Remote Call Control with Microsoft Lync Server 2010 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-30801-01
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 ACCOMPANYING 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

**Introduction** 1  
About Microsoft Lync Server 1  
Get More Information 1  
About Remote Call Control 2  
Integration Overview 2  
Line Appearances 4

## CHAPTER 2

**Integration Requirements** 5  
Software Requirements 5  
Preconfiguration Checklist 6  
Integration License Requirements 6

## CHAPTER 3

**Cisco Unified Communications Manager Server Setup** 9  
Cisco Unified Communications Manager User and Device Setup 9  
Add Users to a Standard CCM Access Control Group 10  
Set Up CTI Gateway Application User 10  
Add Application User to CTI-Enabled Access Control Group 11  
Assign CTI Device Control to Application User 12  
Set Up Dial Rules 12

## CHAPTER 4

**IM and Presence Service Node Setup** 15  
Set Up Service Parameters 15  
Set Up Incoming and Outgoing Access Control Lists 16  
Set Up Routing Settings 16  
Remote Call Control Setup 17  
Set Up IM and Presence Service CTI Connection 17  
Assign User Capabilities 18  
Run Microsoft RCC Troubleshooter 18
## CHAPTER 5

**Microsoft Component Integration Setup for IM and Presence Service**

- Line URI Setup on Microsoft Active Directory 21
- IM and Presence Service User Authentication 22
- Set Up Microsoft Active Directory 23
- Enable Users in Lync Server Control Panel 23
- Microsoft Lync Server Setup Overview 24
  - Set Up Static Route for Microsoft Lync Server 25
  - Set Up Application Pool for Microsoft Lync Server 26
  - Set Up RCC Application for Microsoft Lync Server 28
  - Set Up Lync Server SIP Listen Port 29
  - Commit Lync Server Setup 29

## CHAPTER 6

**Normalization Rules Setup**

- Set Up Normalization Rules on Microsoft Active Directory 31
  - Sample Normalization Rules 32
- Update Microsoft Lync Address Book 33

## CHAPTER 7

**Security Certificate Setup for IM and Presence Service**

- Set Up Standalone Root Certificate Authority (CA) 35
- Download Root Certificate from CA Server 36
- Upload Root Certificate to IM and Presence Service 37
- Generate Certificate Signing Request for IM and Presence Service 38
- Download CSR from IM and Presence Service 38
- Submit Certificate Signing Request on CA Server 39
- Download Signed Certificate from CA Server 39
- Upload Signed Certificate to IM and Presence Service 40

## CHAPTER 8

**Security between IM and Presence Service and Microsoft Lync Setup**

- Security Certificate for Microsoft Lync Setup 43
  - Download CA Certification Chain 43
  - Install CA Certification Chain 44
  - Submit Certificate Request on CA Server 45
  - Approve and Import Certificate 45
  - Assign Imported Certificate 46
Verify Certificate Setup for Server and Client Authentication 47
TLS Route for Microsoft Lync Setup 48
    Set Up Static Route 48
    Set Up Application Pool 49
    Set Up RCC Application 50
    Commit Lync Server Setup 51
Set Up Microsoft Lync for TLSv1 52
Create New TLS Peer Subject for Microsoft Lync 52
Add TLS Peer to TLS Peer Subjects List 53

CHAPTER 9  Lyne Remote Call Control Installation 55
    Install IM and Presence Service Lync Remote Call Control Plugin on Client Computer 55
    Uninstall IM and Presence Service Lync Remote Call Control Plugin 56
    Access Phone Selection Through a Web Browser 57

CHAPTER 10  Microsoft Lync Server and Microsoft Lync Client Logging 59
    Initiate Trace and View Microsoft Lync Server Log 59
    Enable and View Microsoft Lync Client Logs 60

CHAPTER 11  Load Balancer Configuration for Lync RCC Integration 61
    About the Load Balancer 61
    IM and Presence Service node updates 61
    Cisco Adaptive Security Appliance Updates 62
        Static PAT Message Updates 63
        Access List Updates 64
        TLS Proxy Instance Updates 66
    CA-Signed Security Certificate Update 66
        Security Certificate Configuration Between the Load Balancer and Cisco Adaptive Security Appliance 66
        Security Certificate Configuration Between the Load Balancer and IM and Presence Service Node 67
    Microsoft Component Updates 67

CHAPTER 12  Troubleshooting 69
IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser.  69
Lync Error When Using E.164 Numbers  70
Synchronize User to Cisco Unified Communications Manager  70
Enable IM and Presence for User ID  71
Verify User Phone Call Control at the Lync Client Is Enabled  71
Phone Icon with a Red X in the Status Bar in Microsoft Lync Client  72
CHAPTER 1

Introduction

This chapter describes the configuration steps to integrate the IM and Presence Service with Microsoft Lync Server for Remote Call Control.

- About Microsoft Lync Server , page 1
- About Remote Call Control, page 2
- Integration Overview, page 2
- Line Appearances, page 4

About Microsoft Lync Server

Microsoft Lync Server is designed for use in small and medium organization deployments. The server acts as both a SIP registrar and SIP proxy in a single system. The server functionality provides voice capabilities for Remote Call Control to gateways such as the IM and Presence Service and Cisco Unified Communications Manager platforms.

Microsoft Lync Server 2010 Standard Edition installs the Microsoft SQL Server 2008 Express database on the same server to provide data storage for users and configuration system data. Microsoft Lync Server 2010 Enterprise Edition installs the Microsoft SQL Server 2008 Express database on a different server. Commands that are entered from the Lync Server Management Shell are loaded into the SQL database.

Get More Information

IM and Presence Service

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

Cisco Unified Communications Manager

For Cisco Unified Communications Manager documentation, see the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Microsoft Lync

For Microsoft Lync documentation, see the following URLs:


Microsoft Active Directory


About Remote Call Control

Microsoft Remote Call Control (RCC) allows enterprise users to control their Cisco Unified IP Phone or Cisco IP Communicator Phone through Microsoft Lync, a third-party desktop instant-messaging (IM) application. When a user signs in to the Microsoft Lync client, the Lync server sends instructions, through the IM and Presence Service node, to the Cisco Unified Communications Manager to set up, tear down and maintain calling features based on a user's action at the Lync client.

**Note**

SIP federation and Remote Call Control (RCC) do not work together on the same IM and Presence Service cluster. This is because for SIP federation a user cannot be licensed for both Cisco IM and Presence Service and Microsoft Lync/OCS, but for RCC a user must be licensed for Cisco IM and Presence Service and Microsoft Lync/OCS at the same time.

Integration Overview

IM and Presence Service allows enterprise users to control their Cisco Unified IP Phone or Cisco IP Communicator Phone through Microsoft Lync, a third-party desktop IM application.

Microsoft Lync sends session-initiating requests to the Computer Telephony Interface (CTI) Gateway on IM and Presence Service to control Cisco Unified IP Phones or Cisco IP Communicator Phones that are registered in Cisco Unified Communications Manager, as illustrated in the following figure. 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 Lync application using the same path in the opposite direction.

Figure 1: Integration Overview

Microsoft Lync sends requests to IM and Presence Service

Microsoft Lync sends session-initiating requests to IM and Presence Service. These requests are routed to the CTI connection addresses that are configured on IM and Presence Service.

Note

IM and Presence Service supports CTI connections with up to eight Cisco Unified Communications Manager nodes.

The requests are distributed to the CTI connection addresses in a round-robin sequence, for example the first request is routed to first CTI node, second request to next CTI node, and so on. In a dual-node IM and Presence Service cluster, a load balancer can be used to distribute (in a round-robin manner) the session-initiating requests that are sent from Microsoft Lync clients to the publisher and subscriber IM and Presence Service nodes.

CTI Gateway Monitors CTI Connection Addresses for Microsoft Lync User Sign-In

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 Lync user signs in, Microsoft Lync server sends a SIP INVITE request with a CSTA body to the CTI Gateway to monitor the Cisco Unified IP Phone or Cisco IP Communicator Phone for the user. The CTI Gateway creates a session for that Microsoft Lync user, and uses the load-balancing mechanism to send session-initiating requests from that user to any of the CTI connection addresses.

CSTA Application Session Is Established

After the CSTA application session is established, Microsoft Lync 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 Lync 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 reestablish 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 Lync sends an (in-session) SIP INFO request, the CTI Gateway will have a different CTI Manager connection ID because of a new connection. Microsoft Lync sends a new SIP INVITE message, but the Microsoft Lync user is not required to sign in again.

**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 the Microsoft Lync client. 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.

See the *Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager* for information on the configuration steps to integrate IM and Presence Service with Microsoft OCS for Microsoft Office Communicator Call Control.
Integration Requirements

Call forward setting on IP phone: Call forward settings made on the Cisco IP phone, using the soft key button or the Cisco UCM phone configuration page are not reflected in the Microsoft Lync Client, however call forward settings made on Microsoft Lync are reflected on the Cisco IP phone.

The Microsoft Lync Client can override any call forward setting configured on the IP Phone. The IP Phone can override any call forward setting configured on the Microsoft Lync Client.

- Software Requirements, page 5
- Preconfiguration Checklist, page 6
- Integration License Requirements, page 6

Software Requirements

The following software is required for integrating IM and Presence Service with Microsoft Lync Server:

- IM and Presence Service, current release
- IM and Presence Service Lync Remote Call Control Plug-in
- Cisco Unified Communications Manager, current release
  - Lync Server Control Panel
  - Lync Server Deployment Wizard
  - Lync Server Logging Tool
  - Lync Server Management Shell
  - Lync Server Topology Builder
- Microsoft 2010 Lync Client
- (Optional) Cisco CSS 11500 Content Services Switch
Preconfiguration Checklist

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

• Microsoft Domain Controller
• Microsoft Active Directory
• DNS
• Certificate Authority

Before beginning the configuration tasks, we recommend that you complete the following preconfiguration checklist:

1. Verify that all services are running on Microsoft Lync Server.
2. Verify that you updated all SRV records in DNS in support of Microsoft Lync Server as instructed in the Microsoft Lync Server installation instructions.
3. Verify that the computer on which the Microsoft Lync client is installed can resolve the FQDN of the Microsoft Lync server. You can do this by executing the NSLOOKUP command from the Microsoft Lync client computer.
4. Verify that the IM and Presence Service node, Cisco Unified Communications Manager node and Microsoft Lync server are added to DNS and that each of these servers is resolving to its FQDN. You can do this by executing the NSLOOKUP command from another resource in each of their domains.
5. If you are using LDAP synchronization between AD and Cisco Unified Communications Manager server, verify that connections are synchronizing properly.

