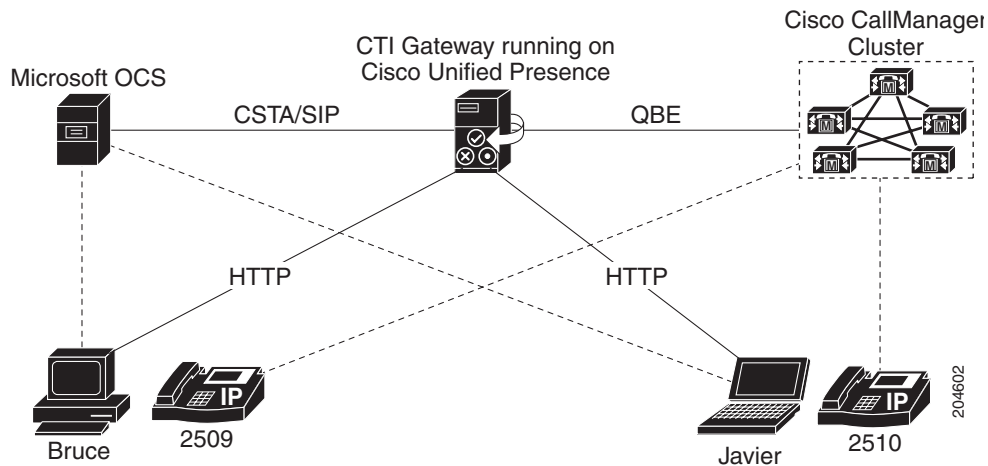
- [How this Integration Works, page 2](#)
- [Line Appearances, page 4](#)

How this Integration Works

Cisco Unified Presence allows enterprise users to control their Cisco Unified IP Phone through Microsoft Office Communicator, a third party desktop IM application. The Microsoft Office Communicator client for this integration can run on either Microsoft Live Communications Server (LCS) 2005 or Microsoft Office Communications Server (OCS) 2007.

Microsoft Office Communicator sends session-initiating requests to the CTI Gateway on Cisco Unified Presence to control Cisco Unified IP Phones registered in Cisco Unified Communications Manager, as illustrated in [Figure 1](#). The CTI Gateway forwards the requests to the CTI Manager on Cisco Unified Communications Manager. The Cisco Unified Communications Manager returns the events to the Microsoft Office Communicator application using the same path in the opposite direction.

Figure 1 Integration Overview



Cisco Unified Presence supports CTI connections with up to eight Cisco Unified Communications Manager nodes; you can configure up to eight CTI connection addresses on Cisco Unified Presence.

Microsoft Office Communicator sends session initiating requests to Cisco Unified Presence. These requests are routed in a round-robin sequence to the CTI connection addresses configured on Cisco Unified Presence. For example, the first request is routed to first CTI node, second request to next CTI node and so on. Priority is assigned to CTI connection addresses in the order in which they are configured. If a dual node Cisco Unified Presence cluster is deployed, you must use a load balancer. In this scenario, the load balancer sends the session initiating requests in a round-robin sequence from Microsoft Office Communicator clients to the Cisco Unified Presence publisher and subscriber nodes. There is a maximum of two nodes in a Cisco Unified Presence cluster when it is configured to support Microsoft Office Communicator Remote Control Client.

In a dual node Cisco Unified Presence cluster, a load balancer can be used to round-robin the session initiating requests sent from Microsoft Office Communicator clients to the publisher and subscriber Cisco Unified Presence nodes.

When the CTI Gateway on Cisco Unified Presence starts, it connects to all CTI connection addresses in the configured list, and monitors these connections by sending periodic heartbeat messages. When a Microsoft Office Communicator user signs in, Microsoft OCS sends a SIP INVITE request with a CSTA body to the CTI Gateway to monitor the Cisco Unified IP Phone for the user. The CTI Gateway creates a session for that Microsoft Office Communicator user, and uses the load balancing mechanism to send session initiating requests from that user to any of the CTI connection addresses.

Once the CSTA application session is established, Microsoft Office Communicator and CTI Gateway exchange a sequence of SIP INFO messages for activities such as monitoring devices, making calls, transferring calls, or changing the status of controlling devices. This message exchange is sent over the same CTI connection address with which the initial session was established.

If connection to any of the CTI Managers fails, outbound call requests from Microsoft Office Communicator are returned until the connection comes back into service. If a Cisco Unified Communications Manager node is down, the CTI Gateway will make periodic attempts to re-establish a connection to it. When the Cisco Unified Communications Manager node comes back in service, the CTI Gateway will reconnect to it and monitor the connection. In this case, when Microsoft OCS sends an (in-session) SIP INFO request, the CTI Gateway will have a different CTI Manager connection ID because of a new connection. Microsoft Office Communicator sends a new SIP INVITE message, but the Microsoft Office Communicator user is not required to sign in again.

Related Topics

- [Line Appearances, page 4](#)
- [Setting Up Redundancy for this Integration, page 27](#)

Line Appearances

When a user selects a phone to use with the remote call control feature, on Cisco Unified Presence the user is selecting a *line appearance* to control through Microsoft Office Communicator. A line appearance is the association of a line with a device. On Cisco Unified Communications Manager, the administrator can associate a device with multiple lines, and a line with multiple devices. Typically it is the role of the Cisco Unified Communications Manager administrator to configure line appearances by specifying the lines and devices that are associated with each other.

Related Topics

- [User and Device Configuration on Cisco Unified Communications Manager, page 5](#)

3 License Requirements for this Integration

Table 1 describes the user and server license requirements for the Cisco Unified Presence MOC call control feature.

Table 1 *Cisco Unified Presence license requirements*

License Requirement	Description
Cisco Unified Presence user feature license	You will require a Cisco Unified Presence user license for each MOC call control user. This will consume one Cisco Unified Communications Manager Device License Unit (DLU). On Cisco Unified Communications Manager, you will need to upload the user DLU, and then assign Cisco Unified Presence capabilities for a user.
Cisco Unified Presence server license	You will require one proxy server license for the Cisco Unified Presence server. You must upload this license to the publisher Cisco Unified Presence server.

See the *Deployment Guide for Cisco Unified Presence* for information on configuring the license requirements for Cisco Unified Presence.

Related Topics

- *Deployment Guide for Cisco Unified Presence:*
http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

4 How to Configure Cisco Unified Communications Manager for Integration with Microsoft OCS



Note Note that because menu options and parameters may vary per Cisco Unified Communications Manager releases, see the Cisco Unified Communications Manager documentation appropriate to your release.

- [User and Device Configuration on Cisco Unified Communications Manager, page 5](#)
- [Adding Users to a Standard CCM User Group, page 5](#)
- [Configuring an Application User for the CTI Gateway, page 6](#)
- [Adding the Application User to a CTI-Enabled User Group, page 6](#)
- [Assigning CTI Device Control to the Application User, page 7](#)

User and Device Configuration on Cisco Unified Communications Manager

Before you configure Cisco Unified Communications Manager for integration with Microsoft OCS, you need to complete the user and device configuration on Cisco Unified Communications Manager. You need to configure the phone devices, configure the users, and then associate a device with each user.

You also need to associate a line to a device, or for users of the Extension Mobility feature, to a device profile. This association forms a line appearance. When a user is associated to the device or to a device profile, the line appearance is associated to the user.

Task	Menu path
Configure the phone devices, and associate a primary extension with each device	Cisco Unified Communications Manager Administration > Device > Phone
Configure the users, and associate a device with each user	Cisco Unified Communications Manager Administration > User Management > End User.
Associate a user with a line appearance	Cisco Unified Communications Manager Administration > Device > Phone



Note If you are running Cisco Unified Presence release 7.0.3 or a later release, you no longer need to associate a primary extension with each device on Cisco Unified Communications Manager.

Related Topics

- [Line Appearances, page 4](#)
- Cisco Unified Communications Manager documentation:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

What To Do Next

[Adding Users to a Standard CCM User Group, page 5](#)

Adding Users to a Standard CCM User Group

Before You Begin

Make sure you have completed the prerequisite user and device configuration on Cisco Unified Communications Manager.

Procedure

Step 1 Select Cisco Unified Communications Manager Administration > User Management > End User.

Step 2 Select Find.

Step 3 Perform the following actions:

- a. Select the user to view the End User Configuration window.
- b. Select **Add to User Group**.
- c. Select **Find**.
- d. Check **Standard CCM End Users**.
- e. Select **Add Selected**.
- f. Select **Save** on the End User Configuration window.

Step 4 Repeat step three for each user that you want to add to the user group.

Related Topics

- [User and Device Configuration on Cisco Unified Communications Manager, page 5](#)

What To Do Next

[Configuring an Application User for the CTI Gateway, page 6](#)

Configuring an Application User for the CTI Gateway

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration > User Management > Application User**.

Step 2 Select **Add New**.

Step 3 Enter an application user name in the User ID field, for example, **CtiGW**.

Step 4 Enter a password for this application user, and confirm the password.

Step 5 Select **Save**.

What To Do Next

[Adding the Application User to a CTI-Enabled User Group, page 6](#)

Adding the Application User to a CTI-Enabled User Group

Before You Begin

Configure an Application user for the CTI Gateway.

Procedure

Step 1 Select **Cisco Unified Communications Manager Administration > User Management > User Group**.

Step 2 Select **Find**.

Step 3 Select **Standard CTI Enabled**.

Step 4 Select **Add Application Users to Group**.

Step 5 Select the Application user that you created for the CTI Gateway.

Step 6 Select **Add Selected**.

Step 7 Select **Save**.

Related Topics

- [Configuring an Application User for the CTI Gateway, page 6](#)

What To Do Next

[Assigning CTI Device Control to the Application User, page 7](#)

Assigning CTI Device Control to the Application User

Before You Begin

Configure an Application user for the CTI gateway.

Procedure

- Step 1** Select **Cisco Unified Communications Manager Administration > User Management > User Group**.
 - Step 2** Select **Find**.
 - Step 3** Select **Standard CTI Allow Control of All Devices**.
 - Step 4** Go back to User Groups Find list.
 - Step 5** If you are deploying an RT model of Cisco Unified IP phones, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
 - Step 6** Select **Add Application Users to Group**.
 - Step 7** Select the Application user that you created for the CTI Gateway.
 - Step 8** Select **Add Selected**.
-

Related Topics

- [Configuring an Application User for the CTI Gateway, page 6](#)
- [Adding the Application User to a CTI-Enabled User Group, page 6](#)

5 How to Configure Cisco Unified Presence for Integration with Microsoft OCS

- [Configuring the Service Parameters, page 7](#)
- [Configuring an Incoming Access Control List, page 8](#)
- [Configuring the Routing Settings, page 8](#)
- [How To Configure the Desk Phone Control Settings, page 8](#)

Configuring the Service Parameters

The SIP message routing from Cisco Unified Presence to Microsoft Office Communicator is based on the Record-Route header added by Microsoft OCS in the initial request. Cisco Unified Presence resolves the hostname in the Record-Route header to an IP address and routes the SIP messages to the Microsoft Office Communicator client.

In addition the transport type on Cisco Unified Presence should be the same as the transport type configured on Microsoft OCS for the Cisco Unified Presence route (either TLS or TCP respectively).

Procedure

- Step 1** Select **Cisco Unified Presence Administration > System > Service Parameters**.
- Step 2** Select the Cisco Unified Presence server,
- Step 3** Select the service **Cisco UP SIP Proxy**.
- Step 4** Verify that the following parameters are configured correctly:
 - The **Proxy Domain** parameter value must define the enterprise top-level domain name (e.g. "example.com"). This parameter specifies which URIs are treated as local and handled by this Cisco Unified Presence installation. Other SIP requests may be proxied.

- Enable the **Add Record-Route Header** parameter.
- Enable the **Use Transport in Record-Route Header** parameter.
- The **SIP Route Header Transport Type** parameter value must be set to the same type as the transport parameter configured on Microsoft OCS for the Microsoft OCS to Cisco Unified Presence route.

Step 5 Select Save.

What To Do Next

[Configuring an Incoming Access Control List, page 8](#)

Configuring an Incoming Access Control List

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Security > Incoming ACL**.

Step 2 Select **Add New**.

Step 3 Enter a description in the **Description** field.

Step 4 Enter IP address, host name, or Fully Qualified Domain Name (FQDN) of the associated Microsoft OCS server in the **Address Pattern** field.

Step 5 Select **Save**.

What To Do Next

[Configuring the Routing Settings, page 8](#)

Configuring the Routing Settings

Procedure

Step 1 Select **Cisco Unified Presence Administration > Presence > Routing > Settings**.

Step 2 Select **On** for **Method/Event Routing Status**.

Step 3 Select **Default Cisco SIP Proxy TCP Listener** for the **Preferred Proxy Server**.

Step 4 Select **Save**.

What To Do Next

[How To Configure the Desk Phone Control Settings, page 8](#)

How To Configure the Desk Phone Control Settings

- [Configuring the CTI Connections on Cisco Unified Presence, page 9](#)
- [Assigning User Capabilities, page 10](#)
- [Running the Desk Phone Control Troubleshooter, page 10](#)

Configuring the CTI Connections on Cisco Unified Presence

Before You Begin

Obtain the username and password that you configured for the Application user account on the associated Cisco Unified Communications Manager server for the CTI Gateway.

Procedure

Step 1 Select **Cisco Unified Presence Administration > Application > Desk Phone Control > Settings**.

Step 2 Select **On** from the Application Status menu.

Step 3 Enter the CTI Gateway application username and password.



Tip The username and password are case sensitive and must match what is configured on Cisco Unified Communications Manager.

Step 4 Enter a value (in seconds) for the heartbeat interval. This is the length of time between heartbeat messages sent from Cisco Unified Presence to the Cisco Unified Communications Manager nodes to monitor the CTI connections.

Step 5 Enter a value (in seconds) for the session timer. This is the session timer for the Microsoft Office Communicator sign-in session.

Step 6 Select the type of Microsoft server you are using from the Microsoft Server Type menu.

Step 7 As required, enter the IP address of each Cisco Unified Communications Manager node with which you want to establish a CTI connection.



Note You can configure a CTI connection with up to eight Cisco Unified Communications Manager nodes. These nodes must all belong to the same Cisco Unified Communications Manager cluster.]

Step 8 Select **Save**.

Troubleshooting Tips

- If you select **MOC server OCS** as the Microsoft Server Type, you must install the Phone Selection plug-in on Microsoft Office Communicator for any users who use more than one line appearance for remote call control. The Phone Selection plug-in adds a tab to the Microsoft Office Communicator client that enables the user to select a line appearance to control.
- If you select **MOC server LCS** as the Microsoft Server Type, the remote call control feature uses the existing device selection logic on Cisco Unified Presence to determine the device to control.

Related Topics

- [Configuring an Application User for the CTI Gateway, page 6](#)
- [How to Deploy the Phone Selection Plug-in, page 28](#)
- [Running the Desk Phone Control Troubleshooter, page 10](#)

What To Do Next

[Assigning User Capabilities, page 10](#)

Assigning User Capabilities

Procedure

- Step 1** Select [Cisco Unified Presence Administration > Application > Desk Phone Control > User Assignment](#).
 - Step 2** Select [Find](#).
 - Step 3** Check the users to whom you want to assign the desk phone capabilities.
 - Step 4** Select [Assign Selected Users](#).
 - Step 5** Check [Enable Desk Phone Control](#) in the Desk Phone Control Assignment window.
 - Step 6** Select [Save](#).
-

Troubleshooting Tips

- Make sure that you have assigned desk phone control capabilities to each Microsoft Office Communicator user.
- If you are using LCS with the remote call control feature, you can configure a maximum of two associated devices per user on Cisco Unified Communications Manager. If the user is signed into an Extension Mobility (EM) device, the EM device is counted as one of the two permitted associated devices for the user.

What To Do Next

[How to Configure Microsoft Components for integration with Cisco Unified Presence, page 10](#)


Related Topics

- [Configuring the CTI Connections on Cisco Unified Presence, page 9](#)
- [Running the Desk Phone Control Troubleshooter, page 10](#)

Running the Desk Phone Control Troubleshooter

The Desk Phone Control Troubleshooter validates the configuration that supports the integration of the Microsoft Office Communicator client with Cisco Unified Presence.

Procedure

- Step 1** Select [Cisco Unified Presence Administration > Diagnostics > Desk Phone Control Troubleshooter](#).
 - Step 2** Enter a valid user ID.
-  **Tip** Select [Search](#) to find the ID for a user.
-
- Step 3** Enter the Microsoft OCS server address.
 - Step 4** Select [Submit](#).
-

6 How to Configure Microsoft Components for integration with Cisco Unified Presence

- [Line URI Configuration on Microsoft Active Directory, page 11](#)
- [User Authentication on Cisco Unified Presence, page 11](#)
- [Configuring Microsoft Active Directory, page 12](#)

- [Microsoft OCS Configuration Overview, page 13](#)

Line URI Configuration on Microsoft Active Directory

Before you configure the Line URI parameter on Microsoft Active Directory, note the following:

- For the Line URI, we recommend that you use the format: `tel:xxxx;phone-context=dialstring`
 - `xxxx` also specifies the directory number that the CTI Manager reports to Cisco Unified Presence as the calling or called number when a call gets placed.
 - `phone-context=dialstring` enables the Microsoft Office Communicator client to control one of the devices that are associated with the directory number.
- If you configure the device ID, the Microsoft Office Communicator client controls that particular device on initial sign in; for example: `tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5`
- If you configure the partition, the Microsoft Office Communicator client specifies the partition for the directory number; for example: `tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5;partition=myPartition`
- The Line URI only takes effect when the Microsoft Office Communicator user signs in.
- After initial sign in, the Microsoft Office Communicator user can change the line appearance that they wish to control using the Phone Selection plug-in.
- If you do not configure the device ID in the Line URI, the CTI Gateway determines the devices that are associated with the line Directory Number (DN). If only one device is associated with the line DN, the CTI Gateway uses that device.
- If you deploy Microsoft LCS, and you do not configure the device ID in the Line URI, and two devices are associated with the line DN (shared line), the CTI Gateway uses the following rules to select a device:
 - If one of the two devices is Cisco IP Communicator and its status is registered, CTI Gateway uses that device.
 - If one of the two devices is Cisco IP Communicator, but it is not registered, CTI Gateway uses the alternate hard device.
 - If none of the two devices is Cisco IP Communicator, both phones will ring when the Microsoft Office Communicator user signs in. The user must answer a phone to control that device.
 - If more than two devices are associated with a line DN, you must specify the desired device in the Line URI.

Related Topics

- [Line Appearances, page 4](#)
- [User Authentication on Cisco Unified Presence, page 11](#)
- [How to Deploy the Phone Selection Plug-in, page 28](#)

User Authentication on Cisco Unified Presence

When configuring the SIP URI on Microsoft Active Directory, consider how Cisco Unified Presence performs the user authentication checks. The user authentication logic is as follows:

1. Cisco Unified Presence checks if the Microsoft Office Communicator (sign in) user ID matches the Cisco Unified Communications Manager user ID. If Cisco Unified Presence cannot find a match:
2. Cisco Unified Presence checks if the Microsoft Office Communicator user email (the From header) matches the Cisco Unified Communications Manager user email. If Cisco Unified Presence cannot find a match:
3. Cisco Unified Presence checks if the Microsoft Office Communicator user email matches the `ocsPrimaryAddress` value of a Cisco Unified Communications Manager user.

For example, a user Joe has the Microsoft Office Communicator user ID `joe@someCompany.com`. The From header in the SIP INVITE is `sip:joe@someCompany.com`.

In this case, Cisco Unified Presence checks the following:

- If there is a user in the Cisco Unified Communications Manager database whose user ID is 'joe'. If this user ID does not exist:

- If there is a user in the Cisco Unified Communications Manager database whose mail is 'joe@someCompany.com'. If this mail does not exist:
- If there is a user in the Cisco Unified Communications Manager database whose ocsPrimaryAddress is 'sip:joe@someCompany.com'.

Configuring Microsoft Active Directory

Before You Begin

- Read the topic describing Line URI configuration on Microsoft Active Directory.
- Read the topic describing the user authentication checks on Cisco Unified Presence.

Procedure

-
- Step 1** From the Microsoft Active Directory application window, add a user name and the telephone number that are associated with each particular user.
- Step 2** For each of the users that you added, open the Properties window on Microsoft Active Directory and configure the following parameters:
- a. Enable the user for the Office Communications Server.
 - b. Enter the SIP URI.
 - c. Enter the Microsoft OCS server name or pool.



Caution

Ensure the OCS server name or pool name does not contain the underscore character.

- d. Under Telephony Settings, select **Configure**.
 - e. Check **Enable Remote call control**.
 - f. Enter the Remote Call Control SIP URI; for example, sip:8000@my-cups.my-domain.com, where my-cups.my-domain.com specifies the FQDN of the Cisco Unified Presence server that you configured for this integration.
 - g. Enter the Line URI value.
-

Troubleshooting Tips

- The SIP URI that you enter on Microsoft Active Directory must match the static route URI that you define when you are configuring static routes on Microsoft OCS.

Related Topics

- [Line URI Configuration on Microsoft Active Directory, page 11](#)
- [User Authentication on Cisco Unified Presence, page 11](#)
- [Line Appearances, page 4](#)
- Microsoft Windows Server Active Directory documentation:
<http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx>

What To Do Next

[Microsoft OCS Configuration Overview, page 13](#)

Microsoft OCS Configuration Overview



Note This topic provides a brief outline of the configuration required on Microsoft OCS for this integration. A detailed description of Microsoft OCS configuration is out of the scope of this module. Please refer to the Microsoft OCS documentation for this information.

Make sure that the Microsoft OCS server is properly installed and activated. Make sure that the following items are configured on Microsoft OCS:

- Certificate configuration
- Static Routes
- Authorized Host
- Domain Name Server
- Pool Properties
- Server Properties
- Pool Users
- User Configuration
- Microsoft Office Communicator (MOC) Configuration

Related Topics

- [Configuring the Normalization Rules on Microsoft Active Directory, page 13](#)
- [How to Configure the Security Certificate for Microsoft OCS, page 21](#)
- [Configuring a TLS Route for Cisco Unified Presence on Microsoft OCS, page 25](#)
- [Configuring Cisco Unified Presence as an Authenticated Host on Microsoft OCS, page 26](#)
- Microsoft OCS documentation:
<http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx>

7 How to Configure the Normalization Rules on Microsoft Active Directory

- [Configuring the Normalization Rules on Microsoft Active Directory, page 13](#)
- [Verifying the Username Displays on the Microsoft Office Communicator Interface, page 14](#)
- [Sample Normalization Rules, page 15](#)

Configuring the Normalization Rules on Microsoft Active Directory

A reverse look-up of a directory number to username does not work under these conditions:

- a Microsoft Office Communicator user is controlling the Cisco Unified IP Phone
- there is an incoming voice call to that user
- the directory number for the user is configured as E.164 in the Active Directory
- Active Directory phone number normalization rules are not set up

Under these conditions, the application identifies the call as coming from an extension number, and the username will not display in Microsoft Office Communicator.

Therefore you must set up the correct normalization rules for the Active Directory address book on the Microsoft Office Communicator server to enable the Microsoft Office Communicator user to see name of the calling party in the popup window that displays when the call is made.



Note You must provide a normalization rule file for extension dialing. See the sample normalization rules topic for an example.

Before you Begin

The CA-signed certificate for Microsoft OCS needs to be on the Microsoft Office Communicator PC to achieve correct certificate distribution for address book synchronization. If a common CA is used to sign certificates, for example Verisign or RSA, the CA certificate may already come installed on the PC.

Procedure

Step 1 Use this directory path to add the Normalization rules to this file: C:\Program Files\Microsoft Office Communications Server 2007\Web Components\Address Book Files\Files\Company_Phone_Number_Normalization_Rules.txt

Step 2 Use this directory path to run the Address Book server (ABServer) and regenerate the Normalization rules: C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -regenUR



Note You might have to wait up to five minutes for a UR regenerate to complete successfully.

Step 3 Use this directory path to synchronize the ABServer: C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>ABServer.exe -syncnow



Note You might have to wait up to five minutes for an ABServer synchronization to complete successfully.

Step 4 After the synchronization is complete, check the Microsoft OCS server Event Viewer and verify that it indicates that the synchronization is complete.

Step 5 Test the Normalization rule on the Phone number: C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -testPhoneNorm <E164 phone number>

Related Topics

- [Sample Normalization Rules, page 15](#)

What To Do Next

[Verifying the Username Displays on the Microsoft Office Communicator Interface, page 14](#)

Verifying the Username Displays on the Microsoft Office Communicator Interface

You must verify that the user is able to see name of the calling party in the Microsoft Office Communicator popup window that displays when the call is made.

Before You Begin

Configure the normalization rules on Microsoft Active Directory.

Procedure

Step 1 Exit Microsoft Office Communicator. Do not just sign out.

Step 2 Delete the address book file contacts.db at the following location: C:\Documents and Settings\\Local Settings\Application Data\Microsoft\Communicator

Step 3 Start the Microsoft Office Communicator client and sign in again.

Step 4 Verify that galcontacts.db is created.

Step 5 Exit Microsoft Office Communicator again, sign in, and verify that the username displays in Microsoft Office Communicator.

Related Topics

- [Configuring the Normalization Rules on Microsoft Active Directory, page 13](#)
- [Sample Normalization Rules, page 15](#)

Sample Normalization Rules

```
# ++ test RTP
## PSTN:+61262637900, Extension:37XXX
# +61262637ddd
[\s()\-\.\./\+]* (61)?[\s()\-\.\./]*0?(2)\)?[\s()\-\.\./]* (6263) [\s()\-\.\./]* (7\d\d\d)
3$4;phone-context=dialstring
# ++ test1 RTP
## Site:, PSTN:+61388043300, Extension:33XXX
[\s()\-\.\./\+]* (61)?[\s()\-\.\./]*0?(3)\)?[\s()\-\.\./]* (8804) [\s()\-\.\./]* (3\d\d\d)
3$4;phone-context=dialstring
#Test input +61388043187, Test result-> tel:33187;phone-context=dialstring
# ++ test2 RTP
## PSTN:+61292929000, Extension:29XXX
[\s()\-\.\./\+]* (61)?[\s()\-\.\./]*0?(2)\)?[\s()\-\.\./]* (9292) [\s()\-\.\./]* (9\d\d\d)
2$4;phone-context=dialstring
# Test input +61292929761, test result-> tel:29761;phone-context=dialstring
```

You must provide a normalization rule file for extension dialing. For example, a sample normalization rule for three digit extension dialing is:

```
^(\d{3})
$1;phone-context=dialstring
```

Related Topics

- [Configuring the Normalization Rules on Microsoft Active Directory, page 13](#)
- [Verifying the Username Displays on the Microsoft Office Communicator Interface, page 14](#)

8 How to Configure the Security Certificate for Cisco Unified Presence

This topic is only applicable if you require a secure connection between Cisco Unified Presence and Microsoft OCS.

This topic describes how to configure security certificates using a standalone CA. If you use an enterprise CA, refer to the *Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation* at the URL below for an example of the certificate exchange procedure using an enterprise CA:

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html



Note SIP Proxy certificates (own and trust) should be X.509 version 3 compliant.

- [Configuring the Standalone Root Certificate Authority \(CA\), page 16](#)
- [Uploading the Root Certificate onto Cisco Unified Presence, page 17](#)
- [Generating a Certificate Signing Request for Cisco Unified Presence, page 18](#)

- [Downloading the Certificate Signing Request from Cisco Unified Presence, page 18](#)
- [Submitting the Certificate Signing Request on the CA Server, page 19](#)
- [Downloading the Signed Certificate from the CA Server, page 19](#)
- [Uploading the Signed Certificate to Cisco Unified Presence, page 20](#)

Configuring the Standalone Root Certificate Authority (CA)

Procedure

Step 1 Sign in to the CA server with Domain Administrator privileges.

Step 2 Insert the Windows Server 2003 CD.

Step 3 Select **Start > Settings > Control Panel**.

Step 4 Double-click **Add or Remove Programs**.

Step 5 Select **Add/Remove Windows Components**.

Step 6 Select **Application Server**.

Step 7 Select **Internet Information Services (IIS)**.

Step 8 Complete the installation procedure.

Step 9 Select **Add/Remove Windows Components**.

Step 10 Select **Certificate Services**.

Step 11 Select **Next**.

Step 12 Select **Standalone root CA**.

Step 13 Select **Next**.

Step 14 Type the name of the CA root.



Note This name can be a friendly name for the CA root in the forest root.

Step 15 Change the time to the number of years required for this certificate.

Step 16 Select **Next** to begin installation.

Step 17 Select the location for the certificate database and the certificate database files.

Step 18 Select **Next**.

Step 19 Select **Yes** when prompted to stop IIS.

Step 20 Select **Yes** when prompted with a message regarding Active Server Pages.

Step 21 Select **Finish**.

What To Do Next

[Downloading the Root Certificate from the CA Server, page 16.](#)

Downloading the Root Certificate from the CA Server

Before You Begin

Configure the Standalone Root Certificate Authority.

Procedure

- Step 1** Sign in to your CA server and open a web browser.
 - Step 2** Open the URL http://<ca_server_IP_address>/certsrv.
 - Step 3** Select on **Download a CA certificate, certificate chain, or CRL**.
 - Step 4** Select **Base 64** for the Encoding Method.
 - Step 5** Select **Download CA Certificate**.
 - Step 6** Save the certificate file certnew.cer to the local disk.
-

Troubleshooting Tips

If you do not know the Subject Common Name (CN) of the root certificate, you can use an external certificate management tool to find out. On Windows operating system, you can right-click the certificate file with a .cer extension and open the certificate properties.

Related Topics

- [Configuring the Standalone Root Certificate Authority \(CA\), page 16](#)

What To Do Next

[Uploading the Root Certificate onto Cisco Unified Presence, page 17](#)

Uploading the Root Certificate onto Cisco Unified Presence

Before You Begin

Download the Root Certificate from the CA Server.

Procedure

- Step 1** Copy the certnew.cer file to the local computer that you use to administer the Cisco Unified Presence server.
- Step 2** Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
- Step 3** Select **Upload Certificate**.
- Step 4** Select **cup-trust** from the Certificate Name menu.



Note Leave the Root Name field blank.

- Step 5** Select **Browse**.
- Step 6** Locate the certnew.cer file on your local computer.



Note You may need to change the certificate file to a .pem extension.

- Step 7** Select **Upload File**.



Tip Make a note of the new CA certificate filename you have uploaded to the cup-trust using the Certificate Management Find screen. This certificate filename (without the .pem or .der extension) is the value you enter in the 'Root CA' field when uploading the CA-signed SIP proxy certificate.

Related Topics

- [Downloading the Root Certificate from the CA Server, page 16](#)
- [Uploading the Signed Certificate to Cisco Unified Presence, page 20](#)

What To Do Next

[Generating a Certificate Signing Request for Cisco Unified Presence, page 18](#)

Generating a Certificate Signing Request for Cisco Unified Presence

Before You Begin

Upload the Root Certificate onto Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Select **Generate CSR**.

Step 3 Select **cup** from the **Certificate Name** menu.

Step 4 Select **Generate CSR**.

Related Topics

- [Uploading the Root Certificate onto Cisco Unified Presence, page 17](#)

What To Do Next

[Downloading the Certificate Signing Request from Cisco Unified Presence, page 18](#)

Downloading the Certificate Signing Request from Cisco Unified Presence

Before You Begin

Generate a Certificate Signing Request for Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Operating System Administration > Security > Certificate Management**.

Step 2 Select **Download CSR**.

Step 3 Select **cup** from the **Certificate Name** menu.

Step 4 Select **Download CSR**.

Step 5 Select **Save** to save the **cup.csr** file to your local computer.

Related Topics

- [Generating a Certificate Signing Request for Cisco Unified Presence, page 18](#)

What To Do Next

[Submitting the Certificate Signing Request on the CA Server, page 19](#)

Submitting the Certificate Signing Request on the CA Server

Before You Begin

Download the Certificate Signing Request from Cisco Unified Presence.

Procedure

- Step 1** Copy the certificate request file cup.csr to your CA server.
 - Step 2** Open the URL <http://local-server/certsrv> or <http://127.0.0.1/certsrv>.
 - Step 3** Select Request a certificate.
 - Step 4** Select Advanced certificate request.
 - Step 5** Select Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
 - Step 6** Using a text editor like Notepad, open the cup self-certificate that you generated.
 - Step 7** Copy all information from and including
-----BEGIN CERTIFICATE REQUEST
to and including
END CERTIFICATE REQUEST-----
 - Step 8** Paste the content of the certificate request into the Certificate Request text box.
 - Step 9** Select Submit.
The Request ID number displays.
 - Step 10** Open Certificate Authority in Administrative Tools.
The Certificate Authority window displays the request you just submitted under Pending Requests.
 - Step 11** Right-click on your certificate request.
 - Step 12** Select All Tasks > Issue.
 - Step 13** Select Issued certificates and verify that your certificate has been issued.
-

Related Topics

- [Downloading the Certificate Signing Request from Cisco Unified Presence, page 18](#)

What To Do Next

[Downloading the Signed Certificate from the CA Server, page 19](#)

Downloading the Signed Certificate from the CA Server

Before You Begin

Submit the Certificate Signing Request on the CA Server.

Procedure

- Step 1** Open http://<local_server>/certsrv on the Windows server that CA is running on.
- Step 2** Select View the status of a pending certificate request.
- Step 3** Select the option to view the request that was just submitted.
- Step 4** Select Base 64 encoded.
- Step 5** Select Download certificate.

- Step 6** Save the signed certificate to the local disk
- Step 7** Rename the certificate `cup.pem`.
- Step 8** Copy the `cup.pem` file to your local computer.
-

Related Topics

- [Submitting the Certificate Signing Request on the CA Server, page 19](#)

What To Do Next

[Uploading the Signed Certificate to Cisco Unified Presence, page 20](#)

Uploading the Signed Certificate to Cisco Unified Presence

Before You Begin

Download the Signed Certificate from the CA Server.

Procedure

- Step 1** Select **Cisco Unified Operating System Administration > Security > Certificate Management**.
- Step 2** Select **Upload Certificate**.
- Step 3** Select `cup` from the **Certificate Name** menu.
- Step 4** Specify the root certificate name. The root certificate name must contain the `.pem` or `.der` extension.
- Step 5** Select **Browse**.
- Step 6** Locate the signed `cup.pem` certificate on your local computer.
- Step 7** Select **Upload File**.
-

Related Topics

- [Downloading the Signed Certificate from the CA Server, page 19](#)

What To Do Next

[How to Configure the Security Certificate for Microsoft OCS, page 21](#)

9 How to Configure Security Between Cisco Unified Presence and Microsoft OCS

This topic is only applicable if you require a secure connection between Cisco Unified Presence and Microsoft OCS.

- [How to Configure the Security Certificate for Microsoft OCS, page 21](#)
- [Configuring a TLS Route for Cisco Unified Presence on Microsoft OCS, page 25](#)
- [Configuring Cisco Unified Presence as an Authenticated Host on Microsoft OCS, page 26](#)
- [Configuring Microsoft OCS to use TLSv1, page 26](#)
- [Creating a new TLS Peer Subject for Microsoft OCS on Cisco Unified Presence, page 27](#)
- [Adding the TLS Peer to the Selected TLS Peer Subjects List on Cisco Unified Presence, page 27](#)

How to Configure the Security Certificate for Microsoft OCS

- [Downloading the CA Certification Chain, page 21](#)
- [Installing the CA Certification Chain, page 21](#)
- [Submitting the Certificate Request on the CA Server, page 22](#)
- [Approving and Installing the Certificate, page 23](#)
- [Configuring the Installed Certificate, page 24](#)

Downloading the CA Certification Chain

Procedure

- Step 1** Select **Start > Run**.
- Step 2** Perform the following actions:
- a. Type `http://<name of your Issuing CA Server>/certsrv`.
 - b. Select **OK**.
- Step 3** Click **Download a CA certificate, certificate chain, or CRL** from **Select a task**.
- Step 4** Select **Download CA certificate chain**.
- Step 5** Select **Save** in the **File Download** dialog box.
- Step 6** Save the file on a hard disk drive on your server.
-

Troubleshooting Tips

The certificate file has an extension of .p7b. If you open this .p7b file, the chain will have the following two certificates:

- name of Standalone root CA certificate
- name of Standalone subordinate CA certificate (if any)

What To Do Next

[Installing the CA Certification Chain, page 21](#)

Installing the CA Certification Chain

Before You Begin

Download the CA Certification Chain.

Procedure

- Step 1** Select **Start > Run**.
- Step 2** Perform the following actions:
- a. Enter `mmc`.
 - b. Select **OK**.
- Step 3** Select **File > Add/Remove Snap-in**.
- Step 4** Select **Add** in the **Add/Remove Snap-in** dialog box.
- Step 5** Select **Certificates** in the list of **Available Standalone Snap-ins**.
- Step 6** Select **Add**.
- Step 7** Select **Computer account**.

- Step 8** Select **Next**.
- Step 9** Perform the following actions from the **Select Computer** dialog box:
- Ensure **Local computer: (the computer this console is running on)** is selected.
 - Select **Finish**.
 - Select **Close**.
 - Select **OK**.
- Step 10** Expand **Certificates (Local Computer)** in the left pane of the **Certificates** console.
- Step 11** Expand **Trusted Root Certification Authorities**.
- Step 12** Right-click **Certificates**.
- Step 13** Perform the following actions:
- Point to **All Tasks**.
 - Select **Import**.
- Step 14** Select **Next** in the **Import Wizard**.
- Step 15** Select **Browse** and locate the certificate chain on your computer.
- Step 16** Select **Open**.
- Step 17** Select **Next**.
- Step 18** Leave the default value **Place all certificates in the following store** selected.
- Step 19** Ensure **Trusted Root Certification Authorities** appears under the **Certificate store**.
- Step 20** Select **Next**.
- Step 21** Select **Finish**.
-

Related Topics

- [Downloading the CA Certification Chain, page 21](#)

What To Do Next

[Submitting the Certificate Request on the CA Server, page 22](#)

Submitting the Certificate Request on the CA Server

Before You Begin

Install the CA Certification Chain.

Procedure

- Step 1** On the computer requiring a certificate, open a Web browser.
- Step 2** Enter the URL `http://<name of your Issuing CA server>/certsrv`.
- Step 3** Select **Enter**.
- Step 4** Select **Request a Certificate**.
- Step 5** Select **Advanced certificate request**.
- Step 6** Select **Create and submit a request to this CA**.
- Step 7** Select **Other** in the **Type of Certificate Needed** list.
- Step 8** In the **Name** field of the **Identifying Information** section, enter the **FQDN**. The name must match the name of the Microsoft OCS, which is usually the **FQDN**.
- Step 9** In the **OID** field, type the following **OID**: `1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2`.



Note A comma separates the two 1s in the middle of the OID.

Step 10 Perform one of the following procedures:

- a. If you are using Windows Certificate Authority 2003, check **Store certificate in the local computer certificate store** in Key Options.
- b. If you are using Windows Certificate Authority 2008, refer to the workaround described in the Troubleshooting Tips of this topic.

Step 11 Enter a friendly name.

Step 12 Select **Submit**.

Step 13 Select **Yes** in the Potential Scripting Violation dialog box.

Troubleshooting Tips

If you are using Windows Certificate Authority 2008, you no longer have the option to store the certificate in the local computer store on the certificate enrollment page. Perform the following workaround to replace Step 10 in the procedure:

- a. Sign out of the Microsoft OCS server.
- b. Sign in to the Microsoft OCS server as a Local user.
- c. Create the certificate.
- d. Approve the certificate from the CA server.
- e. Export the certificate to a file.
- f. Sign out of the Microsoft OCS server.
- g. Sign in to the Microsoft OCS server as a Domain user.
- h. Import the certificate file using the Certificate wizard. The certificate displays in the Microsoft OCS certificate tab (because it is installed in the Local Computer store).

Related Topics

- [Installing the CA Certification Chain, page 21](#)

What To Do Next

[Approving and Installing the Certificate, page 23](#)

Approving and Installing the Certificate

Before You Begin

Submit the Certificate Request on the CA Server.

Procedure

Step 1 Sign in to the enterprise subordinate CA server with Domain Administrator credentials.

Step 2 Select **Start > Run**.

Step 3 Perform the following actions:

- a. Enter **mmc**.
- b. Select **Enter**.

Step 4 Select **File > Add/Remove Snap-in**.

Step 5 Select **Add**.

Step 6 Select **Certification Authority** in Add Standalone Snap-in.

- Step 7** Select **Add**.
- Step 8** In Certification Authority, accept the default option **Local computer (the computer this console is running on)**.
- Step 9** Select **Finish**.
- Step 10** Select **Close**.
- Step 11** Select **OK**.
- Step 12** In the MMC, expand Certification Authority and expand your issuing certificate server.
- Step 13** Select **Pending request**.
- Step 14** In the Details pane, perform the following actions
- Right-click the request identified by its request ID.
 - Point to **All Tasks**.
 - Select **Issue**.
- Step 15** Select **Start > Run** on the server from which you requested the certificate.
- Step 16** Type `http://<name of your Issuing CA Server>/certsrv`.
- Step 17** Select **OK**.
- Step 18** Select **View the status of a pending certificate request** from **Select a task**.
- Step 19** Select your certificate request.
- Step 20** Select **Install this certificate**.
-

Related Topics

- [Submitting the Certificate Request on the CA Server, page 22](#)

What To Do Next

[Configuring the Installed Certificate, page 24](#)

Configuring the Installed Certificate

Before You Begin

Approve and install the Certificate.

Procedure

- Step 1** Select **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
- Step 2** Expand the (local computer) tree on the right pane.
- Step 3** Select **Default Web Site**.
- Step 4** Right-click to open the Properties dialog box.
- Step 5** Select the **Certificate** tab from the **Default Web Site Properties** dialog box.
- Step 6** If a certificate has already been selected, select **Delete Certificate** to remove the selection
- Step 7** Select **Certificate** to launch the Certificate Wizard.
- Step 8** Using the Certificate Wizard, select the certificate that was installed for Microsoft OCS.
- Step 9** Launch the **Microsoft Office Communications Server 2007** application.
- Step 10** In the right pane, select the server that represents the local machine.
- Step 11** Right-click on the server.
- Step 12** Select **Properties > Front End Properties**.
- Step 13** Select the **Certificate** tab.

Step 14 Select on **Select Certificate**.

Step 15 Find and select the installed certificate for Microsoft OCS.



Note If you are using Microsoft LCS, follow steps 1-7 above and then open the **Microsoft Live Communications Server 2005** application. From the Administration Page, right-click on the desired server to open the **Properties** dialog box. Select the **Security** tab, select **Select Certificate** and select the newly installed LCS certificate.

Related Topics

- [Approving and Installing the Certificate, page 23](#)

What To Do Next

[Configuring a TLS Route for Cisco Unified Presence on Microsoft OCS, page 25](#)

Configuring a TLS Route for Cisco Unified Presence on Microsoft OCS

Procedure

Step 1 Launch the **Microsoft Office Communications Server 2007** application.

Step 2 Right-click on Microsoft OCS Server pool in the right pane.

Step 3 Select **Properties > Front End Properties**.

Step 4 Select the **Routing** tab from the **Front End Server Properties** dialog box.

Step 5 Select **Add**.

Step 6 Perform the following actions to add a static route:

- Enter the hostname/FQDN for Cisco Unified Presence in the **Domain** field.



Note This should match with Subject CN of the Cisco Unified Presence certificate otherwise Microsoft OCS will not establish a TLS connection with Cisco Unified Presence.

- Select **TLS** from the **Transport** menu.
 - Enter **5062** in the **Port** field. The port number 5062 is the default Cisco Unified Presence port where it listens for peer authentication TLS connections.
 - Check **Replace host in request URI**.
 - Select **OK**.
-

Troubleshooting Tips

You can check Subject CN of a Cisco Unified Presence certificate by selecting **Cisco Unified Operating System Administration > Security > Certificate Management**, and selecting on a certificate entry in the certificate list.

What To Do Next

[Configuring Cisco Unified Presence as an Authenticated Host on Microsoft OCS, page 26](#)

Configuring Cisco Unified Presence as an Authenticated Host on Microsoft OCS

Procedure

- Step 1** Launch the Microsoft Office Communications Server 2007 application.
 - Step 2** Right-click on Microsoft OCS Server pool in the right pane.
 - Step 3** Select **Properties > Front End Properties**.
 - Step 4** Select the **Host Authorization** tab.
 - Step 5** Select **Add**.
 - Step 6** Select on **FQDN** and enter the CUP X.509 Subject Common Name as it appears in its certificate.
 - Step 7** Check **Throttle as server**.
 - Step 8** Check **Treat as Authenticated**.
 - Step 9** Select **OK**.
 - Step 10** Reboot the Microsoft OCS server.
When the server reboots, the Microsoft OCS server pool should display the outbound static route just configured.
-

What To Do Next

[Configuring Microsoft OCS to use TLSv1, page 26](#)

Configuring Microsoft OCS to use TLSv1

Cisco Unified Presence only supports TLSv1 so you must configure Microsoft OCS to use TLSv1. This procedure describes how to configure FIPS-compliant algorithms on Microsoft OCS to ensure that Microsoft OCS sends TLSv1 with TLS cipher TLS_RSA_WITH_3DES_EDE_CBC_SHA. In this procedure Microsoft OCS is configured on a domain controller.

Procedure

- Step 1** Select **Start > Administrative Tools > Local Security Policy**.
 - Step 2** Select **Security Settings** in the console tree.
 - Step 3** Select **Local Policies**.
 - Step 4** Select **Security Options**.
 - Step 5** Double-click the FIPS security setting in the Details pane.
 - Step 6** Modify the security setting.
 - Step 7** Select **OK**.
 - Step 8** Restart the Windows Server for the change to the FIPS security setting to take effect.
-

What To Do Next

[Creating a new TLS Peer Subject for Microsoft OCS on Cisco Unified Presence, page 27](#)

Creating a new TLS Peer Subject for Microsoft OCS on Cisco Unified Presence

Procedure

- Step 1** Select **Cisco Unified Presence Administration > Cisco Unified Presence > Security > TLS Peer Subjects**.
 - Step 2** Select **Add New**.
 - Step 3** Enter the subject CN of the certificate that Microsoft OCS presents in the Peer Subject Name field.
 - Step 4** Enter the name of the Microsoft OCS server in the Description field.
 - Step 5** Select **Save**.
-

What To Do Next

[Adding the TLS Peer to the Selected TLS Peer Subjects List on Cisco Unified Presence, page 27](#)

Adding the TLS Peer to the Selected TLS Peer Subjects List on Cisco Unified Presence

Before You Begin

Creating a new TLS Peer Subject for Microsoft OCS on Cisco Unified Presence.

Procedure

- Step 1** Select **Cisco Unified Presence Administration > System > Security > TLS Context Configuration**.
 - Step 2** Select **Find**.
 - Step 3** Select **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.
The TLS Context Configuration window displays.
 - Step 4** From the list of available TLS ciphers, select **TLS_RSA_WITH_3DES_EDE_CBC_SHA**.
 - Step 5** Select the right arrow to move this cipher to **Selected TLS Ciphers**.
 - Step 6** Check **Disable Empty TLS Fragments**.
 - Step 7** From the list of available TLS peer subjects, select the TLS peer subject that you configured.
 - Step 8** Select the right arrow to move it to **Selected TLS Peer Subjects**.
 - Step 9** Select **Save**.
-

Related Topics

[Creating a new TLS Peer Subject for Microsoft OCS on Cisco Unified Presence, page 27](#)

10 Setting Up Redundancy for this Integration

- [Load Balancing over TCP, page 27](#)

Load Balancing over TCP

This topic describes how to incorporate a load balancer in a Cisco Unified Presence dual-node configuration for use with incoming CSTA/TCP connections. We recommend the Cisco CSS 11501 Content Services Switch for the load balancer.

Table 2 gives an overview of the necessary tasks for configuring the Cisco CSS 11501 Content Services Switch for this integration. For detailed information on each task, refer to the Cisco CSS 11500 Content Services Switch documentation at the following URL:

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

Table 2 Cisco CSS 11501 Configuration Checklist for Load Balancing over TCP

Task	Additional Notes
Create a SIP service entry for each Cisco Unified Presence server.	<ul style="list-style-type: none"> The keepalive port should be the same port as the content, port 5060. The keepalive message type value should be 'tcp'.
Create a SIP rule that defines the content and the services that will manage this content	<p>The content is SIP on port 5060</p> <p>The SIP service entries (for each Cisco Unified Presence server) must be associated to the rule.</p>
Create a NAT (Network Address Translation) rule to show the Virtual IP Address of Load Balancer	The NAT rule shows the packets returning from the Cisco Unified Presence server to Microsoft OCS as coming from the Load Balancer (and not directly from the Cisco Unified Presence server).

On Microsoft OCS, you must configure the following parameters:

- The next hop address to be the Virtual IP address of Load Balancer for the SIP message routing.
- The default TCP listener on port 5060.

On Cisco Unified Presence, you must configure the Virtual IP address of the Load Balancer. This is configured in the Virtual IP address field in **Cisco Unified Presence Administration > System > Service Parameters > Cisco UP SIP Proxy > General Proxy Parameters (Clusterwide)**.

11 How to Deploy the Phone Selection Plug-in



Note The Phone Selection plug-in is only applicable if you are running Cisco Unified Presence release 7.0.3 or a later release.

The Phone Selection plug-in adds a Cisco Unified Presence tab to the Microsoft Office Communicator client interface that enables the user to select a phone device to control. Microsoft Office Communicator connects to the Cisco Unified Presence server, and the Phone Selection tab displays in a pane below the contacts list on Microsoft Office Communicator, as shown in Figure 2.

You must install the Phone Selection plug-in for the user if:

- on Cisco Unified Presence, the Microsoft Server Type value is “MOC Server OCS”, and
- the user has multiple devices (lines), and
- on Microsoft OCS, the LINE URI for the user does not uniquely identify a line appearance (for example, there is no device=, or partition=, or both, in the LINE URI)



Note You cannot use the Phone Selection plug-in if you are running the remote call control feature with Microsoft LCS 2005 because Microsoft LCS 2005 does not support customized tabs. If you are using Microsoft LCS 2005, the remote call control feature uses the device selection logic on Cisco Unified Presence to determine the device to control. In the Cisco Unified Presence Administration GUI, select **Application > Deskphone Control > Settings**, and select the Microsoft Server Type value **MOC Server LCS**.

- [Installing the Phone Selection Plug-in on a Client PC, page 29](#)
- [Uninstalling the Phone Selection Plug-in, page 31](#)
- [Providing Information about the Plug-in to your Users, page 32](#)

Installing the Phone Selection Plug-in on a Client PC

Before You Begin

For this procedure you will require the Phone Selection plug-in installer file **Cisco MOC RCC Plug-in.msi**, which you can download from Cisco Unified Presence Administration. Select **Application > Plugins** and download the **Cisco Unified Presence MOC Remote Call Control Plugin**.

Procedure

Step 1 Run the following command on the client PC, where CUPFQDN value specifies the FQDN of your Cisco Unified Presence server:

```
msiexec /I "<plug_in_filename>.msi" CUPFQDN=my-CUP.cisco.com /L*V install_log.txt
```



Note If you do not specify the FQDN of your Cisco Unified Presence server in this command the plug-in installation will be aborted.

Step 2 Follow the installation instructions to install to finish installing the Phone Selection plug-in.

Step 3 Launch Microsoft Office Communicator, and verify that the Cisco Unified Presence tab connects and displays on the interface.

Troubleshooting Remote Call Control

Microsoft Office Communicator Users Hear Two Beeps for Each DTMF Tone

When running Microsoft Office Communicator with Remote Call Control, users can select Cisco IP Communicator as their phone device.

In this scenario, when a user makes a call and enters DTMF tones (for example, when entering a voicemail password), the DTMF tones beep twice for each button press—once from Microsoft Office Communicator and once from Cisco IP Communicator. This is normal and expected behavior when DTMF is negotiated in-band; it does not happen if DTMF is negotiated outof-band..

User Unable to Switch Selected Device from Cisco Unified IP Phone to Cisco IP Communicator

This problem can occur if you have configured the device name for Cisco IP Communicator to be the same as the Cisco Unified Communications manager username. This is not a supported configuration, and you should change the device name for Cisco IP Communicator to a unique name.

Remote Call Control is Not Working

If Remote Call Control is not working for the Microsoft Office Communicator users, and the SIP Proxy service is not processing incoming messages from the Microsoft Office Communicator Server, check the following:

This can be caused by a high number of simultaneous sign in attempts on Microsoft Office Communicator after restarting the Microsoft OCS. When many of these attempts are made concurrently, the SIP Proxy service is flooded with INVITES and INFO messages.

1. Notify users about the service outage and recommend that they sign out of Microsoft Office Communicator during this time.
2. Stop the SIP Proxy service.
3. Restart the Microsoft OCS.
4. Restart the SIP Proxy service.
5. Notify users that they must sign in again to ensure that Remote Call Control is working properly.

Microsoft Office Communicator Client Cannot Connect to the Cisco Unified Presence Tab

If the Microsoft Office Communicator client cannot connect to the Cisco Unified Presence tab, check the following:

- You may have specified an invalid IP address or FQDN for your Cisco Unified Presence server. Repeat the plug-in installation procedure, specifying the correct Cisco Unified Presence server address in the command in Step 1.
- If you experience tab connection problems, note the following:
 - You may need to add the web address of the Cisco Unified Presence server to the list of trusted web addresses in the browser on the client PC. In Microsoft Internet Explorer, select **Internet Options > Security > Trusted Sites**, and add the web address **https://<Cisco Unified Presence_server_name>** to the list of trusted web addresses.
 - You may need to add the HTTPS web address of your domain to the security zone of the Cisco Unified Presence server. In Microsoft Internet Explorer, select **Internet Options > Security > Local intranet > Sites > Advanced**, and add the entry **https://*.your-domain** to the list of web addresses for the security zone.
- If an error message displays informing users that they do not have permission to use this feature, you need to enable users for Microsoft Office Communicator on Cisco Unified Presence.

Problems Installing the Plug-in on Microsoft Vista

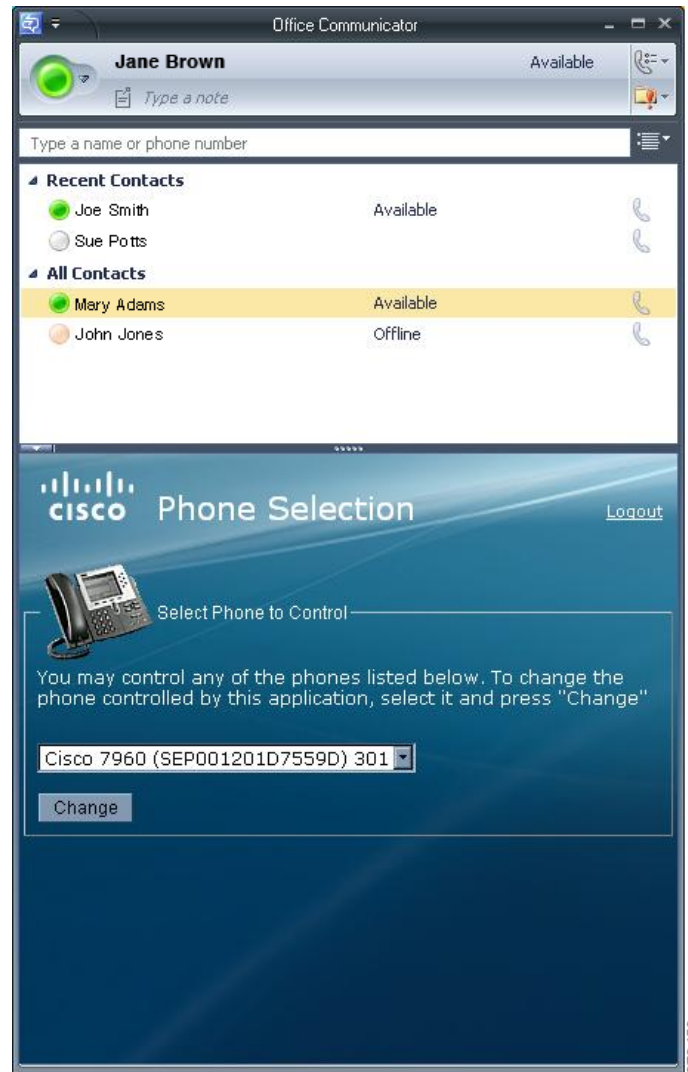
If you are running a Microsoft Vista platform and you experience problems installing the plug-in, you may need to turn off User Access Control (UAC) on the client PC. Follow this procedure to turn off UAC:

1. Sign in to the client PC with the credentials of a member of the local Administrators group.
2. Select **Start > Control Panel > User Accounts**.
3. Select **User Accounts** in the User Accounts pane.
4. Select **Turn User Account Control On or Off** in the User Accounts task pane.
5. If UAC is currently configured in Admin Approval Mode, the User Account Control message displays. Select **Continue**.
6. Uncheck **Use User Account Control (UAC) to help protect your computer**.
7. Select **OK**.
8. Select **Restart Now** to apply the change.

Related Topics

- [Uninstalling the Phone Selection Plug-in, page 31](#)
- [Providing Information about the Plug-in to your Users, page 32](#)

Figure 2 Microsoft Office Communicator client with Phone Selection tab



Uninstalling the Phone Selection Plug-in

To uninstall the Phone Selection plug-in, run the following command on the client PC:

```
msiexec /x "<plug_in_filename>" /L*V install_log.txt
```

Providing Information about the Plug-in to your Users

Provide..	Explanation
Sign in information	Provide your user base with their usernames and passwords for the Cisco Unified Presence interface.
Instructions for using the Phone Selection plug-in.	Provide your users with the <i>Quick Start Guide for the Phone Selection Plug-In for the Microsoft Office Communicator Call Control Feature for Cisco Unified Presence Release 7.03</i> .

12 Getting More Information

Cisco Unified Presence

For additional Cisco Unified Presence documentation, refer to the following URL:

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Cisco Unified Communications Manager

For Cisco Unified Communications Manager documentation, refer to the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Office Communications Server (OCS)

For details on installing, configuring and deploying Microsoft OCS, refer to the following URL:

<http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx>

Microsoft Live Communications Server (LCS)

For details on installing, configuring and deploying Microsoft LCS, refer to the following URL:

<http://office.microsoft.com/en-us/communicationsserver/FX011526591033.aspx>

Microsoft Active Directory

For information about Microsoft Windows Server Active Directory, refer to the following URL:

<http://technet.microsoft.com/windows/Server/en/technologies/festingsp068912ult.msp>

Americas Headquarters
Cisco Systems, Inc.
Windows Server Active Directory
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 800 020 0791
Fax: 31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)