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 of 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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: 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. (1721R)

© 2019 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 7

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 11
   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 17
   Remote Call Control Setup 17
   Set Up IM and Presence Service CTI Connection 17
Assign User Capabilities 18
Run Microsoft RCC Troubleshooter 19

CHAPTER 5
Microsoft Component Integration Setup for IM and Presence Service 21
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 30

CHAPTER 6
Normalization Rules Setup 31
  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 35
  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 37
  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 43
  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
Lync 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 56

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 59

CHAPTER 11
Troubleshooting 61
  IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser 61
  Lync Error When Using E.164 Numbers 62
  Synchronize User to Cisco Unified Communications Manager 62
  Enable IM and Presence for User ID 62
  Verify User Phone Call Control at the Lync Client Is Enabled 63
  Phone Icon with a Red X in the Status Bar in Microsoft Lync Client 63
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, on page 1
- About Remote Call Control, on page 2
- Integration Overview, on page 2
- Line Appearances, on 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:

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.

Note

An IM and Presence Service cluster that is used for RCC does not support Jabber or other IM and Presence Service functionality.

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.
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.
CHAPTER 2

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 Microsft 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.

Note

• Software Requirements, on page 5
• Preconfiguration Checklist, on page 6
• Integration License Requirements, on page 7

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
• Microsoft Lync Server 2010 or 2013 Release 4.x, Standard Edition or Enterprise Edition
  • Lync Server Control Panel
  • Lync Server Deployment Wizard
  • Lync Server Logging Tool
  • Lync Server Management Shell
  • Lync Server Topology Builder
• Microsoft 2010 Lync Client, or, Microsoft 2013 Lync Client
• (Optional) Upgraded Skype for Business 2015 Client
The Skype for Business 2015 client must have been upgraded from a Lync 2013 client and must be registered to a Lync 2013 server.

• (Optional) Cisco CSS 11500 Content Services Switch
• Microsoft Domain Controller
• Microsoft Active Directory
• DNS
• Certificate Authority

Preconfiguration Checklist

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

• An IM and Presence Service node that is set up and configured as described in Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager. The IM and Presence Service node must be correctly deployed with a Cisco Unified Communications Manager (Unified Communications Manager) server as described in Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

• A Microsoft Lync Server that is set up and configured according to the requirements defined in the Microsoft documentation.

• A Microsoft Lync Client or an upgraded Skype for Business 2015 Client that is set up according to the requirements defined in the Microsoft documentation.

Note: If you are using Skype for Business clients, the client must have been upgraded from a Lync 2013 client, and must be registered to a Lync 2013 server.

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
CHAPTER 3

Cisco Unified Communications Manager Server Setup

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, on page 9
- Add Users to a Standard CCM Access Control Group, on page 10
- Set Up CTI Gateway Application User, on page 10
- Add Application User to CTI-Enabled Access Control Group, on page 11
- Assign CTI Device Control to Application User, on page 11
- Set Up Dial Rules, on 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; Phone</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>
<tr>
<td>Associate a user with a line appearance</td>
<td>Cisco Unified Communications Manager Administration &gt; Device &gt; Phone</td>
</tr>
</tbody>
</table>
Add Users to a Standard CCM Access Control Group

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

Procedure

Step 1 Select Cisco Unified Communications Manager Administration > User Management > User Settings > Access Control Group.
Step 2 Select Find.
Step 3 Select Standard CCM End Users.
Step 4 Select Add End Users to Group.
Step 5 Select the end user to add to the Standard CCM access control group.
Step 6 Select Add Selected.
Step 7 Select Save.

Set Up CTI Gateway Application User

Complete the following procedure to configure an application user for the CTI Gateway.

Procedure

Step 1 Select Cisco Unified Communications Manager Administration > User Management > Application User.
Step 2 Select Add New.
Step 3 Enter an application user name in the User ID field.
Example:
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**

1. Select Cisco Unified Communications Manager Administration > User Management > User Settings > Access Control Group.
2. Select Find.
4. Select Add App Users to Group.
5. Select the application user that you created for the CTI Gateway.
6. Select Add Selected.
7. Select Save.

**What to do next**
Assign CTI Device Control to Application User, on page 11

**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 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) For IM and Presence to process any incoming SIP request with SIP URI containing a domain name different from the one configured for IMP Service domain, set the SRV Cluster Name parameter to the same enterprise top-level domain.
   c) Enable the Add Record-Route Header parameter.
   d) Enable the Use Transport in Record-Route Header parameter.
   e) 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.
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**

**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 17
Set Up Routing Settings

Complete the following procedure to configure the routing settings.

Procedure

Step 1  Select Cisco Unified CM IM and Presence Administration > Presence > Routing > Settings.
Step 2  Select On for Method/Event Routing Status.
Step 3  Select Default Cisco SIP Proxy TCP Listener for the Preferred Proxy Server.
Step 4  Select Save.

What to do next

Remote Call Control Setup, on page 17

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.
Assign User Capabilities

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

**Procedure**

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

**Step 2** Select Find.

**Step 3** Check the users to whom you want to assign remote call control capabilities.

**Step 4** Select Assign Selected Users.

**Step 5** Check Enable Microsoft RCC in the Microsoft RCC Assignment window.

**Step 6** Select Save.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <code>Cisco Unified CM IM and Presence Administration &gt; Diagnostics &gt; Microsoft RCC Troubleshooter</code>.</td>
</tr>
<tr>
<td>2</td>
<td>Enter a valid user ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Select Search to find the ID for a user.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the Microsoft Lync server address.</td>
</tr>
<tr>
<td>4</td>
<td>Select <code>Submit</code>.</td>
</tr>
</tbody>
</table>

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, on page 21
- IM and Presence Service User Authentication, on page 22
- Set Up Microsoft Active Directory, on page 23
- Enable Users in Lync Server Control Panel, on page 23
- Microsoft Lync Server Setup Overview, on 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:
  \[ tel:xxxx;phone-context=dialstring \]
  - 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 62.

- 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.

**Note**
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'.

Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager, Release 11.5(1)
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 user name and the telephone number that are associated with each particular user.

Step 2
For each of the users that you added, open the Properties window on Microsoft Active Directory and configure the following parameters:

a) Enable the user for the 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 StartAll 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:

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 @(Add=$tcpRoute)

**Step 5** Verify the new system configuration by entering the Get command from Step 2, on page 25 again.

*Note* 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, -MatchUri &quot;my-cups.my-domain.com&quot;</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. The value of this parameter must be written in double quotes, for example, <code>-Identity &quot;10.0.0.1&quot;</code> 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. Tip You can find the site ID with the <code>Get-CsSite</code> Management Shell command.</td>
</tr>
<tr>
<td>-TreatAsAuthenticated</td>
<td>Always set this value to <code>$True</code></td>
</tr>
<tr>
<td>-ThrottleAsServer</td>
<td>Always set this value to <code>$True</code></td>
</tr>
<tr>
<td>-RequiresReplication</td>
<td>Because authentication is not required for TCP, you must set this value to <code>$False</code></td>
</tr>
</tbody>
</table>
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>
<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.</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 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>
</tbody>
</table>
**Parameter** | **Description**
---|---
-EnableTCP | This parameter sets the transport to TCP. If this parameter is not included, the transport will default to TLS.

**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**

1. In the Lync Server Management Shell enter the following command to verify the current system configuration:
   ```bash
   Get-CSRegistrarConfiguration
   ```

2. Enter the following command to set the Lync server listening port:
   ```bash
   Set-CsRegistrar registrar:<Lync_server_FQDN> -SipServerTcpPort 5060
   ```

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:
   ```bash
   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><strong>Parameter</strong></th>
<th><strong>Description</strong></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 30

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 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, on page 31
- Update Microsoft Lync Address Book, on 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:
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 \
\1\d(10)\EXT\d(5)\+1\$1;ext=$2. 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:

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

```shell
# +1 (ddd) ddd-ddd EXTddd
#
+1\d(10)\EXT\d(5)
+1$1;ext=$2
#
# +1 (ddd) ddd-ddd Xddd
#
+1\d(10)\[Xx]\d(5)
+1$1;ext=$2
#
# 1 (ddd) ddd-ddd
#
1\d(10)
+1$1
#
# +1 (ddd) 70ddd
#
+1\d(3)\70\d(5)
+1$170$2;ext=$2
#
# 70d-ddd Xddd
#
70\d(5)\[Xx]\d(1)\d(5)
```
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:

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

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

Set Up Standalone Root Certificate Authority (CA)

Complete the following procedure to configure the standalone root CA.

Procedure

Step 1  Sign in to the CA server with Domain Administrator privileges.
Step 2  Insert the Windows Server 2003 CD.
Step 3  Select Start > Settings > Control Panel 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).
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.

What to do next
Upload Root Certificate to IM and Presence Service, on page 37
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

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 37

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Cisco Unified Operating System Administration &gt; Security &gt; Certificate Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Generate CSR.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select cup from the Certificate Name menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Generate CSR.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Cisco Unified Operating System Administration &gt; Security &gt; Certificate Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Download CSR.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select cup from the Certificate Name menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Download CSR.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Save to save the cup.csr file to your local computer.</td>
</tr>
</tbody>
</table>

What to do next
Submit Certificate Signing Request on CA Server, on page 39

Related Topics
Generate Certificate Signing Request for IM and Presence Service, on page 37
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 TasksIssue.
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
Upload Signed Certificate to IM and Presence Service
CHAPTER 8

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

Security Certificate for Microsoft Lync Setup

Download CA Certification Chain

Complete the following procedure to download the CA certification chain.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Start &gt; Run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter http://&lt;name of your Issuing CA Server&gt;/certsrv and select OK.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From Select a task, select Download a CA certificate, certificate chain, or CRL.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Download CA certificate chain.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Save in the File Download dialog box.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Save the file on a hard disk drive on your server.</td>
</tr>
</tbody>
</table>
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**

1. Select Start > Run.
2. Enter mmc and select OK.
4. Select Add in the Add/Remove Snap-in dialog box.
5. Select Certificates in the list of Available Standalone Snap-ins and select Add.
6. Select Computer account and select Next.
7. In the Select Computer dialog box, ensure Local computer: (the computer this console is running on) is selected.
8. Select Finish, select Close, and then select OK.
9. Expand Certificates (Local Computer) in the left pane of the Certificates console.
10. Expand Trusted Root Certification Authorities and right-click Certificates.
11. Point to All Tasks and select Import.
13. Select Browse and locate the certificate chain on your computer.
14. Select Open and select Next.
15. Leave the default value Place all certificates in the following store selected.
16. Ensure Trusted Root Certification Authorities appears under the Certificate store.
17. Select Next and select Finish.
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.
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.
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
NotBefore : 6/16/2011 2:08:20 PM
SerialNumber : 152E466D00000000000C
Subject : CN=pool1.rcdnlync.com
AlternativeNames : {sip.rcdnlync.com, ne011a-lyncent.rcdnlync.com, pool1.rcdnlync.com}
Thumbprint : 84BED88F2BFBB463CB4CBC328DA6FD3A5E0677B
Use : Default

What to do next

TLS Route for Microsoft Lync Setup, on page 48
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:

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

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