Integration 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.
What To Do Next

Cisco Unified Communications Manager Server Setup, on page 9
Note that because menu options and parameters may vary for different Cisco Unified Communications Manager releases, see the Cisco Unified Communications Manager documentation appropriate to your release.

- Cisco Unified Communications Manager User and Device Setup, page 9
- Add Users to a Standard CCM Access Control Group, page 10
- Set Up CTI Gateway Application User, page 10
- Add Application User to CTI-Enabled Access Control Group, page 11
- Assign CTI Device Control to Application User, page 12
- Set Up Dial Rules, page 12

Cisco Unified Communications Manager User and Device Setup

Before you configure Cisco Unified Communications Manager for integration with Microsoft Lync, 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; PhonePhone</td>
</tr>
<tr>
<td>Configure the users, and associate a device with each user</td>
<td>Cisco Unified Communications Manager Administration &gt; User Management &gt; End User</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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; User Settings &gt; Access Control Group.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Find.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Standard CCM End Users.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Add End Users to Group.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the end user to add to the Standard CCM access control group.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select Add Selected.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

What to Do Next
Set Up CTI Gateway Application User, on page 10

Related Topics
Cisco Unified Communications Manager User and Device Setup, on page 9

Set Up CTI Gateway Application User

Complete the following procedure to configure an application user for the CTI Gateway.
## Add Application User to 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</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; Application User.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Add New.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter an application user name in the User ID field. <strong>Example:</strong> 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>Select Save.</td>
</tr>
</tbody>
</table>

### What to Do Next
Add Application User to CTI-Enabled Access Control Group, on page 11

## Assign CTI Device Control to 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; User Settings &gt; Access Control Group.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Find.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Standard CTI Enabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select 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>Select Add Selected.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

### What to Do Next
Assign CTI Device Control to Application User, on page 12

## Related Topics
- Set Up CTI Gateway Application User, on page 10
Assign CTI Device Control to Application User

Complete the following procedure to assign CTI device control to the application user.

⚠️ Caution
Do not add devices as controlled devices to the application user because the role "Standard CTI Allow Control of All Devices" gives the application user sufficient privileges to control any Cisco Unified Communications Manager device. Adding devices as controlled devices to the application user can negatively impact Cisco Unified Communications Manager performance because Cisco Unified Communications Manager does not support a single user controlling a large number of devices in this manner.

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 Select 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 Select Add App Users to Group.
Step 5 Select the application user that you created for the CTI Gateway.
Step 6 Select Add Selected.

Related Topics

Set Up CTI Gateway Application User, on page 10
Add Application User to CTI-Enabled Access Control Group, on page 11

Set Up Dial Rules

A dial rule must be set up to strip the + prefix coming from the Lync server. If this is not done, the Cisco Unified Communications Manager will not find the Line URI and the result is a failed call attempt.

⚠️ Note
You perform the following configuration only if users are provisioned with E.164 numbers. If both users and IP phones are provisioned with E.164 numbers, then there is no need to set up an application dial rule to strip the + prefix.
Procedure

**Step 1** Select Cisco Unified Communications Manager Administration > Call Routing > Dial Rules > Application Dial Rules > Add New.

**Step 2** Enter a name and a description for the dial rule.

**Step 3** In the Number Begins With field, enter +.

**Step 4** In the Number of Digits field, enter 12 to support the following number format: xxx-xxx-xxxx.

**Step 5** In the Total Digits to be Removed field, enter 1. This will ensure that the + prefix will be stripped because digits are always stripped from left to right.

**Step 6** Select Save.

What to Do Next

IM and Presence Service Node Setup, on page 15
Set Up Dial Rules
IM and Presence Service Node Setup

- Set Up Service Parameters, page 15
- Set Up Incoming and Outgoing Access Control Lists, page 16
- Set Up Routing Settings, page 16
- Remote Call Control Setup, page 17

Set Up Service Parameters

The SIP message routing from IM and Presence Service to Microsoft Lync is based on the Record-Route header added by Microsoft Lync 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 Lync client.

In addition the transport type on IM and Presence Service should be the same as the transport type configured on Microsoft Lync for the IM and Presence Service route.

**Procedure**

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

**Step 2** Select the IM and Presence server.

**Step 3** Select the service **Cisco SIP Proxy**.

**Step 4** Verify that the following parameters are configured correctly:

a) The proxy domain must define the enterprise top-level domain (for example, "example.com"). This value can be entered in the **CUCM Domain** service parameter field. 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 Lync for the Microsoft Lync to IM and Presence Service route.

**Step 5** Select **Save**.
Set Up Incoming and Outgoing Access Control Lists

This procedure involves adding four access control list (ACL) entries:

- The FQDN of the Lync server for the incoming ACL
- The IP address of the Lync server for the incoming ACL
- The FQDN of the Lync server for the outgoing ACL
- The IP address of the Lync server for the outgoing ACL

Procedure

**Step 1** Select Cisco Unified CM IM and Presence Administration > System > Security > Incoming ACL > Add New.

**Step 2** Enter a description of the incoming ACL, for example, Lync Standard Server.

**Step 3** Enter the FQDN of the Lync server in the Address Pattern field and select Save.

**Tip** To view the new Incoming ACL entry, select Go from the top right of the window. A list of all configured Incoming ACLs is displayed.

**Step 4** Select Add New.

**Step 5** Enter a description of the incoming ACL, for example, Lync Standard Server.

**Step 6** Enter the IP address of the Lync server in the Address Pattern field and select Save.

**Step 7** Select Cisco Unified CM IM and Presence Administration > System > Security > Outgoing ACL > Add New.

**Step 8** Enter a description of the outgoing ACL, for example, Lync Standard Server.

**Step 9** Enter the FQDN of the Lync server in the Address Pattern field and select Save.

**Tip** To view the new Outgoing ACL entry, select Go from the top right of the window. A list of all configured Outgoing ACLs is displayed.

**Step 10** Select Add New.

**Step 11** Enter a description of the outgoing ACL, for example, Lync Standard Server.

**Step 12** Enter the IP address of the Lync server in the Address Pattern field and select Save.

What to Do Next

Set Up Routing Settings, on page 16

Set Up Routing Settings

Complete the following procedure to configure the routing settings.
Remote Call Control Setup

Set Up IM and Presence Service CTI Connection

Complete the following procedure to configure the 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

Step 1 Select Cisco Unified CM IM and Presence Administration > Application > Microsoft RCC > 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 IM and Presence Service 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 Lync sign-in session.
Step 6 Select the type of Microsoft server you are using from the Microsoft Server Type menu.  
Note For Microsoft Lync integration, you must select MOC server OCS.
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.
If you select MOC server OCS as the Microsoft Server Type, you must install the IM and Presence Service Lync Remote Call Control Plug-in on the Microsoft Lync client for any users who use more than one line appearance for remote call control. The IM and Presence Service Lync Remote Call Control Plug-in adds a menu item to the Microsoft Lync client that enables the user to select a line appearance to control.

**Important**

**What to Do Next**

Assign User Capabilities, on page 18

**Related Topics**

- Set Up CTI Gateway Application User, on page 10
- Lync Remote Call Control Installation, on page 55
- Run Microsoft RCC Troubleshooter, on page 18

**Assign User Capabilities**

Complete the following procedure to assign Microsoft Remote Call Control (RCC) capabilities to users.

**Procedure**

1. **Step 1** Select Cisco Unified CM IM and Presence Administration > Application > Microsoft RCC > User Assignment.
2. **Step 2** Select Find.
3. **Step 3** Check the users to whom you want to assign remote call control capabilities.
4. **Step 4** Select Assign Selected Users.
5. **Step 5** Check Enable Microsoft RCC in the Microsoft RCC Assignment window.
6. **Step 6** Select Save.

**Important** Make sure that you have assigned remote call control capabilities to each Microsoft Lync user.

**What to Do Next**

Run Microsoft RCC Troubleshooter, on page 18

**Related Topics**

- Set Up IM and Presence Service CTI Connection, on page 17
- Run Microsoft RCC Troubleshooter, on page 18

**Run Microsoft RCC Troubleshooter**

The Microsoft RCC Troubleshooter validates the configuration that supports the integration of the Microsoft Lync 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 Lync server address.

Step 4: Select Submit.

What to Do Next

Microsoft Component Integration Setup for IM and Presence Service, on page 21
Run Microsoft RCC Troubleshooter
Microsoft Component Integration Setup for IM and Presence Service

- Line URI Setup on Microsoft Active Directory, page 21
- IM and Presence Service User Authentication, page 22
- Set Up Microsoft Active Directory, page 23
- Enable Users in Lync Server Control Panel, page 23
- Microsoft Lync Server Setup Overview, page 24

Line URI Setup 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 where:
  - xxxx specifies the directory number that the CTI Manager reports to IM and Presence Service as the calling or called number when a call is placed.
  - phone-context=dialstring enables the Microsoft Lync client to control one of the devices that are associated with the directory number.

Note

If you are using E.164 numbers, do not include phone-context=dialstring because it will result in an error at the Microsoft Lync client. See Lync Error When Using E.164 Numbers, on page 70.

