Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager, Release 9.1(1)

First Published: November 06, 2013

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-30956-01

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 **Integration Overview** 1

- Partitioned Intradomain Federation 1
  - Partitioned Federation Deployment Overview 2
  - Single Domain Example 3
- Partitioned Intradomain Federation Configuration 4
- Availability 7
  - Availability Subscriptions and Policy 7
    - Subscription to an IM and Presence Service User 7
    - Subscription to Microsoft Lync or Microsoft Office Communicator User 7
  - Availability Mapping States 8
- Instant Messaging 10
- Request Routing 11
  - IM and Presence to Microsoft Server Request Routing 11
    - Basic Routing Mode for Partitioned Intradomain Federation 11
    - Advanced Routing Mode for Partitioned Intradomain Federation 13
  - Microsoft Server to IM and Presence Service Request Routing 13
- Intercluster and Multinode Deployments 14
- Interdomain Federation 15
- High Availability for Intradomain Federation 15
  - High Availability for IM and Presence Service to Microsoft Server Request Routing 15
  - High Availability for Microsoft Server to IM and Presence Service Request Routing 17
- Contact Search 18
- User Migration 19
  - User Migration Tools 19

CHAPTER 2 **Planning for Integration** 21

- Supported Partitioned Intradomain Federation Integrations 21
  - Presence Web Service API Support 22

Limitations for Microsoft Lync Integrations 22
Hardware Requirements 22
Software Requirements 23
Server Software 23
Client Software 24
IM and Presence Service Supported Clients 24
Microsoft Server Supported Clients 24
Integration Preparation 25
Presence Domains 25
User Migration 25
Detailed User Migration Plan 26
HCS-7825-H4 Hardware 27
HCS-7845-H2 Hardware 27
Maintenance of User Identity During Migration 28
Duration Guidelines for User Migration Tools 29
Export Contact List Tool 29
Disable Account Tool 29
Delete Account Tool 30
Bulk Administration Tool Contact List Import 30
DNS Configuration 31
Certificate Authority Server 31
High Availability 31
Prerequisite Configuration for IM and Presence Service 32
Additional Configuration for Routing IM and Presence Service Node 32
Start IM and Presence Service Feature Services 33
Plan Services Restarts during Off-Peak Periods 33

CHAPTER 3 **Configuration Workflows for Partitioned Intradomain Federation 35**
Configuration Workflow for Partitioned Intradomain Federation with Lync 35
Configuration Workflow for Partitioned Intradomain Federation with OCS 37
Configuration Workflow for Partitioned Intradomain Federation with LCS 38
Configuration Workflow for User Migration from Microsoft Servers to the IM and Presence Service 39
Configuration Workflow for Integrating IM and Presence with Microsoft Server Interdomain Federation Capability 40

CHAPTER 4 IM and Presence Service Node Configuration for Partitioned Intradomain Federation 41

Configure Partitioned Intradomain Federation Options 41

Configure Static Routes 42

Configure an Incoming Access Control List 44

TLS Encryption Configuration 45

Configure Application Listener Ports 45

Configure TLS Peer Subjects 46

Configure Peer Authentication TLS Context 48

Import Root Certificate of Certificate Authority 48

Generate Certificate Signing Request for IM and Presence Service 49

Import Signed Certificate from Certificate Authority 50

Deactivate Feature Services on the Routing IM and Presence Service Node 51

CHAPTER 5 Microsoft Lync Configuration for Partitioned Intradomain Federation 53

Domain Verification for Lync Servers 54

Federated Link to Microsoft Lync Server Configuration Task Lists 54

Configure a Static Route on Microsoft Lync for Federation 56

Add Host Authorization for IM and Presence Service on an Enterprise Edition Lync Server 58

Add Host Authorization for IM and Presence Service on Standard Edition Lync Servers 60

Publish Topology 62

Install Certificate Authority Root Certificates on Lync 63

Validate Existing Lync Signed Certificate 64

Request a Signed Certificate from a Certificate Authority for Lync 65

Download a Certificate from the CA Server 66

Import a Signed Certificate for Lync 67

Assign Certificate on Lync 68

Restart Services on Lync Servers 68

CHAPTER 6 Microsoft Office Communications Server Configuration for Partitioned Intradomain Federation 69

Domain Verification for OCS Servers 69

Enable Port 5060/5061 on OCS Server 69

Federated Link to Microsoft OCS Server Configuration Task List 70

Configure Static Routes on OCS to Point to the IM and Presence Service 72

Add Host Authorization on OCS for IM and Presence Service 73
Restart Services on OCS Front-End Servers 74
TLS Encryption Configuration 75
Enable Federal Information Processing Standard Compliance on OCS 75
Configure Mutual TLS Authentication on OCS 76
Install Certificate Authority Root Certificates on OCS 76
Validate Existing OCS Signed Certificate 78
Signed Certificate Request from the Certificate Authority for the OCS Server 79
Install Signed Certificate on the OCS Server 80
Select Installed Certificate for TLS Negotiation 81

CHAPTER 7 Configuration of Microsoft Live Communications Server for Partitioned Intradomain Federation 83
Domain Verification for LCS Servers 83
Enable Port 5060 on LCS Server 83
Configure a LCS Static Route to Point to the IM and Presence Service 84
Add Host Authorization on LCS for IM and Presence Service 85
Restart Services on LCS Servers 86
TLS Encryption Configuration for Microsoft LCS Servers 87
Enable Federal Information Processing Standard Compliance on LCS 87
Configure Mutual TLS Authentication on LCS 88
Install Certificate Authority Root Certificates on LCS 88
Validate Existing LCS Signed Certificate 90
Signed Certificate Requests from Certificate Authority for LCS Server 91
Install Signed Certificate on LCS Server 92
Select Installed Certificate for TLS Negotiation 93

CHAPTER 8 User Migration 95
Cisco User Migration Tools 95
Recommendations before Migration 96
Set Unlimited Contact Lists and Watchers 96
Enable Automatic Authorization of Subscription Requests 97
Subscriber Notification Pop-ups 98
Disable Microsoft Lync Pop-ups 98
Restore Microsoft Lync Pop-up Behavior 98

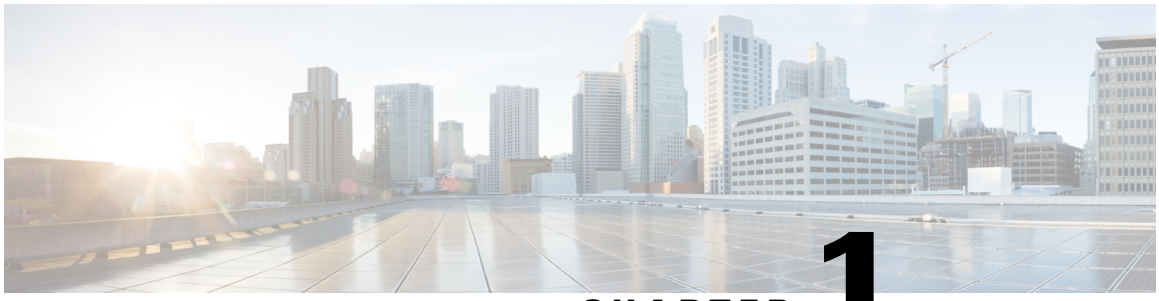
Provision of Microsoft Server Users on Cisco Unified Communications Manager 99
Backups of User Microsoft Server Contact List Information 99
Export of Contact Lists for Migrating Users 100
Log File 100
Run Modes 101
Input File Formats 101
Disable Users on Microsoft Servers 106
Disable Microsoft Server Account for Migrating Users 106
Verify That Active Directory Updates Synchronized to Microsoft Servers 107
Delete User Data from Database for Migrating Users 108
Import Contact Lists for Migrating Users into IM and Presence 110
CSV File Upload Using BAT 111
Creation of a New Bulk Administration Job 111
Results of Bulk Administration Job 111
Deploy an IM and Presence Service Supported Client on Users Desktop 112
Reset Maximum Contact List Size and Maximum Watcher Size 112

CHAPTER 9 **Interdomain Federation and Intradomain Federation Deployment Integration 115**
IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers 115
Interactions and Restrictions 116
IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers 116
Remote Domain Setup for Interdomain Federation through Intradomain Federation Connections on Microsoft Servers 116
Configure a Static Route for a Remote Domain 117
Remove IM and Presence Service Integration with Microsoft Server Interdomain Federation Capability 119
Remove Static Route for Remote Domain 119
Remove the SIP Federation Domain 119

CHAPTER 10 **Integration Troubleshooting 121**
IM and Presence Service Tracing 121
Configure Tracing on the IM and Presence Service 123
Microsoft Server SIP Tracing 124

Enable SIP Tracing on Lync 124
Enable SIP Tracing on OCS 124
Enable SIP Tracing on LCS 125
Common Integration Problems 125
Microsoft Server User Does Not Receive Pop-up when Added to IM and Presence Service Contact List 126
Microsoft Server User Receives a Pop-up when Added to an IM and Presence Service Contact List but Has No Availability after Accepting 127
IM and Presence Service User Does Not Receive a Pop-up when a Microsoft Lync or Microsoft Office Communicator User Adds the User to their Contact List 127
Microsoft Server User Does Not Receive IMs Sent by an IM and Presence Service User 128
IM and Presence User Does Not Receive IMs Sent by a Microsoft Server User 129
Microsoft Server User Updates and IMs Take up to 40 Seconds to Appear 130
When Advanced Routing Is Enabled, No Availability Is Exchanged Between IM and Presence Service and Microsoft Server 130
IM and Presence Service User Does Not Appear in the Microsoft Server Address Book 130
IM and Presence Service Unable to Route Interdomain Federation Requests through Microsoft Server Deployment 131
TLS Handshake Errors between the IM and Presence Service and Microsoft Servers 131
Incorrect SIP URI Specified for Microsoft Lync or Microsoft Office Communicator Users when Added to Cisco Unified Personal Communicator Contact List 132
Display Names not Shown for Microsoft Lync or Microsoft Office Communicator Contacts on Cisco Unified Personal Communicator 132
User Migration Troubleshooting 132
User Migration Tracing 132
Export Contact List Tool 132
Disable Account Tool 134
Delete Account Tool 135
IM and Presence Service BAT Contact List Import 137
Configure Bulk Provisioning Service Logging on the IM and Presence Service 137
Common User Migration Problems 138
Application Failed to Initialize Properly - Error Occurs When Running Any of the User Migration Tools 138
Export Contact List Tool does not Produce an Output File for Lync Users 138

Export Contact List Tool Log Shows getAndPrintContactsForUsers Error 138
Export Contact List Tool - Log Summary Shows Several Users as Not Found 139
Export Contact List Tool - Tool Does Not Show the Progress Bar and Does Not Produce an Output File of Exported Contacts when Run in Normal Mode 139
Disable Account Tool - Log Shows Unable to Connect to LDAP Using IP/FQDN/Hostname 139
Delete Account Tool - Unable to Find the Microsoft Server Database or Server Instance 140
Delete Account Tool - Log Shows Error While Connecting to the SQL Server 140
BAT Contact List Update - Uploaded Contact List File Not in Drop-Down List 140
BAT Contact List Update - No Log file Exists on Results Page after BAT Job 141
BAT Contact List Update - A User's Contacts Are Not Imported During BAT Job 141
BAT Contact List Update - A User's Contacts Are Partially Imported During BAT Job 141
BAT Contact List Update - No Contacts are Imported During BAT Job 141
Migrating User Status Appears as Status Unknown or Presence Unknown to Microsoft Server Users during the Migration Process 142



CHAPTER 1

Integration Overview

- Partitioned Intradomain Federation, page 1
- Partitioned Intradomain Federation Configuration, page 4
- Availability, page 7
- Instant Messaging, page 10
- Request Routing, page 11
- Intercluster and Multinode Deployments, page 14
- Interdomain Federation, page 15
- High Availability for Intradomain Federation, page 15
- Contact Search, page 18
- User Migration, page 19

Partitioned Intradomain Federation

More and more enterprises are choosing Cisco Unified Communications Manager IM and Presence Service as their IM and availability platform. These enterprises already have Microsoft Lync, Microsoft Office Communications Server (OCS) or Microsoft Live Communications Server (LCS) deployed and want to move their users over to an IM and Presence Service supported client.

During this transition, it is important that these users who migrate to an IM and Presence Service supported client can continue to share availability and instant messages with those users who are still using the Microsoft servers. For more information about supported IM and Presence Service clients, see the "Software Requirements" section.

Partitioned intradomain federation enables IM and Presence Service client users and Microsoft Lync or Microsoft Office Communicator users within the same enterprise domain to exchange presence Availability and IM.

This integration supports users within an enterprise domain who are either configured on the IM and Presence Service and use an IM and Presence Service supported client as their desktop client, or are enabled on OCS or LCS and use Microsoft Lync or Microsoft Office Communicator as their desktop client or are enabled on Lync, OCS or LCS and use Microsoft Lync or Microsoft Office Communicator as their desktop client.

Note Partitioned intradomain federation requires that a user is enabled on one system only. This integration does not support a user that is enabled on both IM and Presence Service and the Microsoft server at the same time.

IM and Presence Service uses the standard Session Initiation Protocol (SIP RFC 3261) to provide partitioned intradomain federation support for the following Microsoft server platforms:

- Microsoft Lync Server 2010, Standard Edition and Enterprise Edition
- Microsoft Office Communications Server 2007 R2 Standard Edition and Enterprise Edition
- Microsoft Live Communications Server 2005 Standard Edition and Enterprise Edition

Note The term Microsoft server is used in this document to refer to all supported Lync, OCS and LCS platform types. Any information that is specific to a certain platform is identified.

Related Topics

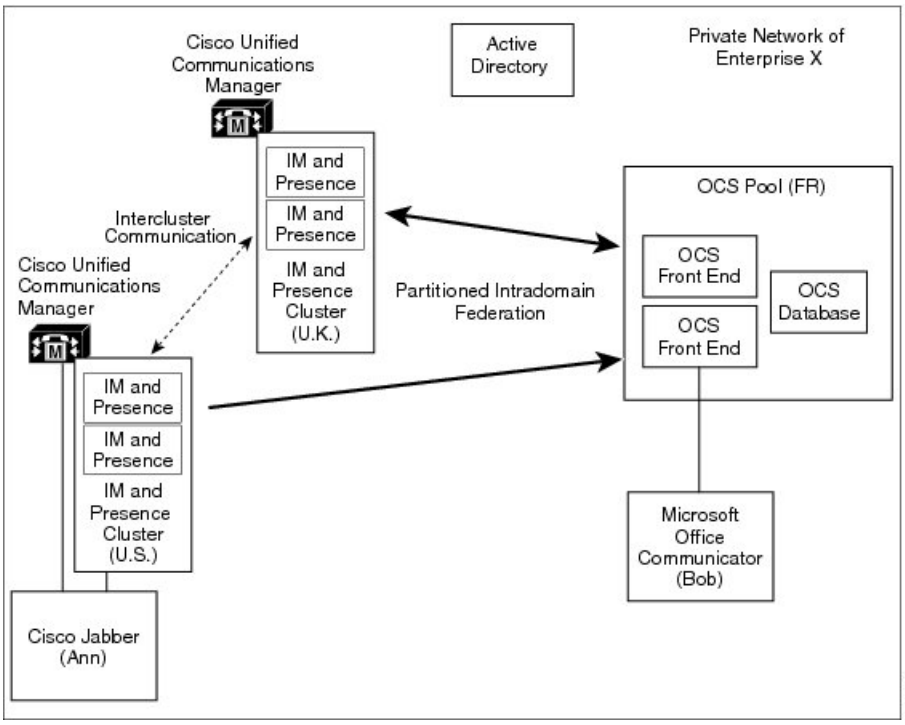
Software Requirements, on page 23

Partitioned Federation Deployment Overview

The following figure shows a high-level sample deployment of IM and Presence Service and Microsoft OCS within the same domain. This example shows an OCS deployment, but it also applies to the other supported Microsoft servers.

For Partitioned Intradomain Federation, you must configure the identical domain on the IM and Presence Service nodes and on the Microsoft servers.

Figure 1: Integration Overview

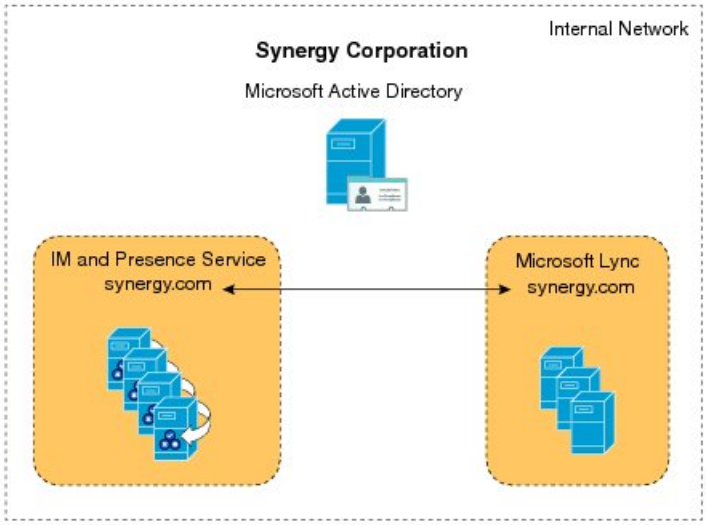


Single Domain Example

In this example, users within the presence domain called synergy.com on both theIM and Presence Service node and the Microsoft Lync server are able to exchange Availability and IM using partitioned intradomain

federation because the synergy.com presence domain is configured on both systems. The common active directory enables contact searches and display name resolution for all users on both systems.