```powershell
$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.

```powershell
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

**Step 5** Verify the new system configuration by entering the following command:

```powershell
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>
</tbody>
</table>
### Parameter | Description
--- | ---
-Port | The port to which the IM and Presence Service node listens. For TLS, the port is 5062.
-MatchUri | 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.
-UseDefaultCertificate | This value is set to True to instruct the static route to use the default certificate.
-CsStaticRoutingConfiguration | The internal command to move parameter values to the routing database.
-Route | This parameter takes the parameters in the variable and adds the static route.

---

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Start &gt; All Programs &gt; Microsoft Lync Server &gt; Lync Server Management Shell.</strong></td>
</tr>
</tbody>
</table>
| **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 6: Application pool parameters

<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>-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>

**Tip** You can find the site ID with the Get-CsSite Management Shell command.

---

### 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>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------</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 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

Set Up Microsoft Lync for TLSv1, on page 52
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.

**What to do next**

Create New TLS Peer Subject for Microsoft Lync, on page 52

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.

**What to do next**

Add TLS Peer to TLS Peer Subjects List, on page 53
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 Administration > System > Security > TLS Context Configuration.

**Step 2** Select Find.

**Step 3** Select Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context.
   The TLS Context Configuration window displays.

**Step 4** From the list of available TLS ciphers, select TLS_RSA_WITH_3DES_EDE_CBC_SHA.

**Step 5** Select the right arrow to move this cipher to Selected TLS Ciphers.

**Step 6** Check Disable Empty TLS Fragments.

**Step 7** From the list of available TLS peer subjects, select the TLS peer subject that you configured.

**Step 8** Select the right arrow to move it to Selected TLS Peer Subjects.

**Step 9** Select Save.

**What to do next**
Lync Remote Call Control Installation, on page 55
Add TLS Peer to TLS Peer Subjects List
Lync Remote Call Control Installation

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

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 an 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 addrcmmenu.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 addrcmmenu.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:

```
addrcmmenu.bat $impserveraddress$
```
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open a supported Web browser on your computer.</td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter your username for Cisco Unified Communications Manager IM and Presence Service User Options.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter your password Cisco Unified Communications Manager IM and Presence Service User Options provided by your system administrator.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
</tr>
</tbody>
</table>
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, on page 59
- Enable and View Microsoft Lync Client Logs, on page 59

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 being 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.
Troubleshooting

• IM and Presence Service Web Page Does Not Open from the Microsoft Lync Client Default Web Browser., on page 61
• Lync Error When Using E.164 Numbers, on page 62
• Synchronize User to Cisco Unified Communications Manager, on page 62
• Enable IM and Presence for User ID, on page 62
• Verify User Phone Call Control at the Lync Client Is Enabled, on page 63
• Phone Icon with a Red X in the Status Bar in Microsoft Lync Client, on page 63

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select Cisco Unified Communications Manager Administration &gt; System &gt; LDAP &gt; LDAP Directory (select the LDAP Configuration Name that matches AD).</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Verify that the configuration is correct.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select Perform Full Sync Now and select OK when prompted.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select Cisco Unified Communications Manager Administration &gt; User Management &gt; End User.</td>
</tr>
</tbody>
</table>

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

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

**Step 2** Search for the user.

**Step 3** Select the user.

**Step 4** Check the *Enable User for Unified CM IM and Presence* check box.

**Step 5** Select *Save.*

---

**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

**Step 1** Sign in to the Lync client.

**Step 2** Click the drop-down arrow on the top right of the window.

**Step 3** Select *Tools > Options > Phones.*

**Step 4** In the *Phone Integration* area, select the option *Enable integration with your phone system.*

**Step 5** Select *Advanced.*

**Step 6** Verify that the Automatic Configuration option is selected.

This option allows the client to access the correct information from the Lync server database.

**Step 7** 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.

---

**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