- If you configure the device ID, the Microsoft Lync 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 Lync 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 Lync user signs in.
• After initial sign in, the Microsoft Lync user can change the line appearance that they wish to control using the Cisco Unified Communications Manager IM and Presence Service Lync Remote Call Control Plugin.

• 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.

You can also use the E.164 format for the Line URI. However, you must ensure that the DNs are also configured with E.164 on Cisco Unified Communications Manager.

Related Topics
- Line Appearances, on page 4
- IM and Presence Service User Authentication, on page 22
- Lync Remote Call Control Installation, on page 55

**IM and Presence Service User Authentication**

When configuring the SIP URI on Microsoft Active Directory, consider how 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 Lync (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 Lync 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 Lync user email matches the ocsPrimaryAddress value of a Cisco Unified Communications Manager user.

For example, a user Joe has the Microsoft Lync 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'.
Set Up 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 username 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 Microsoft Lync Server.
b) Enter the SIP URI.
c) Enter the Microsoft Lync server name or pool.
   Caution Ensure the Microsoft Lync 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.

Important 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 Lync.

What to Do Next
Enable Users in Lync Server Control Panel, on page 23

Enable Users in Lync Server Control Panel

The following procedure describes how to enable new users in the Lync Server Control Panel.
Procedure

Step 1  Go to the Windows server that has Microsoft Lync Server installed.
Step 2  Select Start > All Programs > Microsoft Lync Server > Lync Server Control Panel.
Step 3  Choose Enable users for Lync Server from the Top Actions menu.
Step 4  Select Add.
Step 5  Select the LDAP search option and select Find.
Step 6  Click on the user to enable and select OK.
Step 7  Choose the application pool from the Assign users to a pool drop-down list.
Step 8  Select the Specify a SIP URI option and enter the SIP URI, for example, sip:UserA@lyncdomain.com, where UserA is the user you added and lyncdomain.com specifies the domain name of the Lync server.
Step 9  Choose Remote call control from the Telephony drop-down list.
Step 10 Enter the Line URI in the format tel:<telephone_number>, where <telephone_number> is the telephone number you entered when adding the user.
Step 11 Enter the Line Server URI, for example, sip:UserA@my-cups.my-domain.com, where UserA is the user you added and my-cups.my-domain.com specifies the domain name of the IM and Presence Service node.
   Please note the following:
   a) The Line Server URI domain is the value that is matched by the static route MatchUri parameter. See Set Up Static Route for Microsoft Lync Server, on page 25.
   b) The Line Server URI domain and the value in the MatchUri parameter must match to enable the Lync server to correctly route SIP messages to the IM and Presence Service node.
   c) The IM and Presence Service node must also have this domain set as its proxy domain.
Step 12 Select Enable at the top of the window to enable the new user. The user should have a check mark in the Enabled column.

What to Do Next
Microsoft Lync Server Setup Overview, on page 24

Related Topics
   Line URI Setup on Microsoft Active Directory, on page 21
   IM and Presence Service User Authentication, on page 22
   Line Appearances, on page 4

Microsoft Lync Server Setup Overview

Note  This topic provides a brief description of the configuration required on Microsoft Lync Server for this integration. A comprehensive description of Microsoft Lync configuration is out of the scope of this document. For more information, see the Microsoft Lync documentation at the following URL: http://technet.microsoft.com/en-us/library/gg558664.aspx.
Make sure that the Microsoft Lync server is properly installed and activated. Make sure that the following items are configured on Microsoft Lync:

1. Certificate configuration
2. Static Routes
3. Authorized Host
4. Domain Name Server
5. Pool Properties
6. Server Properties
7. Pool Users
8. User Configuration
9. Microsoft Lync Client Configuration

If the CTI Gateway is configured to use TCP, you must define the IP address of the Gateway in Lync Server Topology Builder. See the following URL for more information: http://technet.microsoft.com/en-us/library/gg602125.aspx.

You configure the Microsoft Lync Server using the Lync Server Management Shell utility. The Management Shell utility is installed by default with the Lync server installation. Set up the following items during Microsoft Lync server configuration:

- static routes
- application pools
- Remote Call Control (RCC) application
- Lync server SIP listen port

After you set up the Microsoft Lync Server, commit the topology and restart the front-end service.

**Set Up Static Route for Microsoft Lync Server**

The Lync server uses the static route to match the URI of the incoming client's SIP message INVITE. The Lync server references the URI value as the Line Server URI.

**Procedure**

**Step 1** Select Start > All Programs > Microsoft Lync Server > Lync Server Management Shell.

**Step 2** Enter the following command to verify the current system configuration:

```
Get-CsStaticRoutingConfiguration
```

**Step 3** Enter the following command to create a static route:

```
$tcpRoute = New-CsStaticRoute -TCPRoute -Destination <IP_address_CUPserver> -Port 5060 -MatchUri "<Line_Server_URI_domain>" -ReplaceHostInRequestUri $true
```

**Step 4** At the prompt, enter the following command to load the static route into the Lync server.

```
Set-CsStaticRoutingConfiguration -Route @($tcpRoute)
```

**Step 5** Verify the new system configuration by entering the Get command from Step 2, on page 25 again.
If you need to modify or delete a static route, enter the following command:

```
Remove-CsStaticRoutingConfiguration -Identity Global
```

The following table describes the parameters that you use to insert a new static route for Lync server.

**Table 1: Static route parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$tcpRoute</td>
<td>The name of the variable. It can be named anything but it must begin with a $ and match the reference in the Set command.</td>
</tr>
<tr>
<td>New-CsStaticRoute</td>
<td>The internal command that populates the static route to a variable.</td>
</tr>
<tr>
<td>-TCPRoute</td>
<td>This parameter configures the route as TCP.</td>
</tr>
<tr>
<td>-Destination</td>
<td>The IP address of the IM and Presence Service node.</td>
</tr>
<tr>
<td>-Port</td>
<td>The port to which the IM and Presence Service node listens. For TCP, the port is 5060.</td>
</tr>
<tr>
<td>-MatchUri</td>
<td>This value is compared to the Line Server URI value that is specified for each user in the Lync Control Panel. See Enable Users in Lync Server Control Panel, on page 23. This MatchURI value and the Line Server URI value must both match the IM and Presence Service node FQDN. The value of this parameter must be written in double quotes, for example, <code>-MatchUri &quot;my-cups.my-domain.com&quot;</code></td>
</tr>
<tr>
<td>-ReplaceHostInRequestUri</td>
<td>This parameter replaces the URI in the initial INVITE to the value that is referenced in the Destination parameter.</td>
</tr>
<tr>
<td>-CsStaticRoutingConfiguration</td>
<td>The internal command to move parameter values to the routing database.</td>
</tr>
<tr>
<td>-Route</td>
<td>This parameter takes the parameters in the variable and adds the static route.</td>
</tr>
</tbody>
</table>

**What to Do Next**

Set Up Application Pool for Microsoft Lync Server, on page 26

**Set Up Application Pool for Microsoft Lync Server**

The following procedure sets up an application pool that is referenced by the Lync server (registrar). It also links the site information to this pool.
Procedure

Step 1  In the Lync Server Management Shell enter the following command to verify the current system configuration:

```
Get-CsTrustedApplicationPool
```

Step 2  Enter the following command to create the application pool:

```
New-CsTrustedApplicationPool -Identity "<IP_address_CUPserver>" -Registrar <Lync_server_FQDN> -Site 1 -TreatAsAuthenticated $True -ThrottleAsServer $True -RequiresReplication $False
```

Step 3  Select Y at the prompt.

Step 4  Verify the new system configuration by entering the Get command from Step 1, on page 27 again.

Tip  If you need to modify or delete the application pool, enter the following command:

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_address_CUPserver>
```

The following table describes the parameters that you use to configure the application pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-CsTrustedApplicationPool</td>
<td>The internal command that adds the application pool.</td>
</tr>
<tr>
<td>-Identity</td>
<td>The reference name of the pool which is also the IP address of the IM and Presence Service node.</td>
</tr>
<tr>
<td></td>
<td>The value of this parameter must be written in double quotes, for example, -Identity &quot;10.0.0.1&quot;</td>
</tr>
<tr>
<td></td>
<td>This value must match the value in the TrustedApplicationPoolFqdn parameter of the TrustedApplication command in Set Up RCC Application for Microsoft Lync Server, on page 28.</td>
</tr>
<tr>
<td>-Registrar</td>
<td>The FQDN of the Lync server.</td>
</tr>
<tr>
<td>-Site</td>
<td>The numeric value of the site.</td>
</tr>
<tr>
<td></td>
<td>Tip You can find the site ID with the Get-CsSite Management Shell command.</td>
</tr>
<tr>
<td>-TreatAsAuthenticated</td>
<td>Always set this value to $True</td>
</tr>
<tr>
<td>-ThrottleAsServer</td>
<td>Always set this value to $True</td>
</tr>
<tr>
<td>-RequiresReplication</td>
<td>Because authentication is not required for TCP, you must set this value to $False</td>
</tr>
</tbody>
</table>

What to Do Next

Set Up RCC Application for Microsoft Lync Server, on page 28
Set Up RCC Application for Microsoft Lync Server

The following procedure adds the Microsoft Remote Call Control (RCC) application to the pool.

**Procedure**

**Step 1**  
In the Lync Server Management Shell enter the following command to verify the current system configuration:

```
Get-CSTrustedApplication
```

**Step 2**  
Enter the following command to add the RCC application to the pool:

```
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn "<IP_address_CUPserver>" -Port 5060 -EnableTcp
```

**Step 3**  
Select Y at the prompt.

**Step 4**  
Verify the new system configuration by entering the Get command from Step 1, on page 28 again.

**Tip**  
If you need to modify or delete the application pool, enter the following command:

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_address_CUPserver>
```

The following table describes the parameters that you use to configure the application pool.

**Table 3: Application configuration parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-CsTrustedApplication</td>
<td>The internal command that adds the RCC application.</td>
</tr>
<tr>
<td>-ApplicationID</td>
<td>The name of the application, for example, RCC.</td>
</tr>
<tr>
<td>-TrustedApplicationPoolFQDN</td>
<td>The IP address of the IM and Presence Service node. The value of this parameter must be written in double quotes, for example, -Identity &quot;10.0.0.1&quot; This value must match the value in the Identity parameter of the TrustedApplicationpool command in Set Up Application Pool for Microsoft Lync Server, on page 26.</td>
</tr>
<tr>
<td>-Port</td>
<td>The SIP TCP listening port of the IM and Presence Service node. For TCP, the port is 5060.</td>
</tr>
<tr>
<td>-EnableTCP</td>
<td>This parameter sets the transport to TCP. If this parameter is not included, the transport will default to TLS.</td>
</tr>
</tbody>
</table>

**Note**  
See Security between IM and Presence Service and Microsoft Lync Setup, on page 43 for more information about Communication with Microsoft Lync server over TLS.

**What to Do Next**

Set Up Lync Server SIP Listen Port, on page 29
Set Up Lync Server SIP Listen Port

The following procedure sets the SIP listen port on the Lync server. This is required for incoming SIP traffic from the IM and Presence Service node.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | In the Lync Server Management Shell enter the following command to verify the current system configuration:  
Get-CsRegistrarConfiguration |
| **Step 2** | Enter the following command to set the Lync server listening port:  
Set-CsRegistrar registrar:<Lync_server_FQDN> -SipServerTcpPort 5060 |
| **Step 3** | Verify the new system configuration by entering the Get command from **Step 1, on page 29** again.  
**Tip** If you need to modify or delete the application pool, enter the following command:  
Remove-CsRegistrarConfiguration |

The following table describes the parameters that you use to configure the Lync server listen port.

**Table 4: Lync server listen port parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set-CsRegistrar</td>
<td>Internal command that sets the Lync server port.</td>
</tr>
<tr>
<td>registrar:</td>
<td>FQDN of the Lync server.</td>
</tr>
<tr>
<td>-SipServerTcpPort</td>
<td>SIP listening port of the Lync server. The default value is typically 5060.</td>
</tr>
</tbody>
</table>

**What to Do Next**

Commit Lync Server Setup, on page 29

Commit Lync Server Setup

This procedure describes how to commit the topology and restart the front-end service.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | In the Lync Server Management Shell enter the following command to enable the topology:  
Enable-CsTopology |
| **Step 2** | Enter the following command to output the topology to an XML file called rcc.xml and save it to the C drive:  
Get-CsTopology -AsXml | Out-File C:\rcc.xml  
**Note** You can select any name and location to output the topology information.
Step 3  Open the rcc.xml file.
Step 4  In the Cluster Fqdn section, change the IPAddress parameter from "<0.0.0.0>" to the IP Address of the IM and Presence Service node.
Step 5  Save the rcc.xml file.
Step 6  Enter the following command in the Lync Server Management Shell:
        Publish-CsTopology -FileName C:\rcc.xml
Step 7  Enter the following command to restart the front-end service:
        Restart-Service RtcSrv

What to Do Next
Normalization Rules Setup, on page 31
Normalization Rules Setup

- Set Up Normalization Rules on Microsoft Active Directory, page 31
- Update Microsoft Lync Address Book, page 33

Set Up Normalization Rules on Microsoft Active Directory

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

- the user is not provisioned for E.164 in Active Directory and
- 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 Lync.

Therefore you must set up the correct normalization rules for the Active Directory address book on the Microsoft Lync server to enable the Microsoft Lync user to see the 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 Lync must be on the Microsoft Lync 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

Ensure that normalization is enabled in Lync Server. To do this, open the Lync Server Management Shell and enter the following command:

Get-CsAddressBookConfiguration
If the UseNormalizationRules value is set to True, normalization is enabled. If the UseNormalizationRules value is set to False, enter the following command to enable normalization:

```powershell
Set-CsAddressBookConfiguration -UseNormalizationRules $True
```

**Step 2**  
Locate the ABFiles subdirectory in the Lync Server's shared directory that was configured during initial server deployment. Select **Topology Builder > File Stores** to identify the file server FQDN and share name. The path is as follows: `\\<Server FQDN>\<Share Folder>\1-WebServices-1\ABFiles`

**Step 3**  
Navigate to the following sample file: `C:\Program Files\Microsoft Lync Server 2010\WebComponents\Address Book Files\Files\Sample.Company.Phone_Number_Normalization_Rules.txt`

**Step 4**  
Make a copy of the `Sample.Company.Phone_Number_Normalization_Rules.txt` file and save it as `Company.Phone_Number_Normalization_Rules.txt` in the ABFiles directory.  
**Note** You must save the `Company.Phone_Number_Normalization_Rules.txt` file in the ABFiles directory, and not where the actual address book files are saved.

**Step 5**  
Open the `Company.Phone_Number_Normalization_Rules.txt` file in Notepad and remove regex code like `\[\s()\-./\]`. Microsoft Lync Server ignores non-telephony related digits and only analyzes the continuous 0-9 numerical digit patterns. However it does recognize the + prefix.

**Step 6**  
In Lync Server Management Shell, enter the following command to import the new settings in the `Company.Phone_Number_Normalization_Rules.txt` file and apply them to numbers stored in the address book files:

```powershell
Update-CsAddressBook
```

**Step 7**  
Wait for five before you force an address book update on the Lync client, see Update Microsoft Lync Address Book, on page 33.

---

### What to Do Next

Update Microsoft Lync Address Book, on page 33

---

### Sample Normalization Rules

```plaintext
## +1 (ddd) ddd-dddd EXTdddd
#
\+l\(d(10)\)EXT\(d(5)\)
+151;ext=$2
#
## +1 (ddd) ddd-dddd Xdddd
#
\+l\(d(10)\)[Xx]{1}\(d(5)\)
+151;ext=$2
#
## 1 (ddd) ddd-dddd
#
1\(d(10)\)
+151
#
## +1 (ddd) 70dddd
#
\+l\(d(3)\)70\(d(5)\)
+15170$2;ext=$2
#
## 70d-dddd Xdddd
#
70\(d(5)\)[Xx]{1}\(d(5)\)
+142570$1;ext=$2
#
## ddd-dddd Xdddd
```

---

Remote Call Control with Microsoft Lync Server 2010 for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)
Update Microsoft Lync Address Book

With the default server/client settings, the Address Book is not immediately updated. To ensure that the Address Book is updated with the latest users added to the Active Directory, you must force the update on the server side and then force Microsoft Lync to pull down the latest files to update its local GalContacts.db file.

Procedure

Step 1 On Lync Server, enter the following command in the Lync Server Management Shell:
Update-CsAddressBook
This command triggers the Lync Server to synchronize current Active Directory information in the SQL database into the downloadable client and device address book files.

Note Wait five minutes for the synchronization process to complete.

Step 2 With Administrator privileges on Microsoft Lync, enter the following command in the Windows Command Prompt:
reg add HKLM\Software\Policies\Microsoft\Communicator /v GalDownloadInitialDelay /t REG_DWORD /d 0 /f
This command forces Microsoft Lync to immediately download the address book.

Step 3 Check whether the GalContacts.db and GalContacts.db.idx files exist on Microsoft Lync. If they do exist, delete them from the user's profile directory.

Step 4 Exit Microsoft Lync. Do not just sign out.

Step 5 Start the Microsoft Lync client and sign in again.

Step 6 Verify that the updated GalContacts.db and GalContacts.db.idx files have been downloaded.

Step 7 Perform a search for the new users and verify that their usernames display in Microsoft Lync.

What to Do Next

Security Certificate Setup for IM and Presence Service, on page 35

Related Topics

Set Up Normalization Rules on Microsoft Active Directory, on page 31
CHAPTER 7

Security Certificate Setup for IM and Presence Service

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

This chapter describes how to configure security certificates using a standalone CA. If you use an enterprise CA, see 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:

• Set Up Standalone Root Certificate Authority (CA), page 35
• Download Root Certificate from CA Server, page 36
• Upload Root Certificate to IM and Presence Service, page 37
• Generate Certificate Signing Request for IM and Presence Service, page 38
• Download CSR from IM and Presence Service, page 38
• Submit Certificate Signing Request on CA Server, page 39
• Download Signed Certificate from CA Server, page 39
• Upload Signed Certificate to IM and Presence Service, page 40

Note

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

Set Up Standalone Root Certificate Authority (CA)

Complete the following procedure to configure the standalone root 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 and double-click Add or Remove Programs.
Step 4  Select Add/Remove Windows Components.
Step 5  Select Application Server, then select Internet Information Services (IIS).
Step 6  Complete the installation procedure.
Step 7  Select Add/Remove Windows Components.
Step 8  Select Certificate Services, then select Next.
Step 9  Select Standalone root CA, then select Next.
Step 10 Type the name of the CA root.
    Note This name can be a friendly name for the CA root in the forest root.
Step 11 Change the time to the number of years required for this certificate and select Next to begin installation.
Step 12 Select the location for the certificate database and the certificate database files.
Step 13 Select Next.
Step 14 Select Yes when prompted to stop IIS.
Step 15 Select Yes when prompted with a message regarding Active Server Pages, then select Finish.

What to Do Next

Download Root Certificate from CA Server, on page 36.

Download Root Certificate from CA Server

Complete the following procedure to download 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.
Important 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 a Windows operating system, you can right-click the certificate file with a .cer extension and open the certificate properties.
Upload Root Certificate to IM and Presence Service

Complete the following procedure to upload the 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.

**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 and locate the certnew.cer file on your local computer.
*Note* You may need to change the certificate file to a .pem extension.

**Step 6** 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.

What to Do Next
Generate Certificate Signing Request for IM and Presence Service, on page 38

Related Topics
Download Root Certificate from CA Server, on page 36
Upload Signed Certificate to IM and Presence Service, on page 40
Generate Certificate Signing Request for IM and Presence Service

Complete the following procedure to generate a Certificate Signing Request (CSR) for IM and Presence Service.

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

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.

What to Do Next
Download CSR from IM and Presence Service, on page 38

Related Topics
Upload Root Certificate to IM and Presence Service, on page 37

Download CSR from IM and Presence Service

Complete the following procedure to download the CSR from IM and Presence Service.

Before You Begin
Generate a CSR for IM and Presence Service.

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.

What to Do Next
Submit Certificate Signing Request on CA Server, on page 39
Submit Certificate Signing Request on CA Server

Complete the following procedure to submit the CSR on the CA server.

Before You Begin
Download the CSR 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 Select Request a certificate, then select Advanced certificate request.
Step 4 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 5 Using a text editor like Notepad, open the cup self-certificate that you generated.
Step 6 Copy all information from and including

-----BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST-----

Step 7 Paste the content of the certificate request into the Certificate Request text box.
Step 8 Select Submit.
The Request ID number displays.
Step 9 Open Certificate Authority in Administrative Tools.
The Certificate Authority window displays the request you just submitted under Pending Requests.
Step 10 Right-click on your certificate request and select All Tasks Issue.
Step 11 Select Issued certificates and verify that your certificate has been issued.

What to Do Next
Download Signed Certificate from CA Server, on page 39

Related Topics
Download CSR from IM and Presence Service, on page 38

Download Signed Certificate from CA Server

Complete the following procedure to download the signed certificate from the CA server.
Before You Begin
Submit the CSR 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.

What to Do Next
Upload Signed Certificate to IM and Presence Service, on page 40

Related Topics
Submit Certificate Signing Request on CA Server, on page 39

Upload Signed Certificate to IM and Presence Service

Complete the following procedure to upload the signed certificate to IM and Presence Service.

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 and locate the signed cup.pem certificate on your local computer.
Step 6 Select Upload File.

What to Do Next
Lync Remote Call Control Installation, on page 55
Related Topics

Download Signed Certificate from CA Server, on page 39
Security between IM and Presence Service and Microsoft Lync Setup

This chapter is only applicable if you require a secure connection between the IM and Presence Service and Microsoft Lync.

- Security Certificate for Microsoft Lync Setup, page 43
- Verify Certificate Setup for Server and Client Authentication, page 47
- TLS Route for Microsoft Lync Setup, page 48
- Set Up Microsoft Lync for TLSv1, page 52
- Create New TLS Peer Subject for Microsoft Lync, page 52
- Add TLS Peer to TLS Peer Subjects List, page 53

Security Certificate for Microsoft Lync Setup

Download CA Certification Chain

Complete the following procedure to download the CA certification chain.

Procedure

Step 1 Select Start > Run.
Step 2 Enter http://<name of your Issuing CA Server>/certsrv and select OK.
Step 3 From Select a task, select Download a CA certificate, certificate chain, or CRL.
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.
Note  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 44

Install CA Certification Chain

Complete the following procedure to install the CA certification chain.

**Before You Begin**
Download the CA certification chain.

**Procedure**

**Step 1** Select Start > Run.
**Step 2** Enter mmc and 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 and select Add.
**Step 6** Select Computer account and select Next.
**Step 7** In the Select Computer dialog box, ensure Local computer: (the computer this console is running on) is selected.
**Step 8** Select Finish, select Close, and then select OK.
**Step 9** Expand Certificates (Local Computer) in the left pane of the Certificates console.
**Step 10** Expand Trusted Root Certification Authorities and right-click Certificates.
**Step 11** Point to All Tasks and select Import.
**Step 12** Select Next in the Import Wizard.
**Step 13** Select Browse and locate the certificate chain on your computer.
**Step 14** Select Open and select Next.
**Step 15** Leave the default value Place all certificates in the following store selected.
**Step 16** Ensure Trusted Root Certification Authorities appears under the Certificate store.
**Step 17** Select Next and select Finish.

What to Do Next
Submit Certificate Request on CA Server, on page 45
Submit Certificate Request on CA Server

Complete the following procedure to submit the certificate request on the CA server.

Before You Begin
Install the CA Certification Chain.

Procedure

Step 1 Select Start > All Programs > Microsoft Lync Server > Lync Server Management Shell.

Step 2 Enter the following command to create a certificate request for Microsoft Lync Server:
Request-CsCertificate -New -Type Default -DomainName <FQDN of Lync Server> -Output c:\cert.csr -ClientEku $true

Step 3 From Microsoft Lync Server, enter the URL http://<name of your Issuing CA server>/certsrv.

Step 4 Select Request a Certificate and then 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 Open the file cert.csr from Step 2, on page 45 and copy all information in the file to the clipboard.

Step 7 Paste the information from the file cert.csr to the Saved Request box in the certificate authority server and select Submit.

What to Do Next
Approve and Import Certificate, on page 45

Related Topics
Install CA Certification Chain, on page 44

Approve and Import Certificate

Complete the following procedure to approve and import the certificate.

Before You Begin
Submit the Certificate Request on the CA Server.
Procedure

Step 1  From the Certificate Authority Server, select Administrative Tools > Certificate Authority.
Step 2  Select Pending Requests and find the new certificate in the list.
Step 3  Right-click on the new certificate and select All Tasks > Issue Certificate.
Step 4  From Microsoft Lync Server, enter the URL http://<name of your Issuing CA server>/certsrv.
Step 5  Select View the status of a pending certificate request.
Step 6  Select Base 64 encoded and download the certificate as a cer file extension to the Microsoft Lync server local drive.
Step 7  Sign in as a member of the Administrators group to the same Microsoft Lync Server on which you created the certificate request.
Step 8  Start the Lync Server Deployment Wizard and select Install or Update Lync Server System.
Step 9  Select Run Again (beside Step 3: Request, Install, or Assign Certificates).
Step 10 From the Available Certificate Tasks page, select Import a certificate from a .p7b, .pfx or .cer file.
Step 11 In the Import Certificate page, enter the full path and filename of the certificate that you retrieved from the Certificate Authority in Step 6, on page 46. Alternatively, you can select Browse to locate and select the file.

What to Do Next
Assign Imported Certificate, on page 46

Related Topics
Submit Certificate Request on CA Server, on page 45

Assign Imported Certificate

Complete the following procedure to assign the imported certificate.

Before You Begin
Approve and import the Certificate.
Procedure

Step 1  From Microsoft Lync Server start the Lync Server Deployment Wizard.
Step 2  Select Install or Update Lync Server System.
Step 3  Select Run Again in Step 3: Request, Install or Assign Certificates.
Step 4  From the Available Certificate Tasks page, select Assign an existing certificate.
Step 5  From the Certificate Assignment page, select Next.
Step 6  From the Advanced Certificate Usages page, select all checkboxes to assign the certificate for all usages.
Step 7  From the Certificate Store page, select the certificate that you requested and imported.
Step 8  In the Certificate Assignment Summary page, review your settings, and select Next to assign the certificates.
Step 9  From the wizard completion page, select Finish.
Step 10  Open the Certificate snap-in on each server, select Certificates (Local computer) > Personal > Certificates, and verify that the certificate is listed in the Details pane.

What to Do Next
Verify Certificate Setup for Server and Client Authentication, on page 47

Related Topics
Approve and Import Certificate, on page 45

Verify Certificate Setup for Server and Client Authentication

Complete the following procedure to verify that the certificate is properly configured for server and client authentication.

Procedure

Step 1  From Microsoft Lync Server, start the Lync Server Deployment Wizard.
Step 2  Select Install or Update Lync Server System.
Step 3  Select Run Again in Step 3: Request, Install or Assign Certificates.
Step 4  In the Certificate Wizard screen, highlight the Default certificate and select View.
Step 5  In the View Certificate screen, select View Certificate Details.
Step 6  In the Certificate screen, select the Details tab.
Step 7  From the Show drop-down list, select Extensions Only.
Step 8  Select Enhanced Key Usage and verify that the following are listed: Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Step 9  Select Start > All Programs > Microsoft Lync Server > Lync Server Management Shell.
Step 10  Enter the following command to view the certificate from Microsoft Lync Server: Get-CsCertificate
Step 11  Verify that the Default certificate is present and similar to the following:
Issuer : CN=ne001a-lyncca
NotAfter : 6/16/2012 2:18:20 PM
TLS Route for Microsoft Lync Setup

Set up the following items to configure a TLS route for IM and Presence Service on Microsoft Lync:

• static routes
• application pools
• Microsoft Remote Call Control (RCC) application

After you set up a TLS route for IM and Presence Service on Microsoft Lync, commit the topology and restart the front-end service.

Set Up Static Route

Complete the following procedure to configure the static route.

Procedure

Step 1  Select Start > All Programs > Microsoft Lync Server > Lync Server Management Shell.

Step 2  If there is a TCP route, remove it with the following command:
        Remove-CsStaticRoutingConfiguration -Identity Global

Step 3  Enter the following command to create a static TLS route:
        $tlsRoute = New-CsStaticRoute -TLSRoute -Destination <FQDN CUP Server> -Port 5062 -MatchUri *.rcdnlync.com -UseDefaultCertificate $true

Step 4  At the prompt, enter the following command to load the static route into the Lync server.
        Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}

Step 5  Verify the new system configuration by entering the following command:
        Get-CsStaticRoutingConfiguration

The following table describes the parameters that you use to insert a new static route for Lync server.
Table 5: Static route parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$tlsRoute</td>
<td>The name of the variable. It can be named anything but it must begin with a $ and match the reference in the Set command.</td>
</tr>
<tr>
<td>New-CsStaticRoute</td>
<td>The internal command that populates the static route to a variable.</td>
</tr>
<tr>
<td>-TLSRoute</td>
<td>This parameter configures the route as TLS.</td>
</tr>
<tr>
<td>-Destination</td>
<td>The FQDN of the IM and Presence Service node.</td>
</tr>
<tr>
<td>-Port</td>
<td>The port to which the IM and Presence Service node listens. For TLS, the port is 5062.</td>
</tr>
<tr>
<td>-MatchUri</td>
<td>This value is a wildcard, denoted by an asterisk (*), followed by a domain. It is compared to the Line Server URI value that is specified for each user in the Lync Control Panel. See Enable Users in Lync Server Control Panel, on page 23.</td>
</tr>
<tr>
<td>-UseDefaultCertificate</td>
<td>This value is set to True to instruct the static route to use the default certificate.</td>
</tr>
<tr>
<td>-CsStaticRoutingConfiguration</td>
<td>The internal command to move parameter values to the routing database.</td>
</tr>
<tr>
<td>-Route</td>
<td>This parameter takes the parameters in the variable and adds the static route.</td>
</tr>
</tbody>
</table>

What to Do Next

Set Up Application Pool, on page 49

Set Up Application Pool

The following procedure sets up an application pool that is referenced by the Lync server (registrar). It also links the site information to this pool.

Procedure

**Step 1** Select **Start > All Programs > Microsoft Lync Server > Lync Server Management Shell**.

**Step 2** Enter the following command to remove any existing TCP application pool:

```
Remove-CsTrustedApplicationPool -Identity TrustedApplicationPool:<IP_Address_CUPserver>
```

**Step 3** Enter the following command to create the application pool:
New-CsTrustedApplicationPool -Identity <FQDN CUP Server> -Registrar <FQDN of Pool> -Site 1
-ThrottleAsServer $true -TreatAsAuthenticated $true

**Step 4** Select Y at the prompt.

**Step 5** Verify the new system configuration by entering the following command:
Get-CsTrustedApplicationPool
The following table describes the parameters that you use to configure the application pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-CsTrustedApplicationPool</td>
<td>The internal command that adds the application pool.</td>
</tr>
<tr>
<td>-Identity</td>
<td>The FQDN of the IM and Presence Service node.</td>
</tr>
<tr>
<td>-Registrar</td>
<td>The reference name of the pool. It can also be the FQDN of the Lync server.</td>
</tr>
<tr>
<td>-Site</td>
<td>The numeric value of the site.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can find the site ID with the Get-CsSite Management Shell command.</td>
</tr>
<tr>
<td>-TreatAsAuthenticated</td>
<td>Always set this value to $True</td>
</tr>
<tr>
<td>-ThrottleAsServer</td>
<td>Always set this value to $True</td>
</tr>
</tbody>
</table>

**What to Do Next**
Set Up RCC Application, on page 50

### Set Up RCC Application

The following procedure adds the Microsoft Remote Call Control (RCC) application to the pool.

**Procedure**

**Step 1** Select Start > All Programs > Microsoft Lync Server > Lync Server Management Shell.

**Step 2** Enter the following command to remove any existing TCP application:
Remove-CsTrustedApplication -Identity <FQDN of IM and Presence server>/urn:application:rcc

**Step 3** Enter the following command to add the RCC application to the pool:
New-CsTrustedApplication -ApplicationID RCC -TrustedApplicationPoolFqdn <FQDN of IM and Presence server> -Port 5062

**Step 4** Select Y at the prompt.

**Step 5** Verify the new system configuration by entering the following command:
Get-CsTrustedApplication
The following table describes the parameters that you use to configure the application pool.

**Table 7: Application configuration parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-CsTrustedApplication</td>
<td>The internal command that adds the RCC application.</td>
</tr>
<tr>
<td>-ApplicationID</td>
<td>The name of the application, for example, RCC.</td>
</tr>
<tr>
<td>-TrustedApplicationPoolFQDN</td>
<td>The FQDN of the IM and Presence Service node.</td>
</tr>
<tr>
<td>-Port</td>
<td>The SIP TLS listening port of the IM and Presence Service node. For TLS, the port is 5062.</td>
</tr>
</tbody>
</table>

**What to Do Next**
Commit Lync Server Setup, on page 51

**Commit Lync Server Setup**

This procedure describes how to commit the topology and restart the front-end service.

**Procedure**

**Step 1**
In the Lync Server Management Shell enter the following command to enable the topology:
Enable-CsTopology

**Step 2**
Enter the following command to output the topology to an XML file called rcc.xml and save it to the C drive:
Get-CsTopology -AsXml | Out-File C:\rcc.xml

**Note** You can select any name and location to output the topology information.

**Step 3**
Open the rcc.xml file.

**Step 4**
In the **Cluster Fqdn** section, change the IP Address parameter from “<0.0.0.0>” to the IP Address of the IM and Presence Service node.

**Step 5**
Save the rcc.xml file.

**Step 6**
Enter the following command in the Lync Server Management Shell:
Publish-CsTopology -FileName C:\rcc.xml

**Step 7**
Enter the following command to restart the front-end service:
Restart-Service RtcSrv
Set Up Microsoft Lync for TLSv1

IM and Presence Service only supports TLSv1 so you must configure Microsoft Lync to use TLSv1. This procedure describes how to configure FIPS-compliant algorithms on Microsoft Lync to ensure that Microsoft Lync sends TLSv1 with TLS cipher TLS_RSA_WITH_3DES_EDE_CBC_SHA.

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 and modify the security setting.
Step 6 Select OK.
Step 7 Restart the Windows Server for the change to the FIPS security setting to take effect.

Create New TLS Peer Subject for Microsoft Lync

Complete the following procedure to create a new TLS Peer Subject for Microsoft Lync on IM and Presence Service.

Procedure

Step 1 Select Cisco Unified CM IM and Presence Administration > IM and Presence > Security > TLS Peer Subjects.
Step 2 Select Add New.
Step 3 In the Peer Subject Name field, enter the subject CN of the certificate that Microsoft Lync presents.
Step 4 In the Description field, enter the name of the Microsoft Lync server.
Step 5 Select Save.
Add TLS Peer to TLS Peer Subjects List

Complete the following procedure to add the TLS Peer to the selected TLS Peer Subjects list on IM and Presence Service.

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

Procedure

Step 1 Select Cisco Unified CM IM and Presence AdministrationSystemSecurityTLS 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.

What to Do Next
Lync Remote Call Control Installation, on page 55
Lync Remote Call Control Installation

- Install IM and Presence Service Lync Remote Call Control Plugin on Client Computer, page 55
- Uninstall IM and Presence Service Lync Remote Call Control Plugin, page 56
- Access Phone Selection Through a Web Browser, page 57

Install IM and Presence Service Lync Remote Call Control Plugin on Client Computer

The Cisco Unified CM IM and Presence Service Lync Remote Call Control Plugin adds a IM and Presence Service menu item to the Microsoft Lync client interface that enables the user to select a phone device to control. You must install this plug-in if the user has multiple devices (lines). When the user selects the IM and Presence Service menu item, IM and Presence Service opens a web page in the user's default web browser. The user can select which phone device to control from this web page.

Before You Begin

- Your username and password for Cisco Unified Communications Manager IM and Presence Service User Options.

- The administrator must assign the user to the "Standard CCM End User" Group. Confirm that you have been added to this group.

- For this procedure you require the Cisco Unified Communications Manager IM and Presence Lync Remote Call Control Plugin batch file called addrccmenu.bat, which you can download from the Cisco Unified CM IM and Presence Administration user interface. Select Application > Plugins and download the Cisco Unified Communications Manager IM and Presence Lync Remote Call Control Plugin. The batch file is downloaded as a zip file. You must save this zip file to a location on the Microsoft Lync client computer and extract its contents.
Procedure

Step 1 Open a Windows command prompt on the Microsoft Lync client computer.
Step 2 Navigate to the location of the extracted addrccmenu.bat file.
Step 3 At the command line, enter the following command, where impserveraddress is the IP address, hostname or FQDN of the IM and Presence Service node:

```
addrccmenu.bat impserveraddress
```

Step 4 If you receive a regedit security warning, allow the operation to continue.
Step 5 When the operation is complete, log out and exit the Microsoft Lync client.
Step 6 Log in to the Microsoft Lync client again and choose the Tools menu option. You can now see the new Cisco menu item.

Note If you need to direct the IM and Presence Service menu item to a different IM and Presence Service node, you can execute this procedure again using the IP address, hostname or FQDN for a different IM and Presence Service node.

What to Do Next

If the IM and Presence Service web page does not open in the user's default web browser when the Microsoft Lync client user accesses the IM and Presence Service menu item, see IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser., on page 69

Uninstall IM and Presence Service Lync Remote Call Control Plugin

To uninstall the Cisco Unified Communications Manager IM and Presence Service Lync Remote Call Control Plugin, you must rerun the batch file without specifying the IP address, hostname or FQDN of the IM and Presence Service node.

Procedure

Step 1 Download the zip file to the Microsoft Lync computer and extract the contents of the zip file.
Step 2 Open a Windows command prompt.
Step 3 Navigate to the location of the extracted addrccmenu.bat file.
Step 4 At the command line, enter the following command:

```
addrccmenu.bat
```

Step 5 If you receive a regedit security warning, allow the operation to continue.
Step 6 When the operation is complete, log out and exit the Microsoft Lync client.
Step 7 Log in to the Microsoft Lync client again and select the Tools menu option. The Cisco menu item should no longer be visible.
Access Phone Selection Through a Web Browser

You use the Cisco Unified Communications Manager IM and Presence Service User Options 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 or IP address for Cisco Unified Communications Manager IM and Presence Service User Options.
- Your username and password for Cisco Unified Communications Manager IM and Presence Service User Options.
- To be able to log in to the Cisco Unified Communications Manager IM and Presence Service User Options Web interface, the administrator must assign the user to the "Standard CCM End User" Group.

Procedure

Step 1  Open a supported Web browser on your computer.
Step 2  Enter the URL addresses for Cisco Unified Communications Manager IM and Presence Service User Options: https://imp_server_address:8443/cupuser/showHomeMini.do?mini=true
Where imp_server_address is the hostname, FQDN, or IP address of the IM and Presence Service node.
Step 3  Enter your username for Cisco Unified Communications Manager IM and Presence Service User Options.
Step 4  Enter your password Cisco Unified Communications Manager IM and Presence Service User Options provided by your system administrator.
Step 5  Click Login.
   To log out of the User Options Web interface, click Logout in the upper right corner of the User Options page. For security purposes, you will be automatically logged out of User Options after thirty minutes of inactivity.
Microsoft Lync Server and Microsoft Lync Client Logging

The Lync Server Logging Tool allows you to initiate traces of the Lync server and view message logs. The Microsoft Lync client also allows you to collect logging information for SIP messaging and other client-related logging information.

- Initiate Trace and View Microsoft Lync Server Log, page 59
- Enable and View Microsoft Lync Client Logs, page 60

Initiate Trace and View Microsoft Lync Server Log

Use the following procedure to initiate a trace of the Microsoft Lync server and view the message logs.

**Procedure**

**Step 1** Select Start > All Programs > Microsoft Lync Server > Lync Server Logging Tool.
**Step 2** In the Components area, check the SIPStack check box.
**Step 3** In the Level area, choose the All option.
**Step 4** In the Flags area, check all the flags.
**Step 5** When you are ready to begin the trace, select Start Logging.
**Step 6** When you are ready to stop the trace, select Stop Logging.
**Step 7** Select Analyze Log Files.
**Step 8** Check the SIPStack and the SIPStackPerf check boxes.
**Step 9** Select Analyze.
**Step 10** Select the Messages tab and click on any message to view its contents.
Enable and View Microsoft Lync Client Logs

Use the following procedure to enable client logging and view the resulting logs.

Procedure

Step 1 Select Start > All Programs > Microsoft Lync > Microsoft Lync Server.
Step 2 Click on the drop-down arrow on the top right of the window.
Step 3 Select Tools > Options.
Step 4 Select General from the left pane.
Step 5 In the Logging area, check the Turn on logging in Lync and Turn on Windows Event logging for Lync check boxes.
Step 6 Select OK.
Step 7 Exit the Lync client. Do not just sign out of the Lync client.
Step 8 Go to C:\Users\Administrator.NE001B-LYNCAD\Tracing> on your client computer.
Step 9 Select all files in this directory and delete them.
Step 10 Sign in to the Lync client.
   Tip You will see new files being created in C:\Users\Administrator.NE001B-LYNCAD\Tracing>.
Step 11 Complete a sign in or call attempt from the Lync client.
Step 12 Exit the Lync client.
Step 13 Open the Communicator-uccapi-0 file in C:\Users\Administrator.NE001B-LYNCAD\Tracing>.
   Note The Communicator-uccapi-0 file contains logs for SIP messaging and other client-related logging information.
Load Balancer Configuration for Lync RCC Integration

- About the Load Balancer, page 61
- IM and Presence Service node updates, page 61
- Cisco Adaptive Security Appliance Updates, page 62
- CA-Signed Security Certificate Update, page 66
- Microsoft Component Updates, page 67

About the Load Balancer

For redundancy and high availability purposes, you can incorporate a load balancer into your Lync RCC Integration. The load balancer is placed between the IM and Presence Service node and the Cisco Adaptive Security Appliance.

The load balancer terminates incoming TLS connections from Cisco Adaptive Security Appliance, and initiates a new TLS connection to route the content to the appropriate backend IM and Presence Service node.

Note

Before carrying out the procedures in this chapter, check your Load Balancer product documentation for further information on the End of Service dates of the Cisco CSS and Cisco ACE models to ensure that they are supported with your current IM and Presence Service deployment.

IM and Presence Service node updates

When using a load balancer for redundancy, you must update settings on the IM and Presence Service publisher and subscriber nodes.
### Task | Procedure
--- | ---
Update the federation routing parameter | Sign into Cisco Unified IM and Presence Administration, choose **System > Service Parameters > Cisco SIP Proxy** from the Service menu and enter these values:
- **Virtual IP Address** - enter the virtual IP address set on the load balancer.
- **Server Name** - set to the FQDN of the load balancer.
- **Federation Routing IM and Presence FQDN** - set to the FQDN of the load balancer.

Create a new TLS peer subject | 1. Sign in to Cisco Unified IM and Presence Administration, choose **System > Security > TLS Peer Subjects**
2. Click **Add New** and enter values:
   - **Peer Subject Name** - enter the external FQDN of the load balancer
   - **Description** - enter the name of the load balancer

Add the TLS peer to the TLS peer subject's list | 1. Sign in to Cisco Unified IM and Presence Administration, choose **System > Security > TLS Context Configuration**.
2. Click **Find**.
3. Click **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.
4. Move the load balancer federation-TLS peer subject for the load balancer to the TLS peer subject's list.

---

### Cisco Adaptive Security Appliance Updates

When using a load balancer, the external domains still send messages to the public IM and Presence Service address, but the Cisco Adaptive Security Appliance maps that address to a virtual IP address on the load balancer. Thus, when the Cisco Adaptive Security Appliance receives messages from the external domain, it forwards it to the load balancer. The load balancer then passes it on to the appropriate IM and Presence Service nodes.

To support this configuration, you must make some changes to the Cisco Adaptive Security Appliance:
- **Static PAT Message Updates**, on page 63
- **Access List Updates**, on page 64
- **TLS Proxy Instance Updates**, on page 66
Static PAT Message Updates

You must update the static PAT messages to include the load balancer details.

**Procedure**

<table>
<thead>
<tr>
<th>Task</th>
<th>Cisco Adaptive Security Appliance Release 8.2 Command</th>
<th>Cisco Adaptive Security Appliance Release 8.3 Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes required for the IM and Presence Service Publisher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change the static PAT to use an arbitrary, unused port for the public IM and Presence Service address.</td>
<td>Change: static (inside,outside) tcp public_imp_ip_address 5061 routing_imp_private_ip_address 5062 netmask 255.255.255.255 to: static (inside,outside) tcp public_imp_ip_address 55061 routing_imp_private_ip_address 5062 netmask 255.255.255.255</td>
<td>Change: object service obj_tcp_source_eq_5061 # service tcp source eq 5061 nat (inside,outside) source static obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061 to: object service obj_tcp_source_eq_55061 # service tcp source eq 55061 nat (inside,outside) source static obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061</td>
</tr>
<tr>
<td>Add a new static PAT to allow messages sent to the public IM and Presence Service address to be forwarded to the virtual port address (on whichever port the load balancer is listening for TLS messages).</td>
<td>static (inside,outside) tcp public_imp_address 5061 load_balancer_vip 5062 netmask 255.255.255.255</td>
<td>object network obj_host_load_balancer_vip # host routing_imp_private_address object service obj_tcp_source_eq_5061 # service tcp source eq 5061 nat (inside,outside) source static obj_host_load_balancer_vip obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061</td>
</tr>
</tbody>
</table>

Changes Required for IM and Presence Service Subscriber
Add a new access list for the load balancer virtual IP address. You must add an access list for each external domain that IM and Presence Service needs to access.

Add a new access list for a extended permit tcp hoseexternal domain to initiate messages to a IM and Presence Service server when the load balancer virtual IP address is in place. You must add an access list for each external domain that needs to access IM and Presence Service.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cisco Adaptive Security Appliance Release 8.2 Command</th>
<th>Cisco Adaptive Security Appliance Release 8.3 Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new access list for the load balancer virtual IP address.</td>
<td><code>access-list ent_lber_to_external_ocs extended permit tcp host subscriber_private_ip_address host external_domain_public_ip_address 5061</code></td>
<td><code>access-list ent_lber_to_external_ocs extended permit tcp host subscriber_private_ip_address host external_domain_public_ip_address 5061</code></td>
</tr>
<tr>
<td>You must add an access list for each external domain that IM and Presence Service needs to access.</td>
<td><code>access-list ent_lcs_to_lber_routg_imp extended permit tcp host external_domain_public_ip_address host imp_public_ip_address 65061</code></td>
<td><code>access-list ent_lcs_to_lber_routg_imp extended permit tcp host external_domain_public_ip_address host imp_public_ip_address 65061</code></td>
</tr>
</tbody>
</table>

**Access List Updates**

To support the load balancer, you also need to update the access lists on the Cisco Adaptive Security Appliance specific to your deployment scenario.

**Note**

The IM and Presence Service public IP address refers to the public IP address of the IM and Presence Service domain as configured on the Cisco Adaptive Security Appliance, and as it appears in the DNS record. This record shows the FQDN of the load balancer containing the public IP of the Cisco Adaptive Security Appliance.

**Procedures**

Deployment Scenario: An IM and Presence Service node federating with one or more external domains.

<table>
<thead>
<tr>
<th>Task</th>
<th>Configuration Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new access list for the new load balancer virtual IP address. You must add an access list for each external domain that IM and Presence Service needs to access.</td>
<td>Publisher: Cisco Adaptive Security Appliance Release 8.2 and 8.3 Command: <code>access-list ent_lber_to_external_ocs extended permit tcp host virtual_IP_address host external_domain_public_ip_address eq 5061</code></td>
</tr>
<tr>
<td>Task</td>
<td>Configuration Example</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add a new access list for an external domain to initiate messages to</td>
<td>Publisher:</td>
</tr>
<tr>
<td>a IM and Presence Service node when the load balancer virtual IP</td>
<td>Cisco Adaptive Security Appliance Release 8.2 Command:</td>
</tr>
<tr>
<td>address is in place. You must add an access list for each external</td>
<td>access-list ent_lcs_to_lber_routgimp extended permit tcp host</td>
</tr>
<tr>
<td>domain that needs to access IM and Presence Service.</td>
<td>external_domain_public_ip_address host</td>
</tr>
<tr>
<td></td>
<td>imp_public_ip_address eq 5062</td>
</tr>
<tr>
<td></td>
<td>Cisco Adaptive Security Appliance Release 8.3 Command:</td>
</tr>
<tr>
<td></td>
<td>access-list ent_external_server_to_lb extended permit tcp host</td>
</tr>
<tr>
<td></td>
<td>external_public_address host</td>
</tr>
<tr>
<td></td>
<td>loadbalancer_virtual_ip_address eq 5062</td>
</tr>
<tr>
<td>For each access list, add a new class to incorporate the new access</td>
<td><strong>class</strong> ent_lber_to_external_ocs match access-list</td>
</tr>
<tr>
<td>list.</td>
<td>ent_lber_to_external_ocs</td>
</tr>
<tr>
<td></td>
<td><strong>policy-map</strong> global_policy class ent_lber_to_external_ocs</td>
</tr>
<tr>
<td></td>
<td>inspect sip sip_inspect tls-proxy ent_imp_to_external</td>
</tr>
<tr>
<td></td>
<td><strong>policy-map</strong> global_policy class ent_lcs_to_lber_routgimp</td>
</tr>
<tr>
<td></td>
<td>inspect sip sip_inspect tls-proxy ent_external_to_imp</td>
</tr>
</tbody>
</table>

Deployment Scenario: IM and Presence Service to IM and Presence Service Federation, where the external domain has added one or more intercluster IM and Presence Service nodes.

<table>
<thead>
<tr>
<th>Task</th>
<th>Configuration Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>The external domain Adaptive Security Appliance must allow access to</td>
<td>access-list ent_imp_to_externalPubimpwlber extended permit tcp host</td>
</tr>
<tr>
<td>the arbitrary ports that were selected for our local domain</td>
<td>external_domain_private_imp_address host</td>
</tr>
<tr>
<td>publisher and subscriber.</td>
<td>public_imp_address_local_domain 55061</td>
</tr>
<tr>
<td></td>
<td>access-list ent_imp_to_externalSubimpwlber extended permit tcp host</td>
</tr>
<tr>
<td></td>
<td>external_domain_private_imp_address host</td>
</tr>
<tr>
<td></td>
<td>public_imp_address_local_domain 65061</td>
</tr>
<tr>
<td>For each access list, add a new class to incorporate the new access</td>
<td></td>
</tr>
<tr>
<td>list.</td>
<td></td>
</tr>
<tr>
<td>For each class, make an entry in the policy-map global_policy.</td>
<td></td>
</tr>
</tbody>
</table>
TLS Proxy Instance Updates

Update the TLS proxy instances on the Cisco Adaptive Security Appliance.

Procedure

Change:

```
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point imp_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
to:
```

```
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
tls-proxy ent_imp_to_external
server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

CA-Signed Security Certificate Update

When adding the load balancer to the configuration, you must also generate CA-signed security certificates between the load balancer, the Cisco Adaptive Security Appliance, and the IM and Presence Service node as described in these sections:

- Security Certificate Configuration Between the Load Balancer and Cisco Adaptive Security Appliance
- Security Certificate Configuration Between the Load Balancer and IM and Presence Service Node

Security Certificate Configuration Between the Load Balancer and Cisco Adaptive Security Appliance

This topic provides an overview of the required steps for configuring the security certificate between the load balancer and the Cisco Adaptive Security Appliance.
<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate CA-signed certificate for the load balancer on the Cisco Adaptive Security Appliance.</td>
<td>Use the <code>crypto ca enroll</code> command and specify the FQDN of the load balancer.</td>
</tr>
<tr>
<td>Import the CA-signed certificate from the Cisco Adaptive Security Appliance to the load balancer.</td>
<td>Refer to your load balancer documentation.</td>
</tr>
<tr>
<td>Generate a CA-signed certificate for the Cisco Adaptive Security Appliance on the load balancer.</td>
<td>Refer to your load balancer documentation.</td>
</tr>
<tr>
<td>Import the CA-signed certificate from the load balancer to the Cisco Adaptive Security Appliance</td>
<td>Use the <code>crypto ca trustpoint</code> command.</td>
</tr>
<tr>
<td></td>
<td>To verify that the certificate was imported, use the <code>show crypto ca certificate</code> command.</td>
</tr>
</tbody>
</table>

**Security Certificate Configuration Between the Load Balancer and IM and Presence Service Node**

This topic provides an overview of the required steps for configuring the security certificate between the load balancer and the IM and Presence Service nodes.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a CA-signed certificate on both the publisher and subscriber nodes.</td>
<td>Follow the instructions to exchange certificates using CA-signed certificates.</td>
</tr>
<tr>
<td>Import the CA-signed certificates (from the publisher and subscriber nodes) to the load balancer</td>
<td>Refer to your load balancer documentation.</td>
</tr>
</tbody>
</table>

**Microsoft Component Updates**

Update the following Microsoft components with the load balancer details.

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update all instances of the FQDN to correspond to the load balancer FQDN</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Procedure</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Update the domain name in the IM Provider list with the load balancer. | 1 On the external Access Edge server, choose **Start > Administrative Tools > Computer Management.**  
2 In the left pane, right-click **Microsoft Office Communications Server 2007.**  
3 Click the **IM Provider** tab.  
4 Click **Add.**  
5 Check the check box for **Allow the IM service provider.**  

Define the network address of the IM service provider as the public FQDN of the load balancer. |
Troubleshooting

- IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser, page 69
- Lync Error When Using E.164 Numbers, page 70
- Synchronize User to Cisco Unified Communications Manager, page 70
- Enable IM and Presence for User ID, page 71
- Verify User Phone Call Control at the Lync Client Is Enabled, page 71
- Phone Icon with a Red X in the Status Bar in Microsoft Lync Client, page 72

IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser.

**Problem** When the Microsoft Lync client user accesses the IM and Presence Service menu item, the default web browser cannot connect to the IM and Presence Service node and the IM and Presence Service web page does not open.

**Solution** When the Microsoft Lync client user accesses the IM and Presence Service menu item, IM and Presence Service should open a web page in the user's default web browser. If the web browser cannot connect to the IM and Presence Service node, check the following:

1. Ensure that JavaScript is enabled in the browser settings.
2. Enter the following address in a web browser to verify that the browser can connect to the IM and Presence Service node: https://imp_server_address:8443/cucmuser/showHomeMini.do?mini=true
   Where `imp_server_address` is the hostname, FQDN, or IP address of the IM and Presence Service node.
3. If you 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.
4. If you experience other connection problems, you may need to do the following:
• Add the web address of the IM and Presence Service node to the list of trusted web addresses in the browser on the Microsoft Lync client computer. In Microsoft Explorer, select Internet Options > Security > Trusted Sites and add the following entry to the list of trusted web addresses:

https://<IM and Presence_server_name>

• Add the HTTPS web address of your domain to the security zone of the IM and Presence Service node. In Microsoft Explorer, select Microsoft Internet Explorer > Internet Options > Security > Local Internet > Sites > Advanced and add the following entry to the list of web addresses for the security zone: https://*.<your_domain>

5 If an error message appears informing the users that they do not have permission to use this feature, you must enable the users for Microsoft Lync in the IM and Presence Service node. See Remote Call Control Setup, on page 17.

6 If an error message appears regarding an un-trusted security certificate issue or similar warning, select Continue. Most browsers allow you to download a website security certificate and mark it as trusted.

Lync Error When Using E.164 Numbers

Solution When you add the tel: value in the Line URI field shown in Enable Users in Lync Server Control Panel, on page 23, do not add phone-context=dialstring if you are using E.164 numbers. For example, the Line URI field must be configured as "tel:+19728131000" and not "tel:+19728131000;phone-context=dialstring."

If phone-context=dialstring is added, the Lync client will produce an error and will not send out the initial INVITE to the Lync server to begin the sign-in sequence.

Synchronize User to Cisco Unified Communications Manager

If the user is provisioned in AD but does not appear in Cisco Unified Communications Manager, perform the following procedure to synchronize the user to Cisco Unified Communications Manager.

Procedure

| Step 1 | Select Cisco Unified Communications Manager Administration > System > LDAP > LDAP Directory (select the LDAP Configuration Name that matches AD). |
| Step 2 | Verify that the configuration is correct. |
| Step 3 | Select Perform Full Sync Now and select OK when prompted. |
| Step 4 | Select Cisco Unified Communications Manager Administration > User Management > End User. The user should now display in the user list. |
Enable IM and Presence for User ID

If the user is configured in Cisco Unified Communications Manager but does not appear in IM and Presence Service, perform the following procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; End User.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Search for the user.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the user.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Enable User for Unified CM IM and Presence check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

Verify User Phone Call Control at the Lync Client Is Enabled

If the user has no call control at the Lync client, the user must complete the following procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign in to the Lync client.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the drop-down arrow on the top right of the window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Tools &gt; Options &gt; Phones.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Phone Integration area, select the option Enable integration with your phone system.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Advanced.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Verify that the Automatic Configuration option is selected. This option allows the client to access the correct information from the Lync server database.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select OK. If the problem persists, ensure that the user is synchronized from Cisco Unified Communications Manager and that the user is enabled for RCC in the IM and Presence Service node.</td>
</tr>
</tbody>
</table>

Related Topics

Assign User Capabilities, on page 18
Phone Icon with a Red X in the Status Bar in Microsoft Lync Client

**Solution** The integration configuration is successful if a user signs into Microsoft Lync client and sees the text “Call forwarding is on” or “Call forwarding is off” in the status bar at the bottom of the window. If there is a phone icon with a red X in the status bar, the integration is unsuccessful. To resolve sign-in problems, you can initiate a trace of the Lync server to identify any problems with the INVITE/INFO SIP message exchange sequence between the IM and Presence server and the Microsoft Lync server. See the Microsoft Lync documentation for more information about Microsoft Lync server logging and Microsoft Lync client logging.

**Related Topics**

Get More Information, on page 1