Figure 2: Single Presence Domain Intradomain Federation Example



Note Presence domains must be identical. For example, user1@abc.synergy.com cannot share IM and Availability with any of the federated users configured for intradomain federation on synergy.com. Move user1 from the abc.synergy.com presence domain to the synergy.com domain to enable user1 to participate in Partitioned Intradomain Federation in this example.

Partitioned Intradomain Federation Configuration

You configure the following key components to enable partitioned intradomain Federation between IM and Presence Service and your Microsoft Lync/OCS/LCS server:

1. IM and Presence Service node
2. Microsoft server
3. User migration

Tip See the detailed configuration workflows for the start-to-finish steps needed to enable partitioned intradomain federation and for links to the procedures that are performed at each step of the process.

Cisco recommends that you back up the Microsoft server user contact list information before proceeding to configure partitioned intradomain federation between IM and Presence Service and your Microsoft server.

Table 1: Partitioned Intradomain Federation High Level Configuration Tasks for the IM and Presence Service Node

Task	O = Optional M = Mandatory
Ensure that the common domain to be used for Partitioned Intradomain Federation is configured on IM and Presence Service node and verify that matching domains are configured on the Microsoft servers	M
Enable partitioned intradomain federation	M
Set up static routes to the Microsoft server	M
Set up access control lists	M
Set up TLS for the Lync server (required if you are using a Lync server)	M
Set up TLS for OCS and LCS servers	O
Deactivate non-essential services on the dedicated routing server (if applicable)	M

Table 2: Partitioned Intradomain Federation High Level Configuration Tasks for the Lync Server

Task	O = Optional M = Mandatory
Ensure that the common domain used for partitioned intradomain federation is configured on the Lync server and verify that it matches the domain that is configured on the IM and Presence Service nodes.	M
Set up static routes to the IM and Presence Service node	M
Set up host authorization	M
Publish the topology	M
Set up TLS	M

The following table lists the high-level Partitioned Intradomain Federation configuration tasks for the OCS and LCS servers

Table 3: Partitioned Intradomain Federation High Level Configuration Tasks for the OCS and LCS Servers

Task	O = Optional M = Mandatory
Ensure that the common domain used for Partitioned Intradomain Federation is configured on the Lync server and verify that it matches the domain that is configured on IM and Presence Service nodes.	M
Enable SIP port	M
Set up static routes to IM and Presence Service node	M
Set up host authorization	M
Set up TLS	O

Table 4: Partitioned Intradomain Federation User Migration Tasks

Task	O = Optional M = Mandatory
Download tools	M
Disable Lync subscriber notification pop-ups	M
Set unlimited contact list sizes and watcher sizes	M
Enable auto authorization of subscriber requests	M
Provision Microsoft server users on Cisco Unified Communications Manager	M
Back up user Microsoft server contact list information	M
Export contact lists for users	M
Disable users on Microsoft server	M
Verify that user accounts are disabled	M
Delete user data from database for migrating users **Note** Depending on your Microsoft server deployment, you may have to perform this procedure on multiple databases.	M
Import contact lists for migrating users in to IM and Presence Service	M
Reset maximum contact list and watcher size	M
Re-enable Lync subscriber notification pop-ups	M

Related Topics

Backups of User Microsoft Server Contact List Information, on page 99
Configuration Workflow for Partitioned Intradomain Federation with LCS, on page 38
Configuration Workflow for Partitioned Intradomain Federation with Lync, on page 35
Configuration Workflow for Partitioned Intradomain Federation with OCS, on page 37
Configuration Workflow for User Migration from Microsoft Servers to the IM and Presence Service, on page 39
Disable Microsoft Lync Pop-ups, on page 98
Restore Microsoft Lync Pop-up Behavior, on page 98

Availability

This section describes Availability functionality.

Availability Subscriptions and Policy

This section describes call flows for IM and Presence Service and Microsoft Lync or Microsoft Office Communicator.

Subscription to an IM and Presence Service User

When a Microsoft Lync or Microsoft Office Communicator user wishes to view the availability of an IM and Presence Service client user, a SIP SUBSCRIBE request is routed from Lync/OCS/LCS to IM and Presence Service. IM and Presence Service accepts the incoming subscription and places it in a pending state. Privacy policy is then applied to this incoming subscription request.

Note Privacy policy applied to subscriptions from Microsoft server users in a partitioned intradomain federation deployment is identical to the privacy policy applied to subscriptions from IM and Presence Service client users.

IM and Presence Service checks whether auto-authorization is enabled or whether the IM and Presence Service client user has previously blocked or allowed presence subscriptions from the Microsoft server user. If either case is true, IM and Presence Service auto-handles policy decision for the subscription request. Otherwise, the IM and Presence Service client user receives an alert regarding the new subscription.

If the subscription is denied, polite blocking is implemented. This means that the presence state of the user appears as offline to the Microsoft server user. If the subscription is authorized,IM and Presence Service sends availability updates to the Microsoft server user and the IM and Presence Service client user also has the option to add the Microsoft server user to their roster.

Subscription to Microsoft Lync or Microsoft Office Communicator User

When an IM and Presence Service client user wishes to view the availability of a Microsoft Lync or Microsoft Office Communicator user, a SIP SUBSCRIBE request is routed from IM and Presence Service to

Lync/OCS/LCS. The Microsoft server accepts the incoming subscription. Policy is then applied to this incoming subscription request.

If the Microsoft server user has previously accepted a subscription from this IM and Presence Server user, the subscription is auto-accepted and availability is returned to the IM and Presence Service client user in line with the policy level applied by the Microsoft server user. If not, the Microsoft server user receives an alert regarding the new subscription. The Microsoft server user can then accept or block the IM and Presence Service client user.

Note The Microsoft server performs a refresh SIP SUBSCRIBE approximately every 1 hour and 45 minutes. Therefore, if an IM and Presence Service node restarts, the maximum duration a Microsoft Lync or Microsoft Office Communicator user is without the availability status of the IM and Presence Service contacts is approximately two hours.

If the Microsoft server restarts, the maximum duration an IM and Presence Service client is without available status of Microsoft Lync or Microsoft Office Communicator contacts is approximately 2 hours.

Availability Mapping States

The following table shows the availability mapping states from Microsoft Lync or Microsoft Office Communicator to the following IM and Presence Service supported clients:

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPad
- Cisco Jabber IM for Mobile (iPhone, Android, Blackberry)
- Cisco Unified Personal Communicator Release 8.x
- Third-party XMPP clients

Table 5: Availability Mapping States from Microsoft Lync or Microsoft Office Communicator

Microsoft Lync or Microsoft Office Communicator Setting	Cisco Jabber[1] Setting	Cisco Unified Personal Communicator 8.x Setting	Third-Party XMPP Clients Setting
Available	Available	Available	Available
Away	Away	Away	Away
Be Right Back	Away	Away	Away
Busy	Busy	Busy	Busy
Do Not Disturb	Busy	Busy	Busy
Appear Offline	Offline	Offline	Offline

Microsoft Lync or Microsoft Office Communicator Setting	Cisco Jabber[1] Setting	Cisco Unified Personal Communicator 8.x Setting	Third-Party XMPP Clients Setting
Offline	Offline	Offline	Offline

1 Applies to all supported Cisco Jabber clients.

The following table shows the availability mapping states from all supported Cisco Jabber clients to Microsoft Lync or Microsoft Office Communicator.

Table 6: Availability Mapping States from Cisco Unified Personal Communicator Release 8.x to Microsoft Lync or Microsoft Office Communicator

Cisco Unified Personal Communicator Release 8.x Setting	Microsoft Lync or Microsoft Office Communicator Setting
Available	Available
Busy	Busy
On the Phone	Busy
Meeting	Busy
Away	Away
Do Not Disturb	Busy
Offline	Offline
Offline—On the Phone	Offline
Offline—Meeting	Offline
Offline—Out of Office	Offline

The following table shows the availability mapping states from Cisco Jabber to Microsoft Lync or Microsoft Office Communicator.

Table 7: Availability Mapping States from Cisco Jabber to Microsoft Lync or Microsoft Office Communicator

Cisco Jabber[2] Setting	Microsoft Lync or Microsoft Office Communicator Setting
Available	Available
Away	Away

Cisco Jabber[2] Setting	Microsoft Lync or Microsoft Office Communicator Setting
Do Not Disturb	Busy
Out of Office	Offline
Offline	Offline

2 Applies to all supported Cisco Jabber clients.

The following table shows the availability mapping states from third-party XMPP clients to Microsoft Lync or Microsoft Office Communicator.

Table 8: Availability Mapping States from Third-Party XMPP Clients to Microsoft Lync or Microsoft Office Communicator

Third-Party XMPP Setting	Microsoft Lync or Microsoft Office Communicator Setting
Available	Available
Away	Away
Extended Away	Away
Do Not Disturb	Busy
Offline	Offline

Instant Messaging

Partitioned intradomain federation supports point-to-point IM between the IM and Presence Service client users and Microsoft Lync or Microsoft Office Communicator users. This includes support for the following IM features:

- Plain text IM format
- Typing indication
- Basic emoticons

SIP Session Mode IM is used to transfer messages and typing indications between the IM and Presence Service and the Microsoft server.

When an IM and Presence Service client user sends an IM to a Microsoft server user, if no existing IM session is established between these two users, IM and Presence Service sends a SIP INVITE message to the Microsoft server to establish a new session. This session is used for any subsequent SIP MESSAGE or SIP INFO (typing indication) traffic from either of these two users.

Note The IM and Presence Service client users and third-party XMPP client users can begin an IM conversation with a Microsoft server user even if they do not have availability.

When a Microsoft user sends an IM to an IM and Presence Service client user, if no existing IM session is established between these two users, the Microsoft server sends a SIP INVITE message to the IM and Presence Service. This session is used for any subsequent SIP MESSAGE or SIP INFO (typing indication) traffic from either of these two users.

Note Due to the proprietary nature of Microsoft server group chat functionality, partitioned intradomain federation does not support group chat between the IM and Presence Service client users and Microsoft Lync or Microsoft Office Communicator users.

Request Routing

This section describes request routing for IM and Presence Service to Lync/OCS/LCS and for Lync/OCS/LCS to IM and Presence Service.

IM and Presence to Microsoft Server Request Routing

To enable basic connectivity from IM and Presence Service to Lync/OCS/LCS, you must configure SIP static routes on IM and Presence Service for the IM and Presence Service domain. These static routes point to an IP address of a Microsoft server or front-end load balancer (Enterprise Edition Microsoft servers only) and allow IM and Presence Service to route same-domain requests to the Microsoft server when the recipient is not an IM and Presence Service user. Transport Layer Security (TLS) encryption can be enabled on these static routes. To support basic connectivity from IM and Presence Service to the Microsoft server, you must also configure entries in the Incoming Access Control List (ACL) to ensure that the Microsoft servers can access the IM and Presence Service node without authentication.

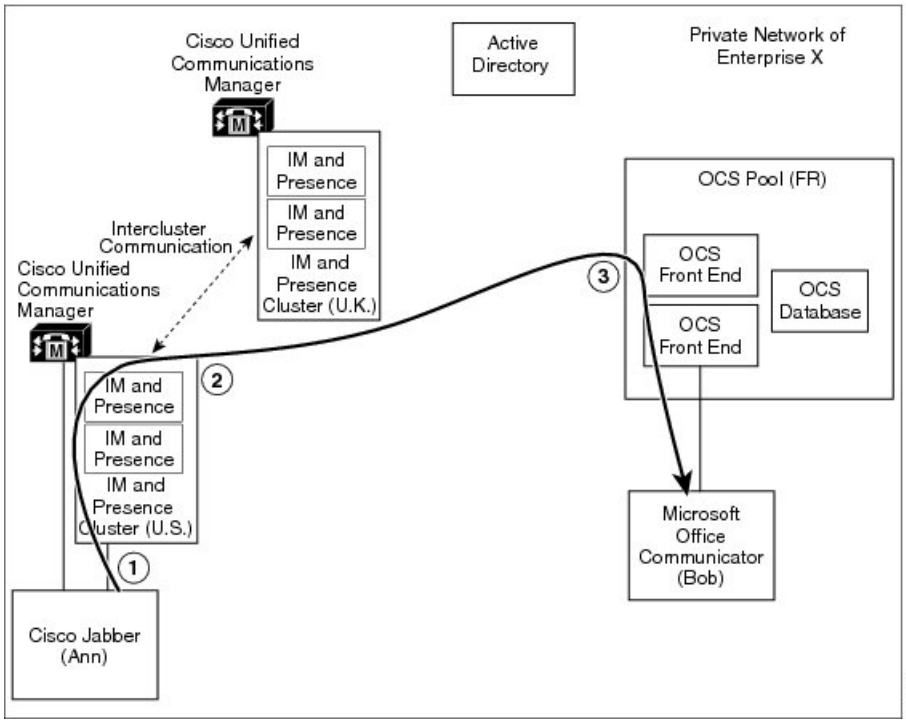
Overlaying this basic connectivity, partitioned intradomain federation provides two modes of request routing from IM and Presence Service to the Microsoft server: Basic Routing and Advanced Routing.

Basic Routing Mode for Partitioned Intradomain Federation

Basic Routing is the default routing mode for partitioned intradomain federation. When Basic Routing is enabled, IM and Presence Service routes a request to Lync/OCS/LCS if the request recipient is within the IM and Presence Service domain but is not a licensed IM and Presence Service user.

The following figure shows the sequence of the routing request from IM and Presence Service to the Microsoft server when Basic Routing is configured. This figure shows an example of an OCS deployment, but it also applies to the other supported Microsoft servers.

Figure 3: IM and Presence Service to Microsoft Server Request Routing



1	Ann, a Cisco Jabber 8.x user, sends a request to Bob, who is a Microsoft Office Communicator user in the same presence domain.
2	Because Bob is within the local presence domain but is not a licensed IM and Presence Service client user, IM and Presence Service translates the request and routes it to OCS.
3	The OCS server forwards the request to Bob's Microsoft Office Communicator client.

Note

- For recipients who are not provisioned on either the IM and Presence Service or a Microsoft server, any such request that is forwarded to the Microsoft server is in turn returned by the Microsoft server to IM and Presence Service.
- IM and Presence Service has built-in loop detection to reject any requests that loop back from the Microsoft server in this manner.

Advanced Routing Mode for Partitioned Intradomain Federation

Advanced Routing ensures less traffic between IM and Presence Service and Lync/OCS/LCS in deployments in which there are a large number of unprovisioned or unknown contacts in the IM and Presence Service database. However, Advanced Routing does add an additional storage overhead on each IM and Presence Service cluster because each cluster must store all Microsoft Lync or Microsoft Office Communicator users so that the Advanced Routing logic can be applied.

Configure Advanced Routing for partitioned intradomain federation only when you have a single-cluster IM and Presence Service deployment and Cisco Unified Communications Manager synchronizes its users from the same Active Directory that the Microsoft server uses. When more than one IM and Presence Service cluster is deployed, you must use the default basic routing method.

For Advanced Routing, the list of users synchronized from Active Directory must include all Microsoft Lync or Microsoft Office Communicator users.

When Advanced Routing is enabled, IM and Presence Service routes the request to the Microsoft server when both of the following conditions are met:

- The request recipient is within the IM and Presence Service domain but is not a licensed IM and Presence Service user

  and

- The request recipient has a valid Microsoft Lync or Microsoft Office Communicator SIP address stored in the IM and Presence Service database.

Microsoft Server to IM and Presence Service Request Routing

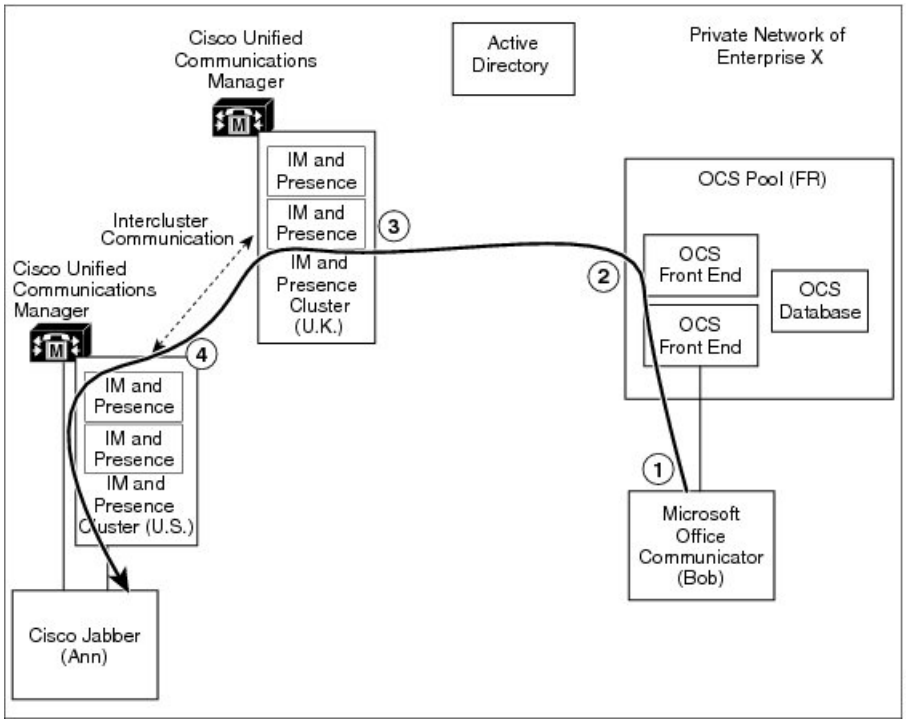
To enable basic connectivity from Lync/OCS/LCS to the IM and Presence Service, you must configure SIP static routes on the Microsoft server for the IM and Presence Service domain. These static routes point to the IP address and port of an IM and Presence Service node, which is designated as the routing IM and Presence Service node. They allow the Microsoft server to route same-domain requests to the IM and Presence Service when the recipient is not a Microsoft server user. TLS encryption can be enabled on these static routes.

To ensure that the Microsoft server is not prompted for authorization to accept SIP Requests from IM and Presence Service, you must also configure Host Authorization entries on the Microsoft server for each IM and Presence Service node.

As mentioned, overlaying the static route configuration, the Microsoft server has just a single routing mode in a partitioned intradomain federation deployment. The Microsoft server routes requests to IM and Presence Service if the request recipient is within one of the Microsoft server managed IM and availability domains but is not a Microsoft Lync or Microsoft Office Communicator user.

The following figure shows the sequence of the routing request from a Microsoft server to IM and Presence Service. This figure shows an example of an OCS deployment, but it also applies to the other Microsoft server deployments.

Figure 4: Microsoft Server to IM and Presence Service Request Routing



1	Bob, a Microsoft Office Communicator user, sends a request to Ann, who is a Cisco Jabber user.	3	IM and Presence Service accepts the request and forwards it to Ann's home IM and Presence Service node.
2	Because Ann is within the local presence domain but is not a Microsoft Office Communicator user, the Microsoft server routes the request to IM and Presence Service.	4	IM and Presence Service translates the request and forwards it to Ann's Cisco Jabber client.

Note For recipients who are not provisioned on either the IM and Presence Service or the Microsoft server, any such requests that are forwarded by the Microsoft server to IM and Presence Service are rejected by IM and Presence Service.

Intercluster and Multinode Deployments

In an intercluster and multinode cluster IM and Presence Service deployment, when establishing an Availability subscription or IM conversation, Lync/OCS/LCS servers route all SIP messages to an IM and Presence Service node that is designated for routing purposes. If the IM and Presence Service routing node does not host the

recipient user, it routes the message to the appropriate IM and Presence Service node within the deployment. The system routes all responses that are associated with this request back through the routing IM and Presence Service node.

Any IM and Presence Service node, when establishing an Availability subscription or IM conversation, can send a SIP message directly to a Microsoft server. When the Microsoft server replies to these messages, the replies are sent directly back to the IM and Presence Service node that began the message.

Interdomain Federation

IM and Presence Service supports interdomain federation. This feature is also available when IM and Presence Service is configured for partitioned intradomain federation. However, any interdomain federation that is configured on IM and Presence Service is available only to IM and Presence Service client users.

If the Lync/OCS/LCS deployment is already configured for SIP interdomain federation through an Access Edge/Access Proxy server, Microsoft Lync or Microsoft Office Communicator users can continue to use this federation capability. It is also possible to configure the IM and Presence Service and the Microsoft server so that IM and Presence Service client users can take advantage of such existing federation capability.

Note

- It is not supported to configure both the IM and Presence Service and the Microsoft server to federate directly with the same remote domain.
- See the document *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for more information about interdomain federation.

Related Topics

IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers, on page 115
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

High Availability for Intradomain Federation

Partitioned intradomain federation supports high availability for request routing between IM and Presence Service and Lync/OCS/LCS.

High Availability for IM and Presence Service to Microsoft Server Request Routing

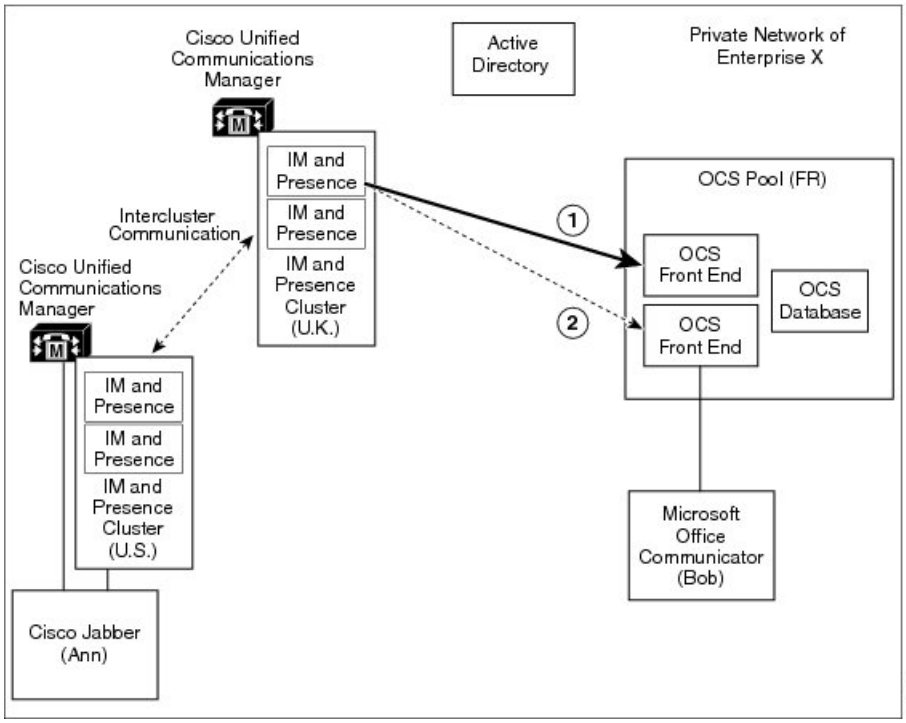
As mentioned earlier, SIP static routes must be configured on IM and Presence Service to enable basic intradomain federation connectivity between IM and Presence Service and Lync/OCS/LCS.

To provide high availability for integration with Microsoft servers, you can configure multiple SIP static routes for each address pattern on IM and Presence Service.

You can assign priority values to these static routes, as required, to define primary and backup static routes. Highest Priority routes are attempted first. If those routes are not available, the request is re-sent using the

backup route as shown in the following figure. This figure shows an example of an OCS deployment, but it also applies to the other supported Microsoft servers.

Figure 5: High Availability for IM and Presence Service to Microsoft Server Request Routing

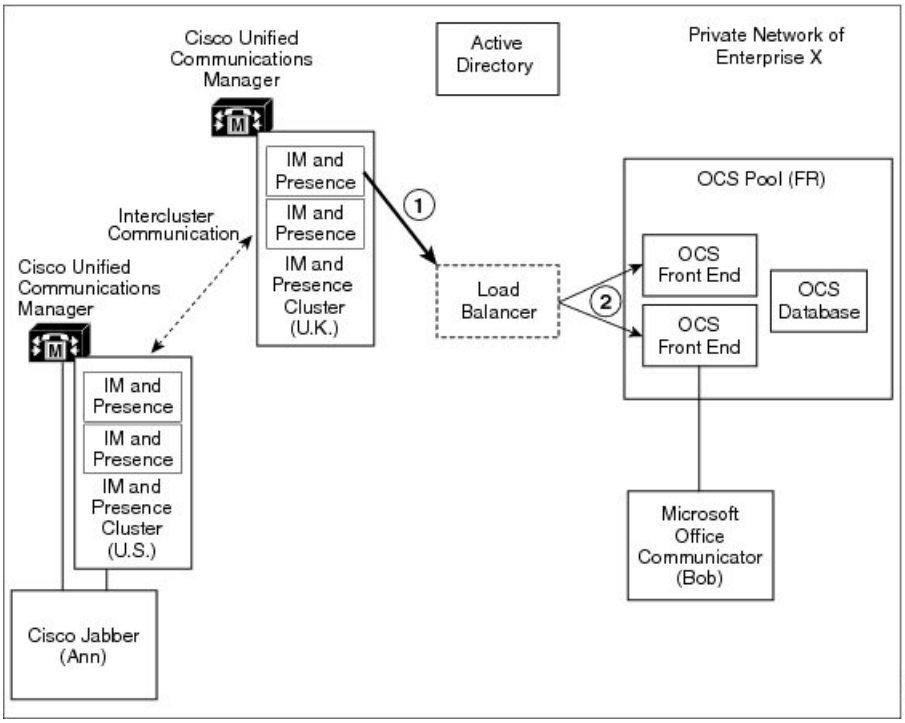


1	When routing to a Microsoft server, IM and Presence Service finds the highest-priority static route and attempts to send the request to the next hop address that is configured for that route.	2	If that next hop is not available, IM and Presence Service falls back to the next-highest priority static route and attempts to send the request to the associated next hop address.

In the case of Enterprise Edition Microsoft servers, you can deploy a front-end load balancer. In such cases, you can configure SIP static routes on IM and Presence Service to point to the IP address of the Microsoft server's front-end load balancer. The front-end load balancer provides high availability within its associated

Microsoft server pool as shown in the following figure. This figure shows an example of an OCS deployment, but it also applies to other Microsoft servers.

Figure 6: High Availability with Load Balancer for IM and Presence to Microsoft Server Request Routing



1	When routing to a Microsoft server, IM and Presence Service finds a static route that points to the OCS front-end load balancer.	2	The Microsoft server's front-end load balancer then routes onward to one of the active front-end servers within the pool.

See the following URL for a list of approved load balancers: http://technet.microsoft.com/en-us/office/ocs/cc843611. It is your responsibility to ensure that those load balancers are deployed and managed correctly.

Note Cisco does not support the configuration of static routes to point to load balancers. Cisco recommends that you configure static routes to bypass the front-end load balancer.

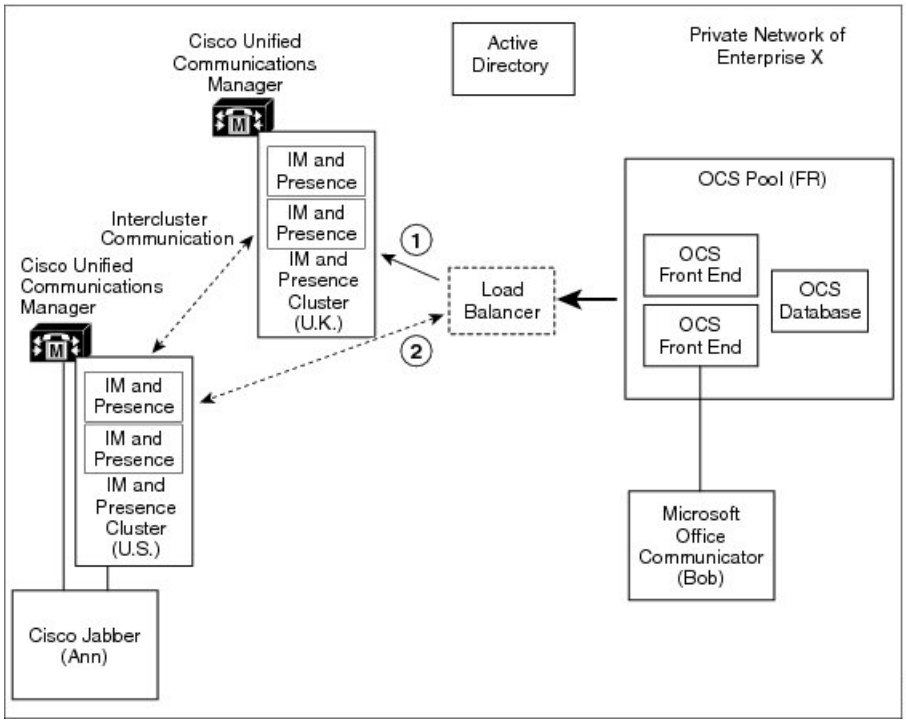
High Availability for Microsoft Server to IM and Presence Service Request Routing

SIP static routes must be configured on Lync/OCS/LCS to enable basic intradomain federation connectivity between Microsoft server and IM and Presence Service.

However, Microsoft servers support configuration of only a single SIP static route for each domain, which means that the static route can point to just a single IM and Presence Service node.

Therefore, to achieve high availability when IM and Presence Service is integrated with a Microsoft server, you must incorporate a load balancer between the IM and Presence Service node and Microsoft server as shown in the following figure. This figure shows an example of an OCS deployment, but it also applies to the other Microsoft servers.

Figure 7: High Availability for Microsoft Server to IM and Presence Service Request Routing



1	The load balancer works in Active/Backup mode. It routes requests to the primary IM and Presence Service node while that server is running and uses heartbeat signaling to check if the IM and Presence Service node is alive.	2	If the IM and Presence Service fails, the load balancer ensures that all subsequent requests are routed to the backup IM and Presence Service node.

Contact Search

Partitioned intradomain federation allows for full search capabilities on both IM and Presence Service-supported clients and Microsoft Lync or Microsoft Office Communicator.

Active Directory (AD) searches by IM and Presence Service-supported clients return users regardless of where they are provisioned. Microsoft server Address Book searches continue to return all Microsoft server users and also any IM and Presence Service client users who have migrated to IM and Presence Service.

Contact Card information is available on both clients for all contacts.

Note If an IM and Presence Service client user was never provisioned on the Microsoft server, you must perform an Active Directory update to the msRTCSIP-PrimaryUserAddress field for such users to ensure that the user is available for the Microsoft server searches.

User Migration

At a high level, the administrative flow for user migration is as follows:

1. License and assign migrating Microsoft server users to the IM and Presence Service.
2. Back up Microsoft server data for migrating Microsoft server users.
3. Export Microsoft server contact lists for each of the migrating Microsoft server users.
4. Disable Microsoft server user accounts for migrating Microsoft server users.
5. Delete Microsoft server user data for migrating Microsoft server users.
6. Import Microsoft server contact lists into the IM and Presence Service database for the migrated users.
7. Deploy an IM and Presence Service supported client on migrated users' desktops.

To further aid the migration process for administrators, a number of tools are available with this feature.

One of the primary advantages of a Partitioned Intradomain Federation deployment is that it allows a seamless transition from a Microsoft server to the IM and Presence Service within an enterprise. Partitioned Intradomain Federation offers the following benefits:

- IM and Presence Service client users and Microsoft Lync or Microsoft Office Communicator users share the same presence domain.
- Users can exchange Availability and Instant Messaging within that shared domain.
- Users can search for and add contacts regardless of where the user or contact is provisioned.

User Migration Tools

IM and Presence Service provides tools for the following Lync/OCS/LCS user migration steps:

- Export Microsoft server contact lists for each of the migrating Microsoft server users.
- Disable Microsoft server user accounts for migrating Microsoft server users.
- Delete Microsoft server user data for migrating Microsoft server users.
- Import Microsoft server contact lists into the IM and Presence Service database for the migrated users.

Note

- While attempting to run any of the user migration tools you may receive the following error: "Application failed to initialize properly". The reason for this error is that you are attempting to run the user migration tools without the .NET 1.1 Framework installed. Each of the user migration tools that Cisco provides requires that at least version 1.1 of the .NET Framework is installed on the server where you are running the tool.
- The Export, Disable and Delete tools are provided in a zip file on cisco.com. The Import tool is accessible through the **Cisco Unified CM IM and Presence Administration** user interface.

Export Microsoft Server Contact Lists for Each of the Migrating Microsoft Server Users

This IM and Presence Service tool allows for bulk export of contact lists from the Microsoft server. The exported contact lists are written to a comma-separated values (CSV) file that is acceptable to the IM and Presence Service Contact List Import Bulk Administration Tool (BAT). The combination of these tools allows for end-to-end administrative bulk contact list migration.

Disable Microsoft Server User Accounts for Migrating Microsoft Server Users

IM and Presence Service contains a tool to disable the Microsoft server user accounts in bulk. This tool disables Microsoft server accounts by connecting to Active Directory and modifying the user's Microsoft server-specific attributes as required.

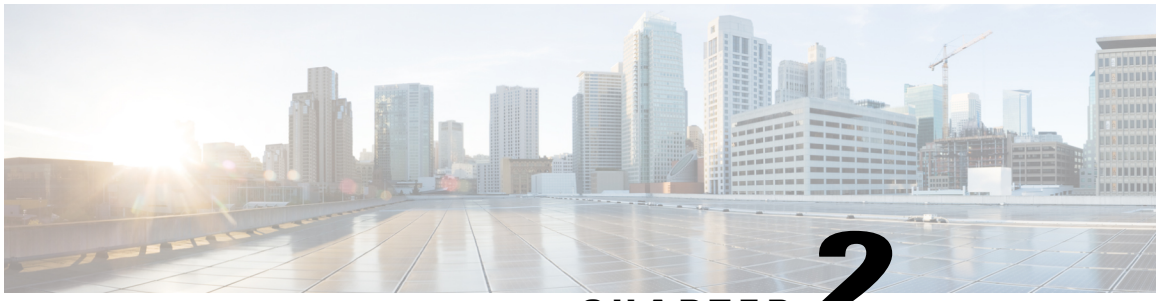
Delete Microsoft Server user Data for Migrating OCS Users

Microsoft server users must be deleted from the Microsoft servers to allow partitioned intradomain federation routing from the Microsoft server to IM and Presence Service. However, when users are deleted from the Microsoft servers, they are removed from the contact list of any Microsoft Lync or Microsoft Office Communicator users also. This IM and Presence Service tool deletes Microsoft server user data in bulk, while ensuring that the users are not removed from the contact list of Microsoft Lync or Microsoft Office Communicator users.

Import Microsoft Server Contact Lists into the IM and Presence Service Database for the Migrated Users

The IM and Presence Service BAT supports bulk contact list import. It takes a CSV file as input for this bulk import. When used in conjunction with the Microsoft server Export Contact List tool, it allows for contact list migration from a Microsoft server to IM and Presence Service.

Note Running the user migration tools has no affect on the capabilities of other Microsoft server users who are signed into Microsoft Lync or Microsoft Office Communicator. However, Cisco recommends that you run the user migration tools during a scheduled maintenance window to reduce the load on the Microsoft server and Active Directory system.



CHAPTER 2

Planning for Integration

- Supported Partitioned Intradomain Federation Integrations, page 21
- Hardware Requirements, page 22
- Software Requirements, page 23
- Integration Preparation, page 25
- Prerequisite Configuration for IM and Presence Service, page 32
- Additional Configuration for Routing IM and Presence Service Node, page 32
- Start IM and Presence Service Feature Services, page 33
- Plan Services Restarts during Off-Peak Periods, page 33

Supported Partitioned Intradomain Federation Integrations

For partitioned intradomain federation with Microsoft Lync, you must configure TLS; TCP is not supported. See the chapter *Configure Microsoft Lync for Partitioned Intradomain Federation* for more information.

This chapter describes the configuration steps for enabling partitioned intradomain federation between IM and Presence Service and Microsoft Lync/OCS/LCS. The following Microsoft server platforms are supported:

- Microsoft Lync Server 2010, Standard Edition and Enterprise Edition
- Microsoft Office Communications Server 2007 Release 2, Standard Edition and Enterprise Edition
- Microsoft Live Communications Server 2005, Standard Edition and Enterprise Edition

IM and Presence Service does not support an ASA in partitioned intradomain federation.

Note If you have a mixed deployment of both Lync and OCS/LCS servers, you must run the user migration tools for the Lync users, and then run the user migration tools for the OCS/LCS users.

Related Topics

Hardware Requirements, on page 22

Software Requirements, on page 23

Presence Web Service API Support

The Presence Web Service is an open interface that allows client applications to share user presence information with IM and Presence Service. Third party developers use this interface to build client applications that can send and retrieve updates about the presence state of a user. Note the following restriction about Presence Web Service API support:

- For partitioned intradomain federation, you cannot use the Presence Web Service API to obtain presence information from non-Cisco clients.

For more information about the Presence Web Service, see the *IM and Presence Service Developer Guide* at https://developer.cisco.com/site/collaboration/call-control/unified-presence/documentation/index.gsp.

Limitations for Microsoft Lync Integrations

There are two scenarios where adding partitioned intradomain federation breaks existing Microsoft Lync integrations:

- **You already have intradomain federation configured for video with Cisco VCS or Cisco Expressway and want to add partitioned intradomain federation with IM and Presence Service:** Microsoft Lync is integrated with Cisco VCS or Cisco Expressway and you have a static route configured on Lync to route video and voice traffic for the local Lync presence domain to Cisco VCS or Cisco Expressway. If you modify the static route to point to IM and Presence Service (a requirement for partitioned intradomain federation) you will break the existing video integration because the traffic that is intended for Cisco VCS or Cisco Expressway would instead be routed to IM and Presence Service. You cannot have both video integration and partitioned intradomain federation to IM and Presence Service.
- **You already have integration with Microsoft Exchange Unified Messaging and want to add partitioned intradomain federation with IM and Presence Service:** You have a Microsoft Lync server configured for Unified Messaging to Microsoft Exchange (either on-premises, or to the cloud (Office365). If you add a static route from Lync for the local Lync presence domain to point to IM and Presence Service (a requirement for partitioned intradomain federation), Unified Messaging integration between Lync and Microsoft Exchange for the domain will be terminated because all Unified Messaging SIP traffic for that domain will be routed to IM and Presence Service. You cannot have both integration to Microsoft Exchange Unified Messaging and partitioned intradomain federation to IM and Presence Service.

Note Neither Microsoft Exchange Unified Messaging nor Cisco VCS (or Cisco Expressway) integrations are supported with partitioned intradomain federation if you are sharing the same domain between Microsoft Lync and IM and Presence Service.

Hardware Requirements

Partitioned intradomain federation between IM and Presence Service and Lync/OCS/LCS requires the following Cisco hardware:

- IM and Presence Service node. For IM and Presence Service hardware support, refer to the IM and Presence Service compatibility matrix.
- Cisco Unified Communications Manager node. For Cisco Unified Communications Manager hardware support, refer to the compatibility information for Cisco Unified Communications Manager document available on Cisco.com.

Related Topics

Compatibility Information for IM and Presence Service and Cisco Unified Communications Manager Software Requirements, on page 23

Software Requirements

The following sections outline the software required for partitioned intradomain federation between IM and Presence Service and Lync/OCS/LCS.

Server Software

The following server software is required for partitioned intradomain federation:

Cisco Software

- IM and Presence Service
- Cisco Unified Communications Manager

Microsoft Software

- Depending on the deployment, one of:
  - Microsoft Lync Server 2010, Standard Edition or Enterprise Edition
  - Microsoft Office Communications Server 2007 Release 2, Standard or Enterprise Edition
  - Microsoft Live Communications Server 2005, Standard or Enterprise Edition
- Depending on the deployment, one of:
  - Lync Administrative Tools (optional install item available during installation of Lync)
  - OCS Administrative Tools (optional install item available during installation of OCS)
  - LCS Administrative Tools (optional install item available during installation of LCS)
- Microsoft Active Directory

Other Software

While attempting to run any of the user migration tools you may receive the following error: "Application failed to initialize properly". The reason for this error is that you are attempting to run the user migration tools

without the .NET 1.1 Framework installed. Each of the user migration tools that Cisco provides requires that at least version 1.1 of the .NET Framework is installed on the server where you are running the tool.

Client Software

The client software required for partitioned intradomain federation deployment between the IM and Presence Service and Lync/OCS/LCS depends on your deployment. You can have any combination of IM and Presence Service supported clients in a partitioned intradomain federation deployment.

IM and Presence Service Supported Clients

The following IM and Presence Service clients are supported in a partitioned intradomain federation deployment between IM and Presence Service and Lync/OCS/LCS:

Cisco Software

- Cisco Unified Personal Communicator Release 8.5
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber IM for Mobile (iPhone, Android, Blackberry)
- Cisco Jabber for iPad
- Cisco Jabber for Cius

Note For version compatibility for all Cisco Jabber clients, see the appropriate Cisco Jabber client documentation.

Third-Party Software

Third-party XMPP clients

Microsoft Server Supported Clients

Depending on the deployment, the following clients are supported:

- Microsoft Lync 2010
- Microsoft Office Communicator 2005
- Microsoft Office Communicator 2007 Release 2
- Communicator Web Access 2005
- Communicator Web Access 2007 Release 2

Related Topic

Hardware Requirements, on page 22

Integration Preparation

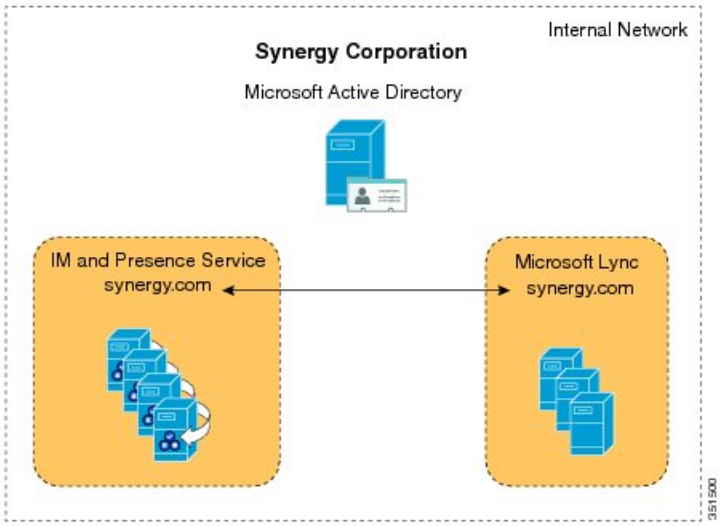
It is essential that you plan carefully for the configuration of partitioned intradomain federation between IM and Presence Service and Lync/OCS/LCS. Read the items in this section before you begin any configuration for this integration.

Presence Domains

Partitioned intradomain federation, by its nature, supports integration between IM and Presence Service and Lync/OCS/LCS within a common presence domain that is configured on both systems. However, the Microsoft server supports the configuration of multiple presence domains for each Microsoft server deployment. All Microsoft Lync or Microsoft Office Communicator users who are not configured on the common presence domain that matches the domain that is configured on IM and Presence Service cannot participate in partitioned intradomain federation.

For example, in the following figure, user1@abc.synergy.com cannot share IM and Availability with any of the federated users configured for Intradomain Federation on synergy.com. Add user1 to the synergy.com domain to enable user1 to participate in Intradomain Federation in this example.

Figure 8: Single Domain Intradomain Federation Example



User Migration

If users are being migrated from Lync/OCS/LCS to the IM and Presence Service as part of this integration, consider the information below.

Detailed User Migration Plan

The partitioned intradomain federation integration between the IM and Presence Service and Lync/OCS/LCS is designed to provide basic communication between users during a phased migration from a Microsoft server to IM and Presence Service.

However, partitioned intradomain federation integration introduces a performance overhead. Because of this, IM and Presence Service can support a maximum of 130,000 SIP intradomain federation contacts per server. To ensure that this federated contact threshold is not exceeded on any IM and Presence Service node during migration of users from the Microsoft server to IM and Presence Service, a detailed user migration plan may be required.

You can use the following calculation to get an estimate of the maximum number of IM and Presence Service users that can be supported without breaking the above federated contact threshold:

Max Supported Users = 130,000 / Average Contact List Size.

Based on this calculation, the following table gives an indication of the maximum number of IM and Presence Service users that can be supported without breaking the 130,000 federated contact threshold.

Table 9: Maximum Number of Supported IM and Presence Service Users

Average Contact List Size	Maximum Supported Users (without high availability)	Maximum Supported Users (with high availability[3])
200	650	325
150	866	433
100	1300	650
75	1733	866
50	2600	1300
25	5000	2500

3 This assumes a 2-node subcluster running in active/active mode.

You require a detailed user migration plan if the number of users to be provisioned on any IM and Presence Service node within your deployment exceeds the relevant limit above. Contact your Cisco Support representative to begin the process of defining a detailed migration plan.

Notes

1. The values for the maximum number of supported users in the table above are based on worst-case figures; that is, in the case where all contacts are federated.

   With proper migration planning, the full complement of users can be deployed on an IM and Presence Service node in a phased manner, without breaking the 130,000 federated contact threshold.

2. When high availability is enabled, each IM and Presence Service node must be able to handle the load associated with all users within the IM and Presence Service 2-node subcluster because, in the event of a

node failure, the second node in the cluster services all users on its own. Therefore, the limit per node must be halved.

3 If you are unsure about the average contact list size within your Microsoft server deployment, assume it to be worst-case (200 contacts) when you are deciding whether a migration plan is required.

4 The values for the maximum number of supported users in the table above assume HCS-7845-I3 hardware or the equivalent Cisco supported virtual platform based on the IM and Presence Service OVA template for 5000 users. The equivalent numbers for a subset of other platforms are detailed below. If your platform is not listed, contact your Cisco Support representative for advice.

HCS-7825-H4 Hardware

The IM and Presence Service can support up to 18,000 SIP Intradomain Federation contacts per server on the HCS-7825-H4 platform. The following table gives an indication of the maximum number of IM and Presence Service users that can be supported without breaking the18,000 federated contact threshold.

Table 10: Maximum Number of Supported IM and Presence Service Users on HCS-7825-H4 Hardware

Average Contact List Size	Maximum Supported Users (without high availability)	Maximum Supported Users (with high availability[4])
200	90	45
150	120	60
100	180	90
75	240	120
50	360	180
25	720	360
18	1000	500

4 This assumes a 2-node subcluster running in active/active mode.

HCS-7845-H2 Hardware

The IM and Presence Service can support up to 90,000 SIP Intradomain Federation contacts per node on the HCS-7845-H2 platform. The following table gives an indication of the maximum number of IM and Presence Service users that can be supported without breaking the 90,000 federated contact threshold.

Table 11: Maximum Number of Supported IM and Presence Service Users on HCS-7845-H2 Hardware

Average Contact List Size	Maximum Supported Users (without high availability)	Maximum Supported Users (with high availability[5])
200	450	225

Average Contact List Size	Maximum Supported Users (without high availability)	Maximum Supported Users (with high availability[5])
150	600	300
100	900	450
75	1200	600
50	1800	900
25	3600	1800
18	5000	2500

5 This assumes a 2-node subcluster running in active/active mode.

Related Topics

User Migration, on page 19

Maintenance of User Identity During Migration

During migration from Lync/OCS/LCS to IM and Presence Service, Microsoft Lync and Microsoft Office Communicator users should maintain the same identity, which is their Uniform Resource Identity (URI). Maintaining the same identity during migration has the following benefits:

- It allows for the user's availability state to be continually monitored by existing followers because the user's identity does not change.
- It also allows for much simpler migration of a user's contact lists because the contact lists can be directly imported from the Microsoft server to IM and Presence Service.

IM and Presence Service URIs are composed by joining the Cisco Unified Communications Manager user ID with the IM and Presence Service domain as follows:

<userid>@<domain>

If users are manually added through the Cisco Unified Communications Manager user interface or through the Cisco Unified Communications Manager Bulk Administration Tool (BAT), you must ensure that the user ID that you specified when you created the user matches the user portion of the user's Microsoft server URI. For example, if the Microsoft user's URI is bobjones@foo.com, you should create the CUCM user with a user ID of bobjones.

If Cisco Unified Communications Manager is configured to synchronize users from Active Directory, you must ensure that the Active Directory field that is used to map to the Cisco Unified Communications Manager user ID matches the user portion of the Microsoft server URI. Note the following:

- Cisco Unified Communications Manager maps to userID from a limited number of Active Directory fields, the most common of which is sAMAccountName.
- If Cisco Unified Communications Manager maps userID to sAMAccountName, the Microsoft server URI for the migrating users must also match the format <sAMAccountName>@<domain>.

- If the sAMAccountName of Bob Jones is bjones, the Microsoft server URI must be bjones@cisco.com.
- If any Microsoft server URIs do not match the format <sAMAccountName>@<domain>, you must modify them before the first migration of users from the Microsoft server to IM and Presence Service.

Duration Guidelines for User Migration Tools

Cisco provides a number of tools to allow bulk migration of users from Lync/OCS/LCS to IM and Presence Service. To allow you to plan your migration, it is important to be aware of the time required for each tool to run when you are migrating a large number of users. This section describes the expected run time for each of those tools.

Note If you have a mixed deployment of both Lync and OCS/LCS servers, you must run the tools on the Lync users and then run the tools again on the OCS/LCS users.

Export Contact List Tool

The Export Contact List tool (ExportContacts.exe) can export contacts from Lync/OCS/LCS at an average rate of 800 contacts per second (or 48,000 contacts per minute). You can use the following equation as a guide to estimate the expected run time for this tool for a set of Microsoft server users.

Time to export contacts (mins) = Number of Microsoft server users x Average Contact List Size / 48000.

The following table shows the expected run time for a number of sample cases.

Table 12: Sample Expected Run Times for the Export Contact List Tool

Number of Microsoft Server Users	Average Contact List Size	Time to Export Contacts
2000	100	5 minutes
5000	75	8 minutes
15000	60	19 minutes

Disable Account Tool

The Disable Account tool (DisableAccount.exe) can disable Lync/OCS/LCS accounts at an average rate of 13 accounts per second (or 800 accounts per minute). You can use the following equation as a guide to estimate the expected run time for this tool for a set of Microsoft server users.

Time to disable accounts (mins) = Number of Microsoft server users / 800

The following table shows the expected run time for a number of sample cases.

Table 13: Sample Expected Run Times for the Disable Account Tool

Number of Microsoft server users	Time to disable accounts
2000	3 minutes

Number of Microsoft server users	Time to disable accounts
5000	7 minutes
15000	20 minutes

Delete Account Tool

The Delete Account tool (DeleteAccount.exe) can delete Lync/OCS/LCS accounts at an average rate of 13 accounts per second (or 800 accounts per minute). You can use the following equation as a guide to estimate the expected run time for this tool for a set of Microsoft server users.

Time to delete accounts (mins) = Number of Microsoft server users / 800.

The following table shows the expected run time for a number of sample cases.

Table 14: Sample Expected Run Times for the Delete Account Tool

Number of Microsoft Server Users	Time to Delete Accounts
2000	3 minutes
5000	7 minutes
15000	20 minutes

Bulk Administration Tool Contact List Import

The IM and Presence Service Bulk Administration Tool (BAT) can import contacts at varying rates, depending on the IM and Presence Service platform. The following table shows the expected import rate for a selection of IM and Presence Service platforms.

Table 15: Import Rate for the IM and Presence Service BAT

IM and Presence Service Platform	Import Rate
MCS-7825-H4/2000 user OVA	6/sec
MCS-7845-H2/5000 user OVA	12/sec
MCS-7845-I3/15000 user OVA	22/sec

The following table shows the expected run time for a number of sample cases

Table 16: Sample Expected Run Times for the BAT Contact List Import Utility

Number of Users	Average Contact List Size	Import Time (Rate = 22/sec[6])
2000	100	2hours, 32 minutes
5000	75	4 hours, 45 minutes
15000	60	11 hours, 22 minutes

6 These estimates apply to the highest specification machines which support a contact import rate of 22/sec.

Notes

1. The calculations for the Export Contact List tool, Disable Account tool, and Delete Account tool are based on the Lync/OCS/LCS and Active Directory (AD) running on hardware with at least 2Ghz CPU processing power, and 2GB of RAM.
2. Running these user migration tools has no affect on the capabilities of other Microsoft server users who are signed into Microsoft Lync or Microsoft Office Communicator.
3. Cisco recommends that you perform user migration during a scheduled maintenance window to reduce the load on the Microsoft server and AD system.

DNS Configuration

Domain Name System (DNS) "A" records must be published within the enterprise for all IM and Presence Service nodes and Lync/OCS/LCS servers.

Microsoft servers must be able to resolve Fully Qualified Domain Names (FQDN) and IP addresses for all IM and Presence Service nodes.

Likewise, IM and Presence Service nodes must be able to resolve FQDNs and IP addresses for all Microsoft server and pool FQDNs.

Certificate Authority Server

If TLS encryption is enabled as part of this partitioned intradomain federation integration, an external or internal Certificate Authority (CA) may be used to sign security certificates on IM and Presence Service and Lync/OCS/LCS. Cisco recommends that you use the same CA to sign the Microsoft server and the IM and Presence Service certificates. If not, the root certificates for each CA must be uploaded onto the Microsoft server and the IM and Presence Service nodes.

High Availability

You need to consider how you are going to configure availability in your partitioned intradomain federation deployment.

If you wish to make your IM and Presence Service partitioned intradomain federation capability highly available, you can deploy a load balancer in front of your designated (routing) IM and Presence Service nodes.

Note To deploy load balancing (for example, round robin), a hardware load balancer needs to be installed. The static route in IM and Presence Service points to the load balancer.

Related Topic

High Availability for Intradomain Federation, on page 15

Prerequisite Configuration for IM and Presence Service

You must complete the following tasks on the IM and Presence Service before you begin to configure partitioned intradomain federation.

1 Install and configure IM and Presence Service.

2 Perform the following checks to ensure that your IM and Presence Service system is operating properly:

- Run the IM and Presence Service System Configuration Troubleshooter.
- Check that you can add local contacts to the Jabber client of IM and Presence Service.
- Check that your clients are receiving availability states from the IM and Presence Service node.

Additional Configuration for Routing IM and Presence Service Node

In multi-server deployments, an IM and Presence Service node must be dedicated as the Routing IM and Presence Service node. This means that it is a front-end server that accepts all new inbound SIP requests from the Lync/OCS/LCS and routes them onwards to the IM and Presence Service node on which the request recipient is homed.

Cisco recommends that you do not assign any users to the Routing IM and Presence Service node; as this ensures that the Routing IM and Presence Service node has the capacity to handle the volume of SIP traffic from the Microsoft server.

Because no users are assigned to the Routing IM and Presence Service node, you can deactivate many of the feature services to free up resources on the Routing IM and Presence Service node. Deactivate the following feature services on the Routing IM and Presence Service node:

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver

- Cisco XCP Directory Service
- Cisco XCP Authentication Service

Related Topic

Deactivate Feature Services on the Routing IM and Presence Service Node, on page 51

Start IM and Presence Service Feature Services

The following services must be running on each IM and Presence Service node to support partitioned intradomain federation:

- Cisco SIP Proxy
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP Router

The Cisco XCP Router is a network service and therefore is started by default. The Cisco SIP Proxy and Cisco SIP Federation Connection Manager are feature services, which you must start.

The following procedure describes how to start the Cisco SIP Proxy and Cisco SIP Federation Connection Manager feature services. You must perform this procedure on all IM and Presence Service nodes.

Note For dedicated Routing IM and Presence Service nodes, do not activate the Cisco XCP SIP Federation Connection Manager service because no users are assigned to dedicated Routing IM and Presence Service nodes.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

Step 2 From the **Server** menu, choose the IM and Presence Service node.

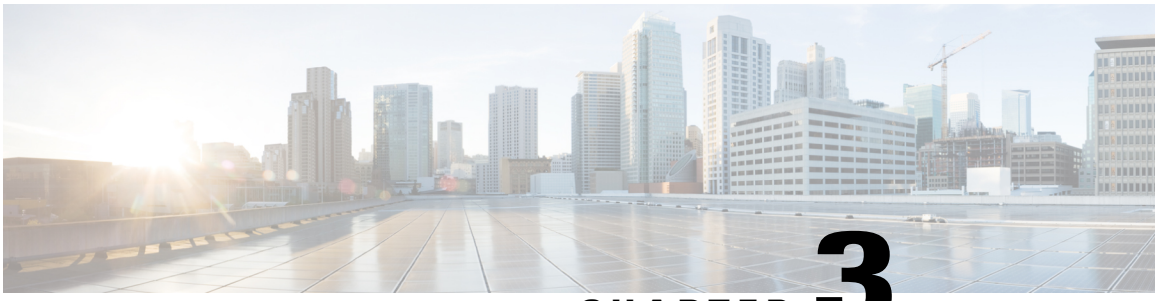
Step 3 Check the following services:

a) Cisco SIP Proxy
b) Cisco XCP SIP Federation Connection Manager

Step 4 Click **Save**.

Plan Services Restarts during Off-Peak Periods

During the integration process, you need to restart the Lync/OCS/LCS server front-end services. Plan to perform the services restart during off-peak periods, such as during a maintenance window, to minimize the impact to users. For more information, see the partitioned intradomain federation configuration workflows and topics related to restarting services for your server type.



CHAPTER 3

Configuration Workflows for Partitioned Intradomain Federation

This chapter provides configuration workflows for Partitioned Intradomain Federation with Microsoft Lync Server (Lync) 2010, Microsoft Live Communications Server (LCS) 2005, and Microsoft Office Communications Server (OCS) 2007 R2. It also describes the configuration workflow for user migration from Lync/OCS/LCS to the IM and Presence Service.

- Configuration Workflow for Partitioned Intradomain Federation with Lync, page 35
- Configuration Workflow for Partitioned Intradomain Federation with OCS, page 37
- Configuration Workflow for Partitioned Intradomain Federation with LCS, page 38
- Configuration Workflow for User Migration from Microsoft Servers to the IM and Presence Service, page 39
- Configuration Workflow for Integrating IM and Presence with Microsoft Server Interdomain Federation Capability, page 40

Configuration Workflow for Partitioned Intradomain Federation with Lync

Use the following workflow to configure partitioned intradomain federation between IM and Presence Service and Microsoft Lync servers:

IM and Presence Service Configuration

1. Verify that the required presence domains are configured on all IM and Presence Service nodes in the cluster.
2. Enable partitioned intradomain federation, see Configure a Static Route on Microsoft Lync for Federation, on page 56.
3. Configure static routes to Lync deployment, see Configure Static Routes, on page 42.
4. Configure Access Control Lists for Lync deployment, see Configure an Incoming Access Control List, on page 44.

5 Configure TLS encryption between the IM and Presence Service and Lync:

   a Configure application listeners, see Configure Application Listener Ports, on page 45.
   b Configure TLS peer subjects, see Configure TLS Peer Subjects, on page 46.
   c Configure peer authentication TLS context, see Configure Peer Authentication TLS Context, on page 48.
   d Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority, on page 48.
   e Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service, on page 49.
   f Import the CA signed certificate, see Import Signed Certificate from Certificate Authority, on page 50.

6 (Optional) If you are configuring a dedicated Routing IM and Presence Service node, deactivate unnecessary feature services on the Routing IM and Presence Service node, see Deactivate Feature Services on the Routing IM and Presence Service Node, on page 51.

Note Partitioned intradomain federation only supports back to back federation between IM and Presence Service and Microsoft Lync or OCS. A firewall (ASA) between the federated servers is not supported.

Lync Configuration

1 Verify that the presence domains for intradomain federation that are configured on the Lync server have matching presence domains configured on the IM and Presence Service nodes.

2 Configure Lync static route to the IM and Presence Service deployment, see Configure Lync Static Route to Point to IM and Presence Service.

3 Add host authorization for the IM and Presence Service deployment and enable port 5061, see Add Host Authorization for IM and Presence Service on an Enterprise Edition Lync Server, on page 58.

4 Publish the topology, see Publish Topology, on page 62.

5 Ensure CA root certificates are installed on each Lync server, see Install Certificate Authority Root Certificates on Lync, on page 63.

6 Ensure all Lync servers have the required signed certificates, see Validate Existing Lync Signed Certificate, on page 64.

7 Request signed certificate from Certificate Authority, see Request a Signed Certificate from a Certificate Authority for Lync, on page 65.

8 Download the certificate from the CA server, see Download a Certificate from the CA Server, on page 66.

9 Import the signed certificate, see Import a Signed Certificate for Lync, on page 67.

10 Assign the certificate, see Assign Certificate on Lync, on page 68.

11 Restart services, see Restart Services on Lync Servers, on page 68.

Tip Plan the restart of the front-end services during off-peak hours to minimize the impact on users.

After the server is configured, you can proceed to migrate the users.

Configuration Workflow for Partitioned Intradomain Federation with OCS

Use the following workflow to configure partitioned intradomain federation between IM and Presence Service and OCS 2007 R2:

IM and Presence Service Configuration

1. Verify that the required domain is configured on all IM and Presence Service nodes in the cluster.
2. Enable partitioned intradomain federation, see Configure Partitioned Intradomain Federation Options, on page 41.
3. Configure static routes to OCS deployment, see Configure Static Routes, on page 42.
4. Configure Access Control Lists for OCS deployment, see Configure an Incoming Access Control List, on page 44.
5. (Optional) Configure TLS encryption between IM and Presence Service and OCS:
   a. Configure application listeners, see Configure Application Listener Ports, on page 45.
   b. Configure TLS peer subjects, see Configure TLS Peer Subjects, on page 46.
   c. Configure peer authentication TLS context, see Configure Peer Authentication TLS Context, on page 48.
   d. Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority, on page 48.
   e. Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service, on page 49.
   f. Import the CA signed certificate, see Import Signed Certificate from Certificate Authority, on page 50.
6. (Optional) If you are configuring a dedicated Routing IM and Presence Service node, deactivate unnecessary feature services on the Routing IM and Presence Service node. See Deactivate Feature Services on the Routing IM and Presence Service Node, on page 51.

OCS Configuration

1. Verify that the domain for Intradomain federation that is configured on the OCS server has matching domains configured on the IM and Presence Service nodes.
2. Enable port 5060, see Enable Port 5060/5061 on OCS Server, on page 69.
3. Configure static routes to the IM and Presence Service deployment, see Configure Static Routes on OCS to Point to the IM and Presence Service, on page 72.

4 Add host authorization for the IM and Presence Service deployment, see Add Host Authorization on OCS for IM and Presence Service, on page 73.

5 (Optional) Configure TLS encryption between IM and Presence Service and OCS:

   a Ensure mutual TLS authentication is configured on each OCS server, see Configure Mutual TLS Authentication on OCS, on page 76.
   b Ensure CA root certificates are installed on each OCS server, see Install Certificate Authority Root Certificates on OCS, on page 76.
   c Ensure all OCS servers have the required signed certificates, see Validate Existing OCS Signed Certificate, on page 78.
   d If required, request a newly signed certificate, see Signed Certificate Request from the Certificate Authority for the OCS Server, on page 79.

6 Restart services, see Restart Services on OCS Front-End Servers, on page 74.

Tip Plan the restart of the front-end services during off-peak hours to minimize the impact on users.

After the server is configured, you can proceed to migrate the users.

Configuration Workflow for Partitioned Intradomain Federation with LCS

Use the following workflow to configure Partitioned Intradomain Federation between the IM and Presence Service and LCS 2005:

IM and Presence Service Configuration

1 Verify that the required domain is configured on all IM and Presence Service nodes in the cluster.

2 Enable Partitioned Intradomain Federation, see Configure Partitioned Intradomain Federation Options, on page 41.

3 Configure static routes to LCS deployment, see Configure Static Routes, on page 42.

4 Configure Access Control Lists for LCS deployment, see Configure an Incoming Access Control List, on page 44.

5 (Optional) Configure TLS encryption between IM and Presence Service and LCS:

   a Configure application listeners, see Configure Application Listener Ports, on page 45.
   b Configure TLS peer subjects, see Configure TLS Peer Subjects, on page 46.
   c Configure peer authentication TLS context, see Configure Peer Authentication TLS Context, on page 48.
   d Import root certificate of the Certificate Authority (CA), see Import Root Certificate of Certificate Authority, on page 48.
   e Request a CA signed certificate, see Generate Certificate Signing Request for IM and Presence Service, on page 49.
   f Import the CA signed certificate, see Import Signed Certificate from Certificate Authority, on page 50.

6 (Optional) If you are configuring a dedicated Routing IM and Presence Service node, deactivate unnecessary feature services on the Routing IM and Presence Service node, see Deactivate Feature Services on the Routing IM and Presence Service Node, on page 51.

LCS Configuration

1 Verify that the domain for Intradomain federation that is configured on the LCS server has matching domains configured on the IM and Presence Service nodes.

2 Enable port 5060, see Enable Port 5060 on LCS Server, on page 83.

3 Configure static routes to the IM and Presence Service deployment, see Configure a LCS Static Route to Point to the IM and Presence Service, on page 84.

4 Add host authorization for the IM and Presence Service deployment, see Add Host Authorization on LCS for IM and Presence Service, on page 85.

5 (Optional) Configure TLS encryption between the IM and Presence Service and LCS:

   a Ensure mutual TLS authentication is configured on each LCS server, see Configure Mutual TLS Authentication on LCS, on page 88.
   b Ensure CA root certificates are installed on each LCS server, see Install Certificate Authority Root Certificates on LCS, on page 88.
   c Ensure all LCS servers have the required signed certificates, see Validate Existing LCS Signed Certificate, on page 90.
   d If required, request a newly signed certificate, see Signed Certificate Requests from Certificate Authority for LCS Server, on page 91.

6 Restart services, see Restart Services on LCS Servers, on page 86.

Tip Plan the restart of the server front-end services during off-peak hours to minimize the impact to users.

After the server is configured, you can proceed to migrate the users.

Configuration Workflow for User Migration from Microsoft Servers to the IM and Presence Service

Use the following workflow to migrate users from Lync/OCS/LCS toIM and Presence Service:

1 Download the user migration tools—see Cisco User Migration Tools, on page 95.

2 Set unlimited contact list sizes and watcher sizes onIM and Presence Service, see Set Unlimited Contact Lists and Watchers, on page 96.

3 Enable automatic authorization of subscription requests, see Enable Automatic Authorization of Subscription Requests, on page 97.

4 Provision migrating users on IM and Presence Service, see Provision of Microsoft Server Users on Cisco Unified Communications Manager.

5 Back up Microsoft server data for migrating users, see Backups of User Microsoft Server Contact List Information.

6 Export Microsoft server contact lists for migrating users, see Export of Contact Lists for Migrating Users, on page 100.

7 Disable Microsoft server accounts for migrating users, see Disable Users on Microsoft Servers.

8 Verify that Microsoft server accounts have been disabled for migrating users, see Verify That Active Directory Updates Synchronized to Microsoft Servers.

9 Delete Microsoft server user data for migrating users, see Delete User Data from Database for Migrating Users, on page 108.

10 Import contact lists into IM and Presence Service for migrating users, see Import Contact Lists for Migrating Users into IM and Presence, on page 110.

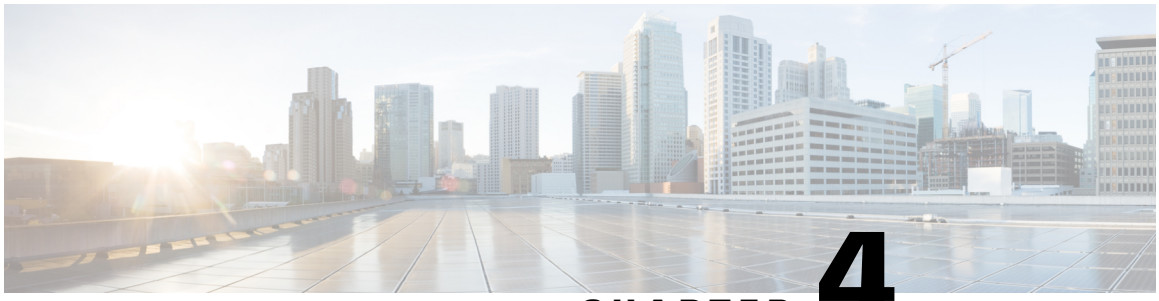
11 Reset the contact list and watcher limits on IM and Presence Service, see Reset Maximum Contact List Size and Maximum Watcher Size, on page 112.

Configuration Workflow for Integrating IM and Presence with Microsoft Server Interdomain Federation Capability

Note Before you begin this workflow, you must configure partitioned intradomain federation with Lync/OCS/LCS and ensure that it is functioning correctly. See the appropriate workflow for configuring partitioned intradomain federation within your deployment.

1 Configure each federated presence domain on IM and Presence Service—see Remote Domain Setup for Interdomain Federation through Intradomain Federation Connections on Microsoft Servers, on page 116

2 Configure static routes to each server hosting a remote presence domain on IM and Presence Service—see Configure a Static Route for a Remote Domain, on page 117



CHAPTER 4

IM and Presence Service Node Configuration for Partitioned Intradomain Federation

- Configure Partitioned Intradomain Federation Options, page 41
- Configure Static Routes, page 42
- Configure an Incoming Access Control List, page 44
- TLS Encryption Configuration, page 45
- Deactivate Feature Services on the Routing IM and Presence Service Node, page 51

Configure Partitioned Intradomain Federation Options

The following procedure describes how to enable partitioned intradomain federation on IM and Presence Service and choose a routing mode.

If you have a multicluster deployment, you must perform this procedure on each cluster. When you enable partitioned intradomain federation or choose a routing mode, these settings are enabled cluster-wide; therefore you only need to enable them on the IM and Presence Service publisher node within any given cluster.

Caution Email Address for Federation is not supported in deployments where Partitioned Intradomain Federation is configured. Email Address for Federation is also not supported for Interdomain Federation if your deployment uses the interdomain federation capabilities of Lync/OCS/LCS. Confirm that Email Address for Federation is not enabled anywhere in the deployment in these deployment scenarios and ensure that the **Enable use of Email Address when Federating** option is not checked for the clusters.

Procedure

Step 1 Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Presence** > **Settings> Standard Configuration**.

Step 2 Check the **Enable Partitioned Intradomain Federation with LCS/OCS/Lync** check box.

Step 3 Read the warning message and click **OK**.

Step 4 Choose one of the following from the partitioned intradomain federation Routing Mode drop-down list:

- **Basic Routing Mode (default)** when you have unlicensed IM and Presence Service request recipients within the IM and Presence Service domain. In Basic Routing mode, the IM and Presence Service routes requests for these recipients to the Microsoft server.
- **Advanced Routing Mode** when you have request recipients within the IM and Presence Service domain who are licensed and have a valid Microsoft Lync or Microsoft Office Communicator SIP address stored in the IM and Presence Service database. Choose Advanced Routing only if Cisco Unified Communications Manager synchronizes users from the same Active Directory that the Microsoft server uses.

  Note The list of users synchronized from Active Directory must include all Microsoft Lync or Microsoft Office Communicator users.

Step 5 Click **Save**.

Step 6 After you enable partitioned intradomain federation or choose a routing mode, you must restart the Cisco XCP Router on all IM and Presence Service nodes in the cluster. To restart the Cisco XCP Router, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Network Services**. Click the appropriate IM and Presence Service node, scroll down and select Cisco XCP Router, and click restart.

Note You are prompted to restart the SIP proxy when you enable partitioned federation.

Related Topics

IM and Presence to Microsoft Server Request Routing, on page 11

Configure Static Routes

The following procedure describes how to configure static routes to enable partitioned intradomain federation routing between the IM and Presence Service and Lync/OCS/LCS. You must add an individual static route for each Microsoft server presence domain. Static routes can have a common next hop address. See topics related to IM and Presence Service to Microsoft server request routing, and basic and advanced routing modes for more information.

Note If you are integrating partitioned intradomain federation with the interdomain federation capabilities of Microsoft servers, then you must configure static routes on the IM and Presence Service for each remote domain. For more information, see topics related to configuring static routes for remote domains.

For the Microsoft server presence domain static route, note the following:

- For Standard Edition Microsoft servers, the static route must point to the IP address of a specific Standard Edition server.
- For Enterprise Edition Microsoft servers, to route federation traffic from the IM and Presence Service cluster directly to one of the front-end Microsoft servers, the static route must point to the IP address of that front-end server

See the following URL for a list of approved load balancers: http://technet.microsoft.com/en-us/office/ocs/cc843611. It is your responsibility to ensure that those load balancers are deployed and managed correctly.

Note Cisco does not support the configuration of static routes to point to load balancers. Cisco recommends that you configure static routes to bypass the front-end load balancer.

For high availability purposes, you can configure additional backup static routes for each Microsoft server presence domain.

The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service database publisher node within any given cluster.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence** > **Routing** > **Static Routes**.

Step 2 Click **Add New**.

Step 3 Enter the Destination Pattern value so that the domain is reversed. For example, if the domain is domaina.com, the Destination Pattern value must be .com.domaina

Step 4 Enter the IP address of the Microsoft server in the Next Hop field.

Step 5 Choose **domain** for the Route Type.

Note The default setting for Route Type is user.

Step 6 Set the Next Hop Port and the Protocol Type as follows:

- For TLS Encryption:
  - Next Hop Port number is **5061**
  - Protocol Type is **TLS**
- For TCP:
  - Next Hop Port number is **5060**
  - Protocol Type is **TCP**

Step 7 Enter the Priority value as follows:

- For primary static routes, enter the default Priority value of **1**.
- For backup static routes, enter a Priority value of greater than 1. (The lower the value, the higher the priority of the static route).

Step 8 Leave the default values for all other parameters.

Step 9 Click **Save**.

What to Do Next

Create an additional static route with the Destination Pattern FQDN in reverse order and with the Next Hop the Microsoft Lync server IP address. For example, if the domain is lyncserver.domaina.com, the Destination Pattern value must be .com.domaina.lyncserver

Configure an Incoming Access Control List

The following procedure describes how to configure entries in the Incoming Access Control List (ACL) to ensure that Lync/OCS/LCS servers can access the IM and Presence Service server without authentication.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

How you configure the Incoming ACLs depends on how strictly you wish to control access to IM and Presence Service:

- To allow open access to IM and Presence Service, you can add an entry with an address pattern of **All**.
- To allow access to IM and Presence Service from specific DNS domains, you can add entries with an address pattern matching the specific DNS domain. For example, to allow access from any server within the foo.com DNS domain, enter **foo.com** as the address pattern.
- To allow access to IM and Presence Service from specific servers, add ACL entries that have an address pattern matching the IP address and the FQDN of those servers. You must create two ACL entries for each server: one entry for the IP address and another entry for the FQDN. For example, to allow access from the server ocs1.foo.com (10.1.10.100) enter **ocs1.foo.com** as the address pattern in one ACL entry, and enter **10.1.10.100** as the address pattern in another ACL entry.

For partitioned intradomain federation, if you decide to restrict access to IM and Presence Service for certain Microsoft server FQDNs or IP addresses only, you must add ACL entries for the following entities:

- Each Microsoft server Enterprise Edition front-end or Standard Edition server
- Each Microsoft server pool FQDN (Enterprise Edition only)

If you choose to restrict access using the FQDN of the server, then you need to also add an ACL entry for any other DNS records that resolve to the same IP address as any of the front end servers or pools. For example,

you can create a DNS record, such as admin.lync.com, on the Lync server to access the Lync control panel and which resolves to the same IP address as one of the Lync front end servers.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System** > **Security** > **Incoming ACL**.

Step 2 Click **Add New**.

Step 3 In the Description field, enter a description of the entry, for example, Lync Server.

Step 4 Enter the address pattern in the **Address Pattern** field. You have the following options:

- Enter **Allow from all** to allow open access to IM and Presence Service
- Enter a specific network domain name. For example, **Allow from foo.com**
- Enter a specific IP address. For example, **Allow from 10.1.10.100**
- Enter a specific FQDN. For example, **Allow from admin.lync.com**

Note If you do not enter **Allow from All** as the address pattern, then you must create at least two ACL entries: one for the IP address of the server and another one for the FQDN of the server. Entering a domain name is optional.

e > Routing > Settings > Restart All Proxy Services.

Step 5 Click **Save**.

Step 6 Restart the SIP Proxy. Go to **Presence** > **Routing** > **Settings** > **Restart All Proxy Services.**

TLS Encryption Configuration

You must complete the procedures in this section to configure TLS encryption between IM and Presence Service and Lync/OCS/LCS. TLS encryption is mandatory for partitioned intradomain federation with Lync servers.

Note If you have a multicluster deployment, you must perform each of these procedures on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

Configure Application Listener Ports

You must change the Default Cisco SIP Proxy TLS Listener port values for both server authentication and peer authentication.IM and Presence Service performs peer (mutual) TLS authentication on port 5062 by default. You must modify this default setting so that peer TLS authentication takes place on port 5061 and configure the server TLS authentication port value to 5062.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Application Listeners**.

Step 2 If they are not already displayed, click **Find** to display all application listeners.

Step 3 Choose **Default Cisco SIP Proxy TLS Listener – Server Auth**.

Step 4 Change the Port value to **5063**.

Step 5 Click **Save** and click **OK** on the pop-up window that appears.

Step 6 From the Related Links drop-down list, choose **Back to Find/List** and click **OK** to return to the Application Listeners list.

Step 7 Choose **Default Cisco SIP Proxy TLS Listener – Peer Auth**.

Step 8 Change the Port value to **5061**.

Step 9 Click **Save** and click **OK** on the dialog-box that appears.

Step 10 From the Related Links drop-down list, choose **Back to Find/List** and click **OK** to return to the Application Listeners list.

Step 11 Choose **Default Cisco SIP Proxy TLS Listener – Server Auth**.

Step 12 Change the Port value from **5063** to **5062**.

Step 13 Click **Save**.

Step 14 Restart the SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the SIP Proxy service, Log in to the **Cisco Unified IM and Presence Serviceability** user interface, choose **Tools** > **Control Center – Feature Services**.

What to Do Next

Configure TLS Peer Subjects, on page 46

Related Topics

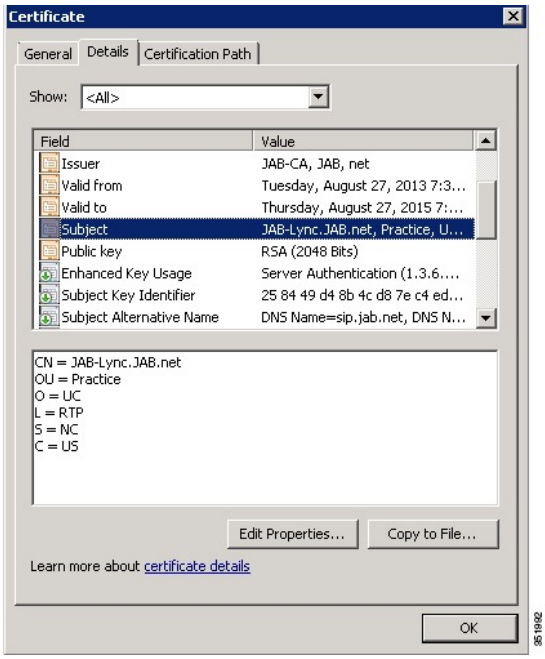
Integration Troubleshooting, on page 121

Configure TLS Peer Subjects

For Peer TLS authentication, IM and Presence Service requires that the Subject Common Name (CN) from the security certificate that is presented by the peer is included in a TLS Peer Subject list. Use the **Cisco Unified IM and Presence Administration** user interface to add a Subject CN to this list.

Include only the Subject CN in the TLS Peer Subject list. Do not include Subject Alternative Name (SAN) entries in the TLS Peer Subject list. The following figure shows an example of a Subject CN certificate with the Subject CN highlighted.

Figure 9: Subject Common Name Certificate



For partitioned intradomain federation, you must add a TLS Peer Subject for the following entities:

- Each Lync/OCS/LCS Enterprise Edition front-end or Standard Edition server
- Each Lync/OCS/LCS pool Fully Qualified Domain Name (FQDN) (Enterprise Edition only)

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Security** > **TLS Peer Subjects**.

Step 2 Click **Add New**.

Step 3 Enter the Peer Subject Name.

- For a Microsoft server Enterprise Edition front-end or Standard Edition server, enter the FQDN of the server.
- For a Microsoft server pool Fully Qualified Domain Name (FQDN), enter the subject CN of the certificate that is presented to the IM and Presence Service.

Step 4 In the Description field, enter a description of the subject, for example, OCS Server.

Step 5 Click **Save**.

Step 6 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose

Tools > **Control Center - Feature Services**. Click the CUCM IM and Presence Server, select **SIP Proxy** and click **Restart**.

What to Do Next

Configure Peer Authentication TLS Context, on page 48

Related Topics

Integration Troubleshooting, on page 121

Configure Peer Authentication TLS Context

To support TLS encryption between IM and Presence Service and Lync/OCS/LCS, you must modify Peer Authentication TLS Context configuration on IM and Presence Service.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **System** > **Security** > **TLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Click the link for **Default Cisco UP SIP Proxy Peer Auth TLS Context**.

Step 4 Ensure that the check box for **Disable Empty TLS Fragments** is checked.

Step 5 In the TLS Cipher Mapping area list of Available TLS Ciphers, choose all of the ciphers and click the **Move Right** arrow to move these ciphers to the Selected TLS Ciphers list.

Step 6 In the TLS peer Subject Mapping area list of Available TLS Peer Subjects, choose the TLS peer subject that you configured in Configure TLS Peer Subjects, on page 46 and click the **Move Right** arrow to move this TLS peer subject to the Selected TLS Peer Subjects list.

Step 7 Click **Save**.

Step 8 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Feature Services**. Click the CUCM IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

What to Do Next

Import Root Certificate of Certificate Authority, on page 48

Related Topics

Integration Troubleshooting, on page 121

Import Root Certificate of Certificate Authority

All Lync/OCS/LCS security certificates are generally signed by a Certificate Authority (CA). The IM and Presence Service certificates should also be signed by the same Certificate Authority used by the Microsoft

server. In order for the IM and Presence Service to use a certificate signed by the Microsoft server CA, and to accept Microsoft server certificates signed by that same CA, the root certificate of the CA must be uploaded into the IM and Presence Service trust store.

Before You Begin

Before importing the root certificate, retrieve the certificate from the certificate authority and copy it to your local computer.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence OS Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/ Certificate Chain**.

Step 3 For the Certificate Purpose drop-down list, choose **cup-trust**.

Step 4 In the Description (friendly name) field, enter a description for the certificate, for example, Certificate Authority Root Certificate.

Step 5 Click **Browse** to find the root certificate on your local computer.

Step 6 Click **Upload** to upload the certificate to the IM and Presence Service node.

Step 7 Restart the Cisco SIP Proxy service on all IM and Presence Service nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the Cisco Unified IM and Presence Serviceability user interface and choose **Tools** > **Control Center – Feature Services**. Click the CUCM IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

What to Do Next

Generate Certificate Signing Request for IM and Presence Service, on page 49

Related Topics

Integration Troubleshooting, on page 121

Generate Certificate Signing Request for IM and Presence Service

IM and Presence Service certificates should be signed by the same Certificate Authority (CA) that is used by Lync/OCS/LCS. You must complete the following two-step process to obtain a CA-signed certificate:

1 Generate an IM and Presence Service Certificate Signing Request (CSR).

2 Upload the CA signed certificate onto IM and Presence Service.

The following procedure describes how to generate and download a CSR from IM and Presence Service. IM and Presence Service CSRs are 2048 bit in size.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Security** > **Certificate Management** on IM and Presence Service.
Step 2 Click **Generate CSR**.
Step 3 From the Certificate Purpose drop-down list, choose **cup**.
Step 4 Click **Generate CSR**.
Step 5 When the Status shows "Success: Certificate Signing Request Generated" click **Close**.
Step 6 Click **Download CSR**.
Step 7 From the Certificate Name drop-down list, choose **cup**.
Step 8 Click **Download CSR** to download the certificate to your local computer.
Step 9 After the certificate has downloaded, click **Close**.

What to Do Next

After you download the CSR, you can use it to request a signed certificate from your chosen CA. This can be a well-known public CA or an internal CA.

Import Signed Certificate from Certificate Authority, on page 50

Related Topics

Integration Troubleshooting, on page 121

Import Signed Certificate from Certificate Authority

The following procedure describes how to upload the CA signed certificate to IM and Presence Service.

Before You Begin

Generate and download a CSR from IM and Presence Service. See Generate Certificate Signing Request for IM and Presence Service, on page 49.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain** and the Upload Certificate/Certificate chain dialog box opens.
Step 3 From the Certificate Name drop-down list, choose **cup**.
Step 4 In the Description (friendly name) field, enter a description of the certificate, for example, CA Signed Certificate.
Step 5 Click **Browse** to find the certificate file on your local computer.
Step 6 Click **Upload** to upload the certificate to the IM and Presence Service node.
Step 7 After the certificate has uploaded, restart the Cisco SIP Proxy service on all IM and Presence nodes in the cluster. To restart the Cisco SIP Proxy service, log in to the **Cisco Unified IM and Presence Serviceability**

user interface. Choose **Tools** > **Control Center – Feature Services**. Click the CUCM IM and Presence Service server, select **Cisco SIP Proxy** and click **Restart**.

Related Topics

Integration Troubleshooting, on page 121

Deactivate Feature Services on the Routing IM and Presence Service Node

To ensure that a Routing IM and Presence Service node has the capacity to handle SIP traffic from Lync/OCS/LCS, you must not assign any users to the Routing IM and Presence Service node. This means that a number of the IM and Presence Service feature services that support assigned users can be deactivated on the Routing IM and Presence Service node. When you deactivate these services, the Routing IM and Presence Service node has extra processing capacity to support its SIP routing role. The following procedure describes how to deactivate feature services.

Restriction The following section only applies when there is a dedicated IM and Presence Service node used only for routing of federation traffic (not used for Jabber login). This routing IM and Presence Service node is separate from an IM and Presence Service node deployed for Cisco Jabber login.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the Routing IM and Presence Service node.

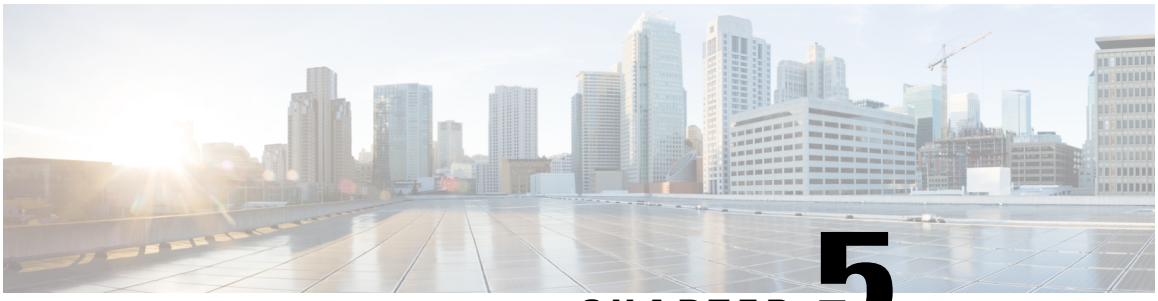
Step 3 Uncheck each of the following feature services check boxes:

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver
- Cisco XCP Directory Service
- Cisco XCP Authentication Service

Step 4 Click **Save**.

Related Topics

Additional Configuration for Routing IM and Presence Service Node, on page 32



CHAPTER 5

Microsoft Lync Configuration for Partitioned Intradomain Federation

To configure Microsoft Lync for partitioned Intradomain federation, you must complete the following procedures in the order they are presented. After the configuration is complete, you must restart services on Lync servers.

Note You must configure TLS for Partitioned Intradomain Federation with Lync. TCP is not supported by Lync.

- Domain Verification for Lync Servers, page 54
- Federated Link to Microsoft Lync Server Configuration Task Lists, page 54
- Configure a Static Route on Microsoft Lync for Federation, page 56
- Add Host Authorization for IM and Presence Service on an Enterprise Edition Lync Server, page 58
- Add Host Authorization for IM and Presence Service on Standard Edition Lync Servers, page 60
- Publish Topology, page 62
- Install Certificate Authority Root Certificates on Lync, page 63
- Validate Existing Lync Signed Certificate, page 64
- Request a Signed Certificate from a Certificate Authority for Lync, page 65
- Download a Certificate from the CA Server, page 66
- Import a Signed Certificate for Lync, page 67
- Assign Certificate on Lync, page 68
- Restart Services on Lync Servers, page 68

Domain Verification for Lync Servers

Before you proceed to set up IM and Presence Service for partitioned intradomain federation, verify that there are matching presencer domains configured on the Microsoft Lync servers and all nodes in the IM and Presence Service cluster.

Federated Link to Microsoft Lync Server Configuration Task Lists

This section provides an overview of the end-to-end steps to configure federated links between IM and Presence Service and Microsoft Lync servers.

The following table provides an overview of the steps to configure static routes for federated links between IM and Presence Service nodes and Microsoft Lync servers. You must configure TLS static routes between IM and Presence Service and Microsoft Lync for federation. For more information about configuring static routes used for federated links to Microsoft Lync servers, see https://technet.microsoft.com/en-us/library/gg615051.aspx.

Table 17: Task List to Configure Static Route for Federated Link to Microsoft Lync Server

Step	Description
Configure a static route on IM and Presence Service	Create a static route on IM and Presence Service for the Lync server. Select TLS as the Protocol Type and 5061 as the Next Hop Port number.
Configure a static route on Lync for IM and Presence Service	Create a static route on the Lync server for IM and Presence Service. You must create the static route only to the IM and Presence Service routing node - or publisher node if no node is configured as a Router node. Do not create static routes to subscriber nodes or any intercluster peer nodes, even if your IM and Presence Service deployment has multiple clusters. **Note** For TLS, theIM and Presence Service Peer Auth Listener port is by default set to 5062. You must switch the Peer Auth Listener port to 5061 to align with the Microsoft server's static route. However, the Server Auth Listener port is by default 5061, so this must be changed to another port. To configure the IM and Presence Service Peer Auth Listener port to use port 5061 and change Server Auth Listener port. Log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Application Listeners**. • Verify that the Peer Auth Listener port is 5061. • If the Server Auth Listener port is configured as 5061 you must change it to another value, for example 5063.
Persist the route	This step is only necessary for the routing node.

After you have configured your static routes, proceed to configure host authorization and publish the topology. The following table lists the tasks to set up host authorization and publish the topology.

Table 18: Task List for Host Authorization Setup and Publishing the Topology

Step	Description
Create trusted application pool	For Enterprise Edition, you create a single trusted application pool to store the trusted application computers for the IM and Presence Service nodes. For Standard Edition, you must create a trusted application pool for each IM and Presence Service node.
Add trusted application computer to the created pool	Add a trusted application computer to the created pool for each IM and Presence Service node, except for the routing IM and Presence Service node. Perform this step only for Enterprise Edition deployments.
Add trusted application server to the created pool	For Enterprise Edition, add an application server to the pool that was created for the IM and Presence Service deployment. For Standard Edition, add an application server to each pool that was created for the nodes.
Enable the topology	Before you enable the topology, ensure that you have completed the following: • Define a TLS route for the routing IM and Presence Service node. • Persist the new static route for the routing IM and Presence Service node. • Create a trusted application pool for the IM and Presence Service deployment. • Add a trusted application computer to the created pool for each IM and Presence Service node. • Add a trusted application server to the created pool for the IM and Presence Service deployment.

You must add CA-signed certificates to the Microsoft Lync server and IM and Presence Service node.

Table 19: Task List to Configure Certificates on the Microsoft Lync Server and IM and Presence Service Node

Step	Description
Configure the certificates on each Lync server	To retrieve the CA root certificate and the Lync signed certificate, perform the following steps: • Download and install the CA certificate chain. • Request a signed certificate from the CA server. • Import and assign the certificate on Lync. See the Microsoft Lync documentation for details to import and assign the certificate on the Lync server: http://technet.microsoft.com/en-us/library/gg558664.aspx.
Configure certificates on IM and Presence Service	You must upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. As well, generate a CSR for IM and Presence Service and have it signed by the CA. Then upload the CA-signed certificate to IM and Presence Service. You must then add a TLS peer subject on IM and Presence Service for the Lync server. See topics related to setting up certificates for detailed instructions.

Configure a Static Route on Microsoft Lync for Federation

IM and Presence Service supports Transport Layer Security (TLS) for federation with Microsoft Lync servers. You must create a static route to the IM and Presence Service routing node only. It is not necessary to create static routes to subscriber nodes, nor any intercluster peer nodes even if your IM and Presence Service deployment has multiple clusters.

The following table lists the sample configuration parameters that are used in this procedure.

Table 20: Sample Parameters for TLS Static Route on Microsoft Lync

Description	Sample Parameters
IM and Presence Service node FQDN (routing IM and Presence Service node) Ensure the FQDN can resolve to the correct IP address.	impserverPub.sip.com
IM and Presence Service node IP address (routing IM and Presence Service node)	10.10.1.10

Description	Sample Parameters
IM and Presence Service node TLS port The TLS port value must match what is configured in the user interface. To check the value, log in to the **Cisco Unified CM IM and Presence Administration** user interface and choose **System** > **Application Listeners** > **Default Cisco SIP Proxy TLS Listener - Peer Auth**. **Note** Cisco recommends port 5061; however, you can use port 5062.	5061
IM and Presence Service node domain	sip.com
Lync Registrar server	lyncserver.synergy.com

Note

- When using Transport Layer Security (TLS), the FQDN used in the destination pattern of the static route must be resolvable from the Lync front-end server. Ensure that the FQDN resolves to the IP address of the IM and Presence Service node to which the static route points.
- The Lync FQDN cannot match the IM and Presence Service domain that is used for partitioned intradomain federation.

Procedure

Step 1 Log in to a computer as the domain administrator, for example, where Lync Server Management Shell is installed.

Tip You must log in as a member of the RTCUniversalServerAdmins group or a role-based access control (RBAC) role to which you have assigned the **New-CsStaticRoute** cmdlet.

Step 2 Choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.

Step 3 Enter the following command to define a TLS route:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination fqdn_of_imp_routing_node -Port
listening_port_imp_routing_node -usedefaultcertificate $true -MatchUri destination_domain
```

Example:

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination impserverPub.sip.com -Port 5061
-usedefaultcertificate $true -MatchUri sip.com
```

where:

Parameter	Description
-Destination	The FQDN of the IM and Presence Service routing node.
-Port	The listening port of the IM and Presence Service routing node.
-MatchUri	The destination IM and Presence Service domain.

Note

- To match child domains of a domain, you can specify a wildcard value in the `-MatchUri` parameter, for example, *.sip.com. That value matches any domain that ends with the suffix sip.com.
-
- If you set `-usedefaultcertificate` to false, you must specify the TLSCertIssuer and TLSCertSerialNumber parameters. These parameters indicate the name of the certificate authority (CA) that issues the certificate used in the static route and the serial number of the TLS certificate, respectively. See the Lync Server Management Shell for more information about these parameters.

Step 4 Make the newly created static route persistent in the Central Management store. Enter the following command:

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

Note Perform this step only for the routing IM and Presence Service node.

Step 5 If you made the new static route persistent, verify that the command was successful. Enter the following command:

```
Get-CsStaticRoutingConfiguration | select-object -ExpandProperty Route
```

Step 6 Open the Lync control panel; in the **External User Access** area:

a) Click **New** and create a Public Provider for the domain that Lync is federating with (your IM and Presence Service domain) and the FQDN of the IM and Presence Service node.

b) In the new Public Provider, configure the Verification level of your users to Allow all communications with this provider.

Add Host Authorization for IM and Presence Service on an Enterprise Edition Lync Server

To allow Lync to accept SIP requests from IM and Presence Service without being prompted for authorization, you must configure host authorization entries on Lync for each IM and Presence Service node. For Enterprise Edition, you must perform this procedure on all pools.

Note You must configure TLS for partitioned intradomain federation with Lync. TCP is not supported.

To configure the required host authorization entries for TLS encryption between Lync and IM and Presence Service, you must add a host authorization entry for the FQDN of each IM and Presence Service node.

Procedure

Step 1 Create a trusted application server pool for the IM and Presence Service deployment using the following commands:

Tip You can enter `Get-CsPool` to verify the FQDN value of the Registrar service for the pool.

```
New-CsTrustedApplicationPool -Identity trusted_application_pool_name_in FQDN_format -Registrar
Lync_Registrar_service_FQDN -Site ID_for_the_trusted_application_pool_site
-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly
$false -Computerfqdn first_trusted_application_computer
```

Example:

```
New-CsTrustedApplicationPool -Identity trustedpool.sip.com -Registrar lyncserver.synergy.com
-Site 1 -TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false
-OutboundOnly $false -Computerfqdn impserverPub.sip.com
```

where:

Parameter	Description
-Identity	Enter the name of the trusted application pool for the IM and Presence Service deployment. This must be in FQDN format. For example: `trustedpool.sip.com`. **Tip** Ignore warning messages regarding the machine not found in Active Directory and proceed to apply the changes.
-Registrar	The service ID or FQDN of the Registrar service for the pool. For example: `lyncserver.synergy.com`. You can check this value using the command **Get-CsPool**.
-Site	The numeric value of the site where you want to create the trusted application pool. **Tip** Use the **Get-CsSite** Management Shell command.
-Computerfqdn	The FQDN of the IM and Presence Service routing node. For example: `impserverPub.sip.com`. • impserverPub = the IM and Presence Service hostname. • sip.com = the IM and Presence Service domain.

Step 2 For each IM and Presence Service node, enter the following commands to add the FQDN of the node as a trusted application computer to the new application pool:

```
New-CsTrustedApplicationComputer -Identity imp_FQDN -Pool new_trusted_app_pool_FQDN
```

Example:

```
New-CsTrustedApplicationComputer -Identity impserver2.sip.com -Pool trustedpool.sip.com
```

where:

Parameter	Description
-Identity	The FQDN of the IM and Presence Service node. For example: `impserver2.sip.com`. **Note** Do not add the IM and Presence Service routing node as a trusted application computer using this command.

Parameter	Description
-Pool	The FQDN of the trusted application pool that is used for the IM and Presence Service deployment. For example: `trustedpool.sip.com`.

Step 3 Enter the following command to create a new trusted application and add it to the new application pool:

New-CsTrustedApplication -ApplicationID *new_application_name* **-TrustedApplicationPoolFqdn** *new_trusted_app_pool_FQDN* **-Port 5061**

Example:

New-CsTrustedApplication -ApplicationID *imptrustedapp.sip.com* **-TrustedApplicationPoolFqdn** *trustedpool.sip.com* **-Port 5061**

where:

Parameter	Description
-ApplicationID	The name of the application. This can be any value. For example: imptrustedapp.sip.com.
-TrustedApplicationPoolFqdn	The FQDN of the trusted application pool server for the IM and Presence Service deployment. For example: `trustedpool.sip.com`.
-Port	The SIP listening port of the IM and Presence Service node. For TLS the port is 5061.

What to Do Next

Proceed to publish the topology.

Related Topics

Integration Troubleshooting, on page 121

Add Host Authorization for IM and Presence Service on Standard Edition Lync Servers

To allow Lync to accept SIP requests from IM and Presence Service without being prompted for authorization, you must configure host authorization entries for each IM and Presence Service node on all Standard Edition Lync servers in your deployment. Create one trusted application pool for each IM and Presence Service node on the Lync server.

Note You must configure TLS for partitioned intradomain federation with Lync. TCP is not supported.

To configure the required host authorization entries for TLS encryption between Lync and IM and Presence Service, you must add a host authorization entry for the FQDN of each IM and Presence Service node.

Procedure

Step 1 Create a trusted application server pool for each IM and Presence Service node using the following commands:

Tip You can enter **Get-CsPool** to verify the FQDN value of the Registrar service for the pool.

New-CsTrustedApplicationPool -Identity *fqdn_of_the_im_and_presence_service_node* **-Registrar** *fqdn_of_the_lync_registrar_service* **-Site** *site_id_for_where_you_want_to_create_trusted_app_pool* **-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false**

Example:

New-CsTrustedApplicationPool -Identity *impserverPub.sip.com* **-Registrar** *lyncserver.synergy.com* **-Site** *1* **-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false**

where:

Parameter	Description
-Identity	Enter the FQDN name of the IM and Presence Service node as the trusted application pool. For example: `impserverPub.sip.com`. **Tip** Ignore warning messages regarding the machine not found in Active Directory and proceed to apply the changes.
-Registrar	The service ID or FQDN of the Registrar service for the pool. For example: `lyncserver.synergy.com`. You can check this value using the command **Get-CsPool**.
-Site	The numeric value of the site where you want to create the trusted application pool. **Tip** Use the **Get-CsSite** Management Shell command.

Step 2 For each IM and Presence Service node, enter the following commands to create a trusted application for the node and then assign it to the trusted application server pool of that node.

New-CsTrustedApplication -ApplicationID *new_app_name* **-TrustedApplicationPoolFqdn** *new_trusted_app_pool_fqdn* **-Port 5061**

Example:

New-CsTrustedApplication -ApplicationID *imptrustedapp.sip.com* **-TrustedApplicationPoolFqdn** *impserverPub.sip.com* **-Port 5061**

where:

Parameter	Description
-ApplicationID	The application ID of the trusted application computer, which can also be the FQDN of the node. For example: `impserverPub.sip.com`.
-TrustedApplicationPoolFqdn	The FQDN of the trusted application pool that is used for the IM and Presence Service node. For example: `impserverPub.sip.com`.
-Port	The SIP listening port of the IM and Presence Service node. For TLS the port is 5061.

What to Do Next

Publish Topology, on page 62

Related Topics

Integration Troubleshooting, on page 121

Publish Topology

The following procedure describes how to commit the topology.

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 `topology.xml` and save it to the C drive:
```
Get-CsTopology -AsXml | Out-File C:\topology.xml
```
Note You can choose any name and location to output the topology information.

Step 3 Open the `topology.xml` file.

Step 4 In the Cluster Fqdn section, change the IPAddress parameter from "*0.0.0.0*" to the IP Address for each IM and Presence Service node that you added to the trusted pool.

Step 5 Save the `topology.xml` file.

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

What to Do Next

Install Certificate Authority Root Certificates on Lync, on page 63

Install Certificate Authority Root Certificates on Lync

TLS configuration must be used for partitioned intradomain federation between the IM and Presence Service and Lync servers. TCP cannot be used. To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate. This signed certificate, along with the root certificate of the Certificate Authority (CA) that signed the certificate, must be installed on each Lync server.

Cisco recommends that Lync and IM and Presence Service servers share the same CA. If not, the root certificate of the CA that signed the IM and Presence Service certificates must also be installed on each Lync server.

Generally, the root certificate of the Lync CA is already installed on each Lync server. Therefore, if Lync and IM and Presence Service share the same CA, there may be no need to install a root certificate. However, if a root certificate is required, see the following details.

If you are using Microsoft Certificate Authority, refer to the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for information about installing the root certificate from the Microsoft Certificate Authority onto Lync:

- Downloading the CA Certification Chain
- Installing the CA Certification Chain

If you are using an alternative CA, the following procedure is a generic procedure for installing root certificates onto Lync servers. The procedure for downloading the root certificate from the CA differs depending on your chosen CA.

Note The *Integration Guide for Configuring IM and Presence Service for Interdomain Federation* document refers to the Access Edge Server. For partitioned intradomain federation, you can replace references to the Access Edge Server with Lync Standard Edition server or Enterprise Edition front-end server.

Before You Begin

Download the root certificate or certificate chain from your CA and save it to the hard disk of your Lync server.

Procedure

Step 1 On your Lync server, choose **Start** > **Run**.
Step 2 Enter mmc and click **OK.**
Step 3 From the **File** menu, choose **Add/Remove Snap-in**.
Step 4 From the **Add/Remove Snap-in** dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account**, and then click **Next**.
Step 7 In the **Select Computer** dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Trusted Root Certification Authorities**.
Step 11 Right-click **Certificates** and choose **All Tasks**.
Step 12 Click **Import.**
Step 13 In the Import Wizard, click **Next**.
Step 14 Click **Browse** and navigate to where you saved the root certificate or certificate chain.
Step 15 Choose the file and click **Open**.
Step 16 Click **Next**.
Step 17 Leave the default value **Place all certificates in the following store** and verify that **Trusted Root Certification Authorities** appears under the Certificate store.
Step 18 Click **Next** and then click **Finish**.
Step 19 Repeat Step 11 to Step 18 as necessary for other CAs.

What to Do Next

Validate Existing Lync Signed Certificate, on page 64

Related Topics

Integration Troubleshooting, on page 121

Validate Existing Lync Signed Certificate

To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate that supports Client Authentication. If a signed certificate is already installed on the Lync server, the following procedure describes how to check if that existing signed certificate supports Client Authentication.

Verify that the certificate is assigned one of the following OID values:

- If the certificate is configured for both server and client authentication, the OID value is “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”
- If the certificate is configured for server authentication only, the OID value is “1.3.6.1.5.5.7.3.1”

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On your Lync server, choose **Start** > **Run**.
Step 2 Enter mmc and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the **Add/Remove Snap-in** dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the **Select Computer** dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal** and choose **Certificates**.
Step 11 Find the signed certificate currently used by Lync in the right pane.
Step 12 Verify that **Client Authentication** is listed in the Intended Purposes column.

What to Do Next

Request a Signed Certificate from a Certificate Authority for Lync, on page 65

Related Topics

Integration Troubleshooting, on page 121

Request a Signed Certificate from a Certificate Authority for Lync

To support TLS encryption between IM and Presence Service and Lync, each Lync server must have a signed security certificate that supports Client Authentication and Server Authentication. The following procedure outlines how to request a newly signed certificate from the Certificate Authority (CA) and install it onto a Lync server.

The following procedure is based on a Windows Server 2003 certification authority. The procedure may be slightly different on other Windows server versions.

Note The CA must have a certificate template that supports client authentication and server authentication Extended Key Usage (EKU), and this template must be used to sign the certificate.

Verify that the certificate is assigned one of the following OID values before you install the certificate onto a Lync server:

- If the certificate is configured for both server and client authentication, the OID value is "1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2"
- If the certificate is configured for server authentication only, the OID value is "1.3.6.1.5.5.7.3.1"

Tip If a specific template type is not specified when you generate the Certificate Signing Request (CSR), a default template format is used. The template type that you specify during the certificate enrollment process must match the template type that is specified in the certificate, otherwise the certificate enrollment process fails.

Procedure

Step 1 In the Lync Server Management Shell enter the following command to create the CSR file:
`Request-CsCertificate -New -Type Default -Output filename -ClientEku $true`

Note If you want to create a specific request for an internal or external certificate, use the `-Type Internal` or `-Type External` parameters instead of `-Type Default`.

If you are using a custom certificate template on your CA to sign the certificate, add the `-Template template_name` parameter to the command string.

Step 2 Log in to the Lync server and open a web browser.

Step 3 Open the following URL: `http://ca_server_IP_address/certsrv` (If it is SSL encrypted, use https instead of http.)

Step 4 Click **Request a Certificate** and then click **Advanced Certificate Request**.

Step 5 Choose **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 request file you created using a text editor.

Step 7 Select and copy all of the text from the request file and paste it into the browser in the field **Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)**:

Step 8 Click **Submit**.

What to Do Next

Download a Certificate from the CA Server, on page 66

Download a Certificate from the CA Server

Complete the following procedure to download the certificate from the CA server.

Procedure

Step 1 Log into the CA server.
Step 2 Choose **Start** > **Administrative Tools** > **Certificate Authority** to launch the CA console.
Step 3 Click **Pending Requests**.
Step 4 From the right pane, right-click on the certificate request that you submitted and choose **All Tasks** > **Issue**.
Step 5 Log into the Lync server and open a web browser.
Step 6 Open the following URL: `http://ca_server_IP_address/certsrv` (If it is SSL encrypted, use https instead of http.)
Step 7 From **View the Status of a Pending Certificate Request**, choose your certificate request.
Step 8 Download the certificate.

What to Do Next

Import a Signed Certificate for Lync, on page 67

Import a Signed Certificate for Lync

Complete the following procedure to import the signed certificate.

Before You Begin

Note Verify that the certificate is assigned one of the following OID values:

- If the certificate is configured for both server and client authentication, the OID value is "1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2"
- If the certificate is configured for Server Authentication only, the OID value is "1.3.6.1.5.5.7.3.1"

Procedure

In the Lync Server Management Shell, enter the following command to import the signed certificate:
`Import-CsCertificate -Path` *"signed_certificate_path"* **`-PrivateKeyExportable $false`**

Note If the certificate contains a private key, use the **`-PrivateKeyExportable $true`** parameter.

What to Do Next

Assign Certificate on Lync, on page 68

Related Topics

Integration Troubleshooting, on page 121

Assign Certificate on Lync

Complete the following procedure to assign the certificate.

Procedure

Step 1 Choose **Start** > **Lync Server Deployment Wizard**.
Step 2 Click **Install or Update Lync Server System**.
Step 3 Click **Run Again** to Request, Install or Assign Certificates.
Step 4 On the Certificate Wizard window, choose the default certificate.
Step 5 Click **Assign**.
Step 6 On the Certificate assignment window, click **Next**.
Step 7 Choose the imported certificate in the certificate store window and click **Next**.
Step 8 In the certificate assignment summary window click **Next**.
Step 9 On the executing commands window, wait for the task status to report **Completed** and then click **Finish**.
Step 10 Close the certificate wizard window.

What to Do Next

Restart Services on Lync Servers, on page 68

Restart Services on Lync Servers

After you complete all the configuration steps on Lync, you must restart the Lync front-end services to ensure that the configuration takes effect.

Note

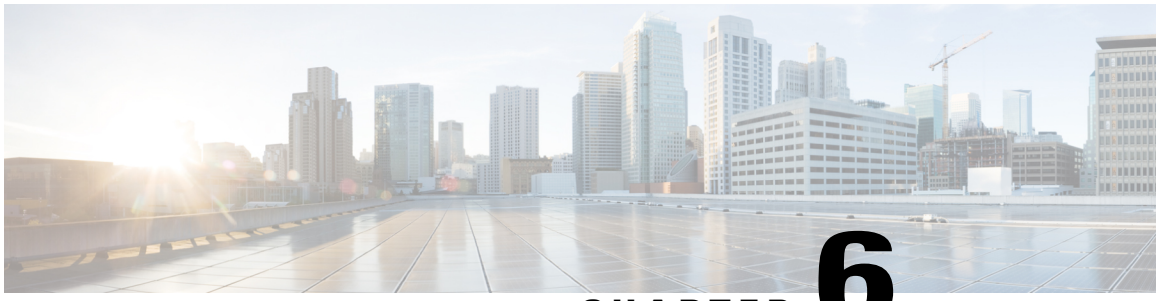
- Cisco recommends that you perform this procedure during a scheduled maintenance window.
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Services**.
Step 2 Right-click the service **Lync front end server** and choose **Restart**.

Related Topics

Integration Troubleshooting, on page 121



CHAPTER 6

Microsoft Office Communications Server Configuration for Partitioned Intradomain Federation

Microsoft Office Communications server configuration for partitioned intradomain federation applies only to Microsoft Office Communications Server (OCS) 2007 R2.

- Domain Verification for OCS Servers, page 69
- Enable Port 5060/5061 on OCS Server, page 69
- Federated Link to Microsoft OCS Server Configuration Task List, page 70
- Configure Static Routes on OCS to Point to the IM and Presence Service, page 72
- Add Host Authorization on OCS for IM and Presence Service, page 73
- Restart Services on OCS Front-End Servers, page 74
- TLS Encryption Configuration, page 75

Domain Verification for OCS Servers

Before you proceed to set up IM and Presence Service for partitioned intradomain federation, verify that there are matching domains configured on the Microsoft OCS servers and all nodes in the IM and Presence Service cluster.

Enable Port 5060/5061 on OCS Server

To use unencrypted TCP connections for SIP traffic between IM and Presence Service and OCS, configure the OCS server to listen on TCP SIP port 5060. For federated TLS connections, configure the OCS server to listen on TLS port 5061.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition or Enterprise Edition front-end server and choose **Properties** > **Front End Properties**.

Step 3 Click the **General** tab.

Step 4 If port 5060 or 5061 is not listed under Connections, click **Add**.

Step 5 Choose **All** as the IP Address Value.

Step 6 Enter the Transport and Port values.

- For TCP, enter **TCP** as the Transport Value and **5060** as the Port Value.
- For TLS, enter **TLS** as the Transport Value and **5061** as the Port Value.

Step 7 Click **OK** to close the **Add Connection** window. The port value should now be listed under the Connections list.

Step 8 Click **OK** again to close the **Front End Server Properties** window.

What to Do Next

Configure static routes on the OCS server to point to the IM and Presence Service.

Related Topics

Integration Troubleshooting, on page 121

Federated Link to Microsoft OCS Server Configuration Task List

The following table provides an overview of the steps to configure federated links between IM and Presence Service and Microsoft OCS servers.

If you are using direct federation from IM and Presence Service to OCS without the Access Edge server or Cisco Adaptive Security Appliance, you must configure a TLS or TCP static route on the OCS server. The static route points to an IM and Presence Service node. The Cisco Adaptive Security Appliance or the Microsoft Access Edge are not required.

- For Standard Edition, you must you must configure static routes on all Standard Edition servers.
- For Enterprise Edition, you must you must configure static routes on all pools.

Table 21: Task List for End-to-End Configuration of Federated Links to Microsoft OCS Server

Step	Description
Configure a static route on IM and Presence Service	TLS or TCP is supported. For TLS, select TLS as the Protocol Type and 5061 as the Next Hop Port number. For TCP, select TCP as the Protocol Type and 5060 as the Next Hop Port number.
Configure a static route on OCS for IM and Presence Service	TLS or TCP is supported. For TLS, the static route port should be 5061 For TCP, the static route port should be 5060. **Important** When using TLS with static routes on OCS, you must specify the FQDN of the IM and Presence Service node, rather than an IP address. Verify the Peer Auth Listener port is configured as 5061 and change Server Auth Listener port. Log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Application Listeners**. • Verify that the Peer Auth Listener port is 5061. • If the Server Auth Listener port is configured as 5061, you must change it to another value, for example 5063.
Configure a host authorization entry for the IM and Presence Service	This procedure applies to TLS and TCP. For TLS, you must add two host authorization entries for each IM and Presence Service node, one entry using the IP address of the IM and Presence Service node, and the second entry using the IM and Presence Service FQDN. For TCP, only one host authorization entry using the IM and Presence Service IP address needs to be added for each IM and Presence Service node.
Configure the certificates on OCS	This procedure is only for TLS. To retrieve the CA root certificate and the OCS signed certificate, perform the following steps: • Download and install the CA certificate chain. • Request a certificate from the CA server • Download the certificate from the CA server In the OCS Front End Server Properties, ensure the TLS listener for port 5061 on OCS is configured. (The transport can be MTLS or TLS). From the OCS Front End Server Properties, choose the Certificates tab, and click **Select Certificate** to choose the OCS signed certificate.

Step	Description
Configure OCS to use FIPS (TLSv1 rather than SSLv3), and import the CA root certificate.	This procedure is only for TLS. **1** Open the Local Security Settings on OCS. **2** In the console tree, choose **Local Polices.** **3** Choose **Security Options**. **4** Double-click **System Cryptography:Use FIPS Compliant algorithms for encryption, hashing and signing**. **5** Enable the security setting. **6** Click **OK**. **Note** You may need to restart OCS for this to take effect. **7** Import the CA root certificate for the CA that signs the IM and Presence Service certificate. Import the CA root certificate in to the trust store on OCS using the certificate snap-in.
Configure the certificates on IM and Presence Service	This procedure is only for TLS. You must upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service. As well, generate a CSR for IM and Presence Service and have it signed by the CA. Then upload the CA-signed certificate to IM and Presence Service. You must then add a TLS peer subject on IM and Presence Service for the OCS Server. See topics related to setting up certificates for detailed instructions.

Configure Static Routes on OCS to Point to the IM and Presence Service

To allow OCS to route requests to IM and Presence, you must configure a TLS or TCP static route on the OCS server. The static route points to an IM and Presence Service node.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the Enterprise Edition pool name or the Standard Edition server name, as appropriate.

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

Step 4 Choose the **Routing** tab and click **Add**.

Step 5 Enter the domain for the IM and Presence Service node, for example, foo.com.

Step 6 Ensure that the check box for **Phone URI** is unchecked.

Step 7 Set the next hop transport, port, and IP address/FQDN values:

- For TCP, choose **TCP** as the Next Hop Transport value and enter a Next Hop Port value of **5060**. Enter the IP address of the IM and Presence Service node as the Next Hop IP Address.
- For TLS, choose **TLS** as the Next Hop Transport value and enter a Next Hop Port value of **5061**. Enter the IP address of the IM and Presence Service node as the FQDN.

Note
- The port used for the TLS static route must match the Peer Auth Listener port that is configured on the IM and Presence Service node.
- The FQDN must be resolvable by the OCS server. Ensure that the FQDN resolves to the IP address of the IM and Presence Service node.

Step 8 Ensure that the check box for **Replace host in request URI** is unchecked.

Step 9 Click **OK** to close the **Add Static Route** window. The new static route should appear in the Routing list.

Step 10 Click **OK** again to close the **Front End Server Properties** window.

What to Do Next

Proceed to add the host authorization on OCS forIM and Presence Service.

Add Host Authorization on OCS for IM and Presence Service

To allow OCS to accept SIP requests from IM and Presence Service without being prompted for authorization, you must configure Host Authorization entries on OCS for each IM and Presence Service node.

For TCP, only one host authorization entry using the IM and Presence Service IP address needs to be added for each IM and Presence Service node.

If you are configuring TLS encryption between OCS and IM and Presence Service, you must add two Host Authorization entries for each IM and Presence Service node, as follows:

- The first entry must contain the FQDN of the IM and Presence Service node.
- The second entry must contain the IP address of the IM and Presence Service node.

If you are not configuring TLS encryption, then you add only one Host Authorization entry for each IM and Presence Service node. This host authorization entry must contain the IP address of the IM and Presence Service node.

The following procedure describes how to add the required Host Authorization entries.

Note

- For Standard Edition, you must complete this procedure on all Standard Edition servers.
- For Enterprise Edition, you must complete this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the Enterprise Edition pool name or the Standard Edition server name, as appropriate.

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

Step 4 Choose the **Host Authorization** tab and click **Add**.

Step 5 If you are entering an FQDN, choose **FQDN** and enter the FQDN of the IM and Presence Service node. For example, imp1.foo.com.

Step 6 If you are entering an IP address, choose **IP Address** and enter the IP address of the IM and Presence Service node. For example, 10.x.x.x.

Step 7 Ensure that the **Outbound Only** check box is unchecked.

Step 8 Check the **Throttle as Server** check box.

Step 9 Check the **Treat as Authenticated** check box.

Step 10 Click **OK** to close the **Add Authorized Host** window.

Step 11 Repeat Step 4 to Step 10 for each IM and Presence node.

Step 12 After you add all the Host Authorization entries, click **OK** to close the **Front End Server Properties** window.

What to Do Next

Restart Services on OCS Front-End Servers, on page 74

Related Topics

Integration Troubleshooting, on page 121

Restart Services on OCS Front-End Servers

After you complete all the configuration steps on OCS, you must restart the OCS services to ensure that the configuration takes effect.

Note

- Cisco recommends that you perform this procedure during a scheduled maintenance window.
- For Standard Edition, you must follow this procedure on all Standard Edition servers.
- For Enterprise Edition, you must follow this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Stop** > **Front End Services** > **Front End Service**.

Step 3 After the services stop, right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Start** > **Front End Services** > **Front End Service**.

Related Topics

Integration Troubleshooting, on page 121

TLS Encryption Configuration

You must complete the procedures in this section to configure TLS encryption between IM and Presence Service and OCS.

After the TLS configuration is complete, you must restart services on OCS servers. See Restart Services on OCS Front-End Servers, on page 74.

Enable Federal Information Processing Standard Compliance on OCS

To support TLS encryption between IM and Presence Service and OCS, you must enable TLSv1 on OCS servers. TLSv1 is included as part of the Federal Information Processing Standard (FIPS) compliance on Windows servers. The following procedure describes how to enable FIPS compliance.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On the OCS server, choose **Start** > **Programs** > **Administrative Tools** > **Local Security Policy**.

Step 2 From the console tree, choose **Local Policies**.

Step 3 Choose **Security Options**.

Step 4 Double-click **System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing**.

Step 5 Enable the security setting.

Step 6 Click **OK**.

Step 7 Close the Local Security Settings window.

What to Do Next

Configure Mutual TLS Authentication on OCS, on page 76

Related Topics

Integration Troubleshooting, on page 121

Configure Mutual TLS Authentication on OCS

To configure TLS encryption betweenIM and Presence Service and OCS, you must configure port 5061 on the OCS servers for Mutual TLS authentication. The following procedure describes how to configure port 5061 for Mutual TLS authentication.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise front-end server and choose **Properties** > **Front End Properties**.

Step 3 Choose the **General** tab.

Step 4 If the Transport associated with Port 5061 is **MTLS**, go to Step 8.

Step 5 If the Transport associated with Port 5061 is not **MTLS**, click **Edit**.

Step 6 From the Transport drop-down list, choose **MTