Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)

First Published: July 18, 2012
Last Modified: April 17, 2014

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

Text Part Number: OL-30804-01
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://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. (1110R)

© 2012-2014 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

Configuration of IM and Presence Service with Microsoft OCS  1
Integration Requirements  1
Integration Overview  2
How this Integration Works  2
Line Appearances  4
License Requirements  4
Service Restart  4
More Information  4

CHAPTER 2

Configuration of Cisco Unified Communications Manager for Integration with Microsoft OCS  7
User and Device Configuration on Cisco Unified Communications Manager  7
Add Users to a Standard CCM Access Control Group  8
Configure an Application User for CTI Gateway  9
Add Application User to a CTI-Enabled Access Control Group  9
Assign CTI Device Control to the Application User  10

CHAPTER 3

Configuration of IM and Presence Service for Integration with Microsoft OCS  11
Configure Service Parameters  11
Configure an Incoming Access Control List  12
Configure Routing Settings  12
Remote Call Control Settings Configuration  13
Configure CTI Connections on IM and Presence Service  13
Assign User Capabilities  14
Run Microsoft RCC Troubleshooter  14

CHAPTER 4

Configuration of Microsoft Components for Integration with IM and Presence Service  17
Line URI Configuration on Microsoft Active Directory  17
User Authentication on IM and Presence Service  18
Install Phone Selection Plug-in on a Client PC  50
Uninstall Phone Selection Plug-in  50
Access Phone Selection through a Web Browser  50
Troubleshooting Remote Call Control  51
  User Unable to Switch Selected Device from Cisco Unified IP Phone to Cisco IP Communicator  51
Distribution of Plug-in Information  54
Configuration of IM and Presence Service with Microsoft OCS

Integration Requirements

This document describes the configuration steps for integrating the IM and Presence Service with Microsoft Office Communications Server or Microsoft Live Communications Server for Microsoft Office Communicator (MOC) call control.

Note

This document describes the procedure for integrating IM and Presence Service with Microsoft Office Communications Server (OCS).

Use this module as a guide for setting up this integration between IM and Presence Service and Microsoft Live Communications Server (LCS).

Software Requirements

- Latest release of IM and Presence Service Server
- Latest release of Cisco Unified Communications Manager Server
- Microsoft Office Communications (OCS) 2007 R2 Server, Standard or Enterprise
- Microsoft Live Communications (LCS) 2005 Server, Standard or Enterprise
- Microsoft Office Communicator (MOC)
- Microsoft Windows Server
Integration Overview

How this Integration Works

The IM and Presence Service 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 R2.

Microsoft Office Communicator sends session-initiating requests to the CTI Gateway on IM and Presence Service to control Cisco Unified IP Phones registered in Cisco Unified Communications Manager, as illustrated in the following figure. The CTI Gateway forwards the requests to the CTI Manager on CiscoUnified
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**

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

Microsoft Office Communicator sends session initiating requests to IM and Presence Service. These requests are routed in a round-robin sequence to the CTI connection addresses configured on IM and Presence Service. For example, the first request is routed to the 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 IM and Presence Service 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 IM and Presence Service publisher and subscriber nodes. There is a maximum of two nodes in an IM and Presence Service cluster when it is configured to support Microsoft Office Communicator Remote Control Client.

In a dual node IM and Presence Service 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 IM and Presence Service nodes.

When the CTI Gateway on IM and Presence Service 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, on page 4
- Redundancy Setup for this Integration

## Line Appearances

When a user selects a phone to use with the remote call control feature, on IM and Presence Service 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, on page 7

## License Requirements

You must assign IM and Presence Service to each Microsoft Lync Remote Call Control (RCC) user. IM and Presence Service capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). See the *Cisco Unified Communications Manager Enterprise License Manager User Guide* for more information.

You can assign IM and Presence Service to a user in the **End User Configuration** window in Cisco Unified Communications Manager. See the *Cisco Unified Communications Manager Administration Guide* for more information.

## Service Restart

After you configure the IM and Presence Service node to allow Remote Call Control through a Microsoft server, you will need to restart the Cisco UP SIP Proxy service on the node. For instructions to restart services for an IM and Presence Service node, see the *Cisco Unified Serviceability Administration Guide*.

## More Information

**IM and Presence Service**

For additional IM and Presence Service documentation, refer to the following URL:

Cisco Unified Communications Manager

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

Microsoft Active Directory

For information about Microsoft Windows Server Active Directory, refer to the following URL
Configuration of Cisco Unified Communications Manager for Integration with Microsoft OCS

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 7
- Add Users to a Standard CCM Access Control Group, page 8
- Configure an Application User for CTI Gateway, page 9
- Add Application User to a CTI-Enabled Access Control Group, page 9
- Assign CTI Device Control to the Application User, page 10

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Menu path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the phone devices, and associate a primary extension with each device</td>
<td>Cisco Unified Communications Manager Administration &gt; Device &gt; Phone</td>
</tr>
</tbody>
</table>
### Add Users to a Standard CCM Access Control Group

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

#### Procedure

1. **Step 1** Select **Cisco Unified Communications Manager Administration > User Management > User Settings > Access Control Group**.
2. **Step 2** Click **Find**.
3. **Step 3** Select **Standard CCM End Users**.
4. **Step 4** Select the end user to add to the Standard CCM access control group.
5. **Step 5** Click **Add Selected**.
6. **Step 6** Click **Save**.

#### What to Do Next
- **Configure an Application User for CTI Gateway**, on page 9

#### Related Topics
- **User and Device Configuration on Cisco Unified Communications Manager**, on page 7
Configure an Application User for CTI Gateway

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; Application User.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter an application user name in the User ID field, for example, CtiGW.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a password for this application user, and confirm the password.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

What to Do Next

Add Application User to a CTI-Enabled Access Control Group, on page 9

Add Application User to a CTI-Enabled Access Control Group

Complete the following procedure to add the application user to a CTI-enabled access control group.

Before You Begin

Configure an Application user for the CTI Gateway.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; User Settings &gt; Access Control Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Find.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Standard CTI Enabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add App Users to Group.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the Application user that you created for the CTI Gateway.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Add Selected.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

What to Do Next

Assign CTI Device Control to the Application User, on page 10

Related Topics

Configure an Application User for CTI Gateway, on page 9
Assign CTI Device Control to the Application User

Complete the following procedure to assign 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 Settings > Access Control Group.

**Step 2** Click Find.

**Step 3** Select Standard CTI Allow Control of All Devices. 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 4** Click Add App Users to Group.

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

**Step 6** Click Add Selected.

**Related Topics**
- Configure an Application User for CTI Gateway, on page 9
- Add Application User to a CTI-Enabled Access Control Group, on page 9
Configuration of IM and Presence Service for Integration with Microsoft OCS

Configure Service Parameters

The SIP message routing from IM and Presence Service to Microsoft Office Communicator is based on the Record-Route header added by Microsoft OCS in the initial request. IM and Presence Service 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 IM and Presence Service should be the same as the transport type configured on Microsoft OCS for the IM and Presence Service route (either TLS or TCP respectively).

Procedure

Step 1
Select Cisco Unified CM IM and Presence Administration > System > Service Parameters.

Step 2
Select the IM and Presence Service node.

Step 3
Select the service Cisco SIP Proxy.

Step 4
Verify that the following parameters are configured correctly:

a) 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 IM and Presence Service installation. Other SIP requests may be proxied.

b) Enable the **Add Record-Route Header** parameter.

c) Enable the **Use Transport in Record-Route Header** parameter.
d) 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 IM and Presence Service route.

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

**Step 6** Restart the Cisco UP SIP Proxy service on IM and Presence Service. For more information, see the *Cisco Unified Serviceability Administration Guide*.

### Configure an Incoming Access Control List

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Cisco Unified CM IM and Presence Administration &gt; System &gt; Security &gt; Incoming ACL</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter a description in the <strong>Description</strong> field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter IP address, host name, or Fully Qualified Domain Name (FQDN) of the associated Microsoft OCS server in the <strong>Address Pattern</strong> field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**What to Do Next**

Configure Routing Settings, on page 12

### Configure Routing Settings

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Cisco Unified CM IM and Presence Administration &gt; Presence &gt; Routing &gt; Settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>On</strong> for Method/Event Routing Status.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Default Cisco SIP Proxy TCP Listener</strong> for the Preferred Proxy Server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**What to Do Next**

Remote Call Control Settings Configuration, on page 13
Remote Call Control Settings Configuration

Configure CTI Connections on IM and Presence Service

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>Cisco Unified CM IM and Presence Administration</strong> &gt; <strong>Application</strong> &gt; <strong>Microsoft RCC &gt; Settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>On</strong> from the Application Status menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the CTI Gateway application username and password.</td>
</tr>
<tr>
<td>Tip</td>
<td>The username and password are case sensitive and must match what is configured on Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a value (in seconds) for the heartbeat interval. This is the length of time between heartbeat messages sent from IM and Presence Service to the Cisco Unified Communications Manager nodes to monitor the CTI connections.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter a value (in seconds) for the session timer. This is the session timer for the Microsoft Office Communicator sign-in session.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select the type of Microsoft server you are using from the Microsoft Server Type menu.</td>
</tr>
<tr>
<td>Step 7</td>
<td>As required, enter the IP address of each Cisco Unified Communications Manager node with which you want to establish a CTI connection.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

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 IM and Presence Service to determine the device to control.

What to Do Next
Assign User Capabilities, on page 14

Related Topics

- Configure an Application User for CTI Gateway, on page 9
- Deployment of Phone Selection Plug-in, on page 49
Assign User Capabilities

**Procedure**

**Step 1** Select Cisco Unified CM IM and Presence Administration > Application > Microsoft RCC > User Assignment.

**Step 2** Click Find.

**Step 3** Check the users to whom you want to assign the remote call control capabilities and click Assign Selected Users.

**Step 4** Check Enable Microsoft RCC in the Microsoft RCC Assignment window and click Save.

**Troubleshooting Tips**

- Make sure that you have assigned remote call 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**

**Configuration of Microsoft Components for Integration with IM and Presence Service, on page 17**

**Related Topics**

- Configure CTI Connections on IM and Presence Service, on page 13
- Run Microsoft RCC Troubleshooter, on page 14

**Run Microsoft RCC Troubleshooter**

The Microsoft RCC Troubleshooter validates the configuration that supports the integration of the Microsoft Office Communicator client with IM and Presence Service.

**Procedure**

**Step 1** Select Cisco Unified CM IM and Presence Administration > Diagnostics > Microsoft RCC 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  Click Submit.
Run Microsoft RCC Troubleshooter
Configuration of Microsoft Components for Integration with IM and Presence Service

- Line URI Configuration on Microsoft Active Directory, page 17
- User Authentication on IM and Presence Service, page 18
- Configure Microsoft Active Directory, page 19
- Microsoft OCS Configuration Overview, page 20

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 IM and Presence Service 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, on page 4
- User Authentication on IM and Presence Service, on page 18
- Deployment of Phone Selection Plug-in, on page 49

User Authentication on IM and Presence Service

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

1. IM and Presence Service checks if the Microsoft Office Communicator (sign in) user ID matches the Cisco Unified Communications Manager user ID. If IM and Presence Service cannot find a match:

2. IM and Presence Service checks if the Microsoft Office Communicator user email (the From header) matches the Cisco Unified Communications Manager user email. If IM and Presence Service cannot find a match:

3. IM and Presence Service 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, IM and Presence Service 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'.
Configure 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 IM and Presence Service.

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 IM and Presence Service node that you configured for this integration.

g) Enter the Line URI value.

Troubleshooting Tip
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.

What to Do Next
Microsoft OCS Configuration Overview, on page 20

Related Topics

- Line URI Configuration on Microsoft Active Directory, on page 17
- User Authentication on IM and Presence Service, on page 18
- Line Appearances, on page 4
Microsoft OCS Configuration Overview

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
OCS Front-End Properties - Host Authorization

Figure 2: OCS Front-End Properties - Host Authorization

Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth.

<table>
<thead>
<tr>
<th>Servers</th>
<th>Outbound Only</th>
<th>Throttle As 5ms</th>
<th>Treat As a</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.10.0.100</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Microsoft OCS Configuration Overview

OCS Front-End Properties - Routing

Figure 3: OCS Front-End Properties - Routing

![Routing Configuration](image)

Warning: The host address must also be added to the Host Authorization tab.

Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)
OCS Front-End Server Properties - General Tab

Figure 4: OCS Front-End Server Properties - General Tab

Related Topics

Configure Normalization Rules on Microsoft Active Directory, on page 25
Security Certificate Configuration for Microsoft OCS, on page 37
Configure a TLS Route for IM and Presence Service on Microsoft OCS, on page 42
Configure IM and Presence Service as an Authenticated Host on Microsoft OCS, on page 43
CHAPTER 5

Configuration of Normalization Rules on Microsoft Active Directory

• Configure Normalization Rules on Microsoft Active Directory, page 25
• Verify Username Displays on Microsoft Office Communicator Interface, page 26
• Sample Normalization Rules, page 27

Configure 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.
Verify Username Displays on 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\<username>\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.
Sample Normalization Rules

# ++ test RTP## PSTN:+61262637900, Extension:37XXX # +61262637ddd
[\s()\-./\+]*\d{3}[\s()\-./\+]*3\d{3};phone-context=dialstring # ++ test1 RTP ## Site:, PSTN:+61388043300,
Extension:33XXX
[\s()\-./\+]*\d{3}[\s()\-./\+]*3\d{3};phone-context=dialstring # ++ test2 RTP ## PSTN:+61292929000,
Extension:29XXX
[\s()\-./\+]*\d{3}[\s()\-./\+]*3\d{3};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

Configure Normalization Rules on Microsoft Active Directory, on page 25
Verify Username Displays on Microsoft Office Communicator Interface, on page 26
Sample Normalization Rules
Security Certificate Configuration for IM and Presence Service

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

This topic describes how to configure security certificates using a standalone CA. If you use an enterprise CA, refer to the Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager for an example of the certificate exchange procedure using an enterprise CA.

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

- Configure Standalone Root Certificate Authority (CA), page 30
- Download Root Certificate from CA Server, page 30
- Upload Root Certificate onto IM and Presence Service, page 31
- Generate a Certificate Signing Request for IM and Presence Service, page 32
- Download Certificate Signing Request from IM and Presence Service, page 32
- Submit Certificate Signing Request on CA Server, page 33
- Download Signed Certificate from CA Server, page 34
- Upload Signed Certificate to IM and Presence Service, page 34
Configure Standalone Root Certificate Authority (CA)

**Procedure**

**Step 1** Sign into 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** Click `Add/Remove Windows Components`.

**Step 6** Select `Application Server`.

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

**Step 8** Complete the installation procedure.

**Step 9** Click `Add/Remove Windows Components`.

**Step 10** Select `Certificate Services`.

**Step 11** Click `Next`.

**Step 12** Select `Standalone root CA`.

**Step 13** Click `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** Click `Next` to begin installation.

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

**Step 18** Click `Next`.

**Step 19** Click `Yes` when prompted to stop IIS.

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

**Step 21** Click `Finish`.

**What to Do Next**

Download Root Certificate from CA Server, on page 30.

Download Root Certificate from 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** Click on **Download a CA certificate, certificate chain, or CRL**.

**Step 4** Click **Base 64** for the Encoding Method.

**Step 5** Click **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.

---

**What to Do Next**

Upload Root Certificate onto IM and Presence Service, on page 31

**Related Topics**

Configure Standalone Root Certificate Authority (CA), on page 30

---

**Upload Root Certificate onto IM and Presence Service**

**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 IM and Presence Service node.

**Step 2** Select **Cisco Unified IM and Presence Operating System Administration** > **Security** > **Certificate Management**.

**Step 3** Click **Upload Certificate**.

**Step 4** Select **cup-trust** from the Certificate Name menu.

**Note** Leave the Root Name field blank.

**Step 5** Click **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** Click **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.
Generate a Certificate Signing Request for IM and Presence Service

Before You Begin
Upload the Root Certificate onto IM and Presence Service.

Procedure

Step 1 Select Cisco Unified IM and Presence Operating System Administration > Security > Certificate Management.
Step 2 Click Generate CSR.
Step 3 Select cup from the Certificate Name menu.
Step 4 Click Generate CSR.

What to Do Next
Download Certificate Signing Request from IM and Presence Service, on page 32

Related Topics
Upload Root Certificate onto IM and Presence Service, on page 31

Download Certificate Signing Request from IM and Presence Service

Before You Begin
Generate a Certificate Signing Request for IM and Presence Service.
Procedure

Step 1 Select Cisco Unified IM and Presence Operating System Administration > Security > Certificate Management.

Step 2 Click Download CSR.

Step 3 Select cup from the Certificate Name menu.

Step 4 Click Download CSR.

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

What to Do Next

Submit Certificate Signing Request on CA Server, on page 33

Related Topics

Generate a Certificate Signing Request for IM and Presence Service, on page 32

Submit Certificate Signing Request on CA Server

Before You Begin

Download the Certificate Signing Request from IM and Presence Service.

Procedure

Step 1 Copy the certificate request file cup.csr to your CA server.

Step 2 Open the URL http://local-server/certserv or http://127.0.0.1/certsrv.

Step 3 Click Request a certificate.

Step 4 Click 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 Click 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.

What to Do Next
Download Signed Certificate from CA Server, on page 34

Related Topics
Download Certificate Signing Request from IM and Presence Service, on page 32

Download Signed Certificate from 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  Click View the status of a pending certificate request.
Step 3  Select the option to view the request that was just submitted.
Step 4  Click Base 64 encoded.
Step 5  Click 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.

What to Do Next
Upload Signed Certificate to IM and Presence Service, on page 34

Related Topics
Submit Certificate Signing Request on CA Server, on page 33

Upload Signed Certificate to IM and Presence Service

Before You Begin
Download the Signed Certificate from the CA Server.
**Procedure**

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

**Step 2** Click 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** Click Browse.

**Step 6** Locate the signed cup.pem certificate on your local computer.

**Step 7** Click Upload File.

---

**What to Do Next**

Security Certificate Configuration for Microsoft OCS, on page 37

**Related Topics**

Download Signed Certificate from CA Server, on page 34
CHAPTER 7

Configuration of Security between IM and Presence Service and Microsoft OCS

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

- Security Certificate Configuration for Microsoft OCS, page 37
- Configure a TLS Route for IM and Presence Service on Microsoft OCS, page 42
- Configure IM and Presence Service as an Authenticated Host on Microsoft OCS, page 43
- Configure Microsoft OCS to Use TLSv1, page 44
- Create a New TLS Peer Subject for Microsoft OCS on IM and Presence Service, page 44
- Add TLS Peer to Selected TLS Peer Subjects List on IM and Presence Service, page 45

Security Certificate Configuration for Microsoft OCS

Download 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) Click OK.
Step 3 Click Download a CA certificate, certificate chain, or CRL from Select a task.
Step 4 Click Download CA certificate chain.
Step 5 Click 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
Install CA Certification Chain, on page 38

Install 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) Click OK.
Step 3 Select File > Add/Remove Snap-in.
Step 4 Click Add in the Add/Remove Snap-in dialog box.
Step 5 Select Certificates in the list of Available Standalone Snap-ins.
Step 6 Click Add.
Step 7 Click Computer account.
Step 8 Click Next.
Step 9 Perform the following actions from the Select Computer dialog box:
   a) Ensure Local computer: (the computer this console is running on) is selected.
   b) Click Finish.
   c) Click Close
   d) Click 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:
   a) Point to All Tasks.
b) Click **Import**.

**Step 14** Click **Next** in the Import Wizard.

**Step 15** Click **Browse** and locate the certificate chain on your computer.

**Step 16** Click **Open**.

**Step 17** Click **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** Click **Next**.

**Step 21** Click **Finish**.

---

**What to Do Next**

Submit Certificate Request on CA Server, on page 39

**Related Topics**

Download CA Certification Chain, on page 37

---

**Submit Certificate Request on 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** Click **Enter**.

**Step 4** Click **Request a Certificate**.

**Step 5** Click **Advanced certificate request**.

**Step 6** Click **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** Click **Submit**.

**Step 13** Click **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).

---

**What to Do Next**

**Approve and Install Certificate**, on page 40

**Related Topics**

Install CA Certification Chain, on page 38

---

**Approve and Install 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) Click Enter.

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

**Step 5** Click Add.

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

**Step 7** Click Add.

**Step 8** In Certification Authority, accept the default option Local computer (the computer this console is running on).

**Step 9** Click Finish.

**Step 10** Click Close.

**Step 11** Click 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

a) Right-click the request identified by its request ID.

b) Point to All Tasks.

c) 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** Click OK.

**Step 18** Select View the status of a pending certificate request from Select a task.

**Step 19** Select your certificate request.

**Step 20** Click Install this certificate.

---

**What to Do Next**

Configure Installed Certificate, on page 41

**Related Topics**

Submit Certificate Request on CA Server, on page 39

---

**Configure Installed Certificate**

**Before You Begin**

Approve and install the Certificate.
Configure a TLS Route for IM and Presence Service on Microsoft OCS

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  Click 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 Click 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.

What to Do Next

Configure a TLS Route for IM and Presence Service on Microsoft OCS, on page 42

Related Topics

Approve and Install Certificate, on page 40

Configure a TLS Route for IM and Presence Service 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  Click Add.
Step 6  Perform the following actions to add a static route:
a) Enter the hostname/FQDN for IM and Presence Service in the **Domain** field.
   **Note** This should match with Subject CN of the IM and Presence Service certificate otherwise Microsoft OCS will not establish a TLS connection with IM and Presence Service.
b) Select **TLS** from the Transport menu.
c) Enter **5062** in the **Port** field. The port number 5062 is the default IM and Presence Service port where it listens for peer authentication TLS connections.
d) Check **Replace host in request URI**.
e) Click **OK**.

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

---

**What to Do Next**

Configure IM and Presence Service as an Authenticated Host on Microsoft OCS, on page 43

---

## Configure IM and Presence Service 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** Click **Add**.
**Step 6** Select 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** Click **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**

Configure Microsoft OCS to Use TLSv1, on page 44
Configure Microsoft OCS to Use TLSv1

IM and Presence Service 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.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Start &gt; Administrative Tools &gt; Local Security Policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Security Settings in the console tree.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Local Policies.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Security Options.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Double-click the FIPS security setting in the Details pane.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Modify the security setting.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click OK.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart the Windows Server for the change to the FIPS security setting to take effect.</td>
</tr>
</tbody>
</table>

What to Do Next

Create a New TLS Peer Subject for Microsoft OCS on IM and Presence Service, on page 44

Create a New TLS Peer Subject for Microsoft OCS on IM and Presence Service

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Cisco Unified CM IM and Presence Administration &gt; System &gt; Security &gt; TLS Peer Subjects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the subject CN of the certificate that Microsoft OCS presents in the Peer Subject Name field.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the name of the Microsoft OCS server in the Description field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

What to Do Next

Add TLS Peer to Selected TLS Peer Subjects List on IM and Presence Service, on page 45
Add TLS Peer to Selected TLS Peer Subjects List on IM and Presence Service

Before You Begin
Creating a new TLS Peer Subject for Microsoft OCS on IM and Presence Service.

Procedure

**Step 1** Select Cisco Unified CM IM and Presence Administration > System > Security > TLS Context Configuration.

**Step 2** Click 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** Click 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** Click the right arrow to move it to Selected TLS Peer Subjects.

**Step 9** Click Save.

Related Topics
Create a New TLS Peer Subject for Microsoft OCS on IM and Presence Service, on page 44
Add TLS Peer to Selected TLS Peer Subjects List on IM and Presence Service
Load Balancing over TCP

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

The following table 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Additional Notes</th>
</tr>
</thead>
</table>
| Create a SIP service entry for each IM and Presence Service node. | • 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 | The content is SIP on port 5060  
The SIP service entries (for each IM and Presence Service node) must be associated to the rule. |
| 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 IM and Presence Service node to Microsoft OCS as coming from the Load Balancer (and not directly from the IM and Presence Service node). |

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 IM and Presence Service, you must configure the Virtual IP address of the Load Balancer. This is configured in the Virtual IP address field in Cisco Unified CM IM and Presence Administration > System > Service Parameters > Cisco SIP Proxy > General Proxy Parameters (Clusterwide).
Microsoft OCS Remote Call Control Installation

- Deployment of Phone Selection Plug-in, page 49
- Install Phone Selection Plug-in on a Client PC, page 50
- Uninstall Phone Selection Plug-in, page 50
- Access Phone Selection through a Web Browser, page 50
- Troubleshooting Remote Call Control, page 51
- Distribution of Plug-in Information, page 54

Deployment of Phone Selection Plug-in

The Phone Selection plug-in adds a Device Selection 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 IM and Presence Service node, and the Phone Selection tab displays in a pane below the contacts list on Microsoft Office Communicator, as shown in User Unable to Switch Selected Device from Cisco Unified IP Phone to Cisco IP Communicator, on page 51.

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

- on IM and Presence Service, 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 IM and Presence Service to determine the device to control. In the Cisco Unified CM IM and Presence Administration GUI, select Application > Microsoft RCC > Settings, and select the Microsoft Server Type value MOC Server LCS.
Install Phone Selection Plug-in on a Client PC

Before You Begin

For this procedure you will require:

- Your username and password for Cisco Unified Communications Manager IM and Presence Service User Options.
- The Phone Selection plug-in installer file Cisco MOC RCC Plug-in.msi, which you can download from Cisco Unified CM IM and Presence Administration. To download the plug-in select Application > Plugins and click the link Cisco Unified CM IM and Presence MOC Remote Call Control Plugin.
- The administrator must assign the user to the "Standard CCM End User" Group. Confirm that you have been added to this group.

Procedure

Step 1 Run the following command on the client PC, where the CUPFQDN value specifies the FQDN of your IM and Presence Service node:

```
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 IM and Presence Service node in this command the plug-in installation will be aborted.

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

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

Uninstall 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
```

Access Phone Selection through a Web Browser

You use the Cisco Unified Communications Manager IM and Presence Service User Options Web interface (Web interface) to customize settings, create personal response messages, and organize contacts.

Before You Begin

Confirm the following information from your system administrator:

- The hostname, FQDN, or IP address for the Web interface.
- Your username and password for the Web interface.
To be able to log in to the Web interface, the administrator must assign the user to the "Standard CCM End User" Group. Confirm that you have been added to this group.

**Procedure**

**Step 1**
Open a supported Web browser on your computer.

**Step 2**
Enter the URL for the Web interface:
Where *imp_ip* is the hostname, FQDN, or IP address of the IM and Presence Service node.

**Step 3**
Enter your username for the Web interface.

**Step 4**
Enter your password for the Web interface that was provided by your system administrator.

**Step 5**
Click **Login**.
To log out of the Web interface, click **Logout** in the upper right corner of the **User Options** page. For security purposes, you will be automatically logged out of the Web interface after thirty minutes of inactivity.

**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 out-of-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 Following OCS Restart**

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 IM and Presence Service Tab**

If the Microsoft Office Communicator client cannot connect to the IM and Presence Service tab, check the following:

- You may have specified an invalid IP address or FQDN for your IM and Presence Service node. Repeat the plug-in installation procedure, specifying the correct IM and Presence Service node 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 IM and Presence Service node 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://<IM and Presence Service_node_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 IM and Presence Service node. 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 IM and Presence Service.

**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.

![Figure 5: Microsoft Office Communicator client with Phone Selection tab](image)

**Related Topics**
- Uninstall Phone Selection Plug-in, on page 50
- Distribution of Plug-in Information, on page 54
## Distribution of Plug-in Information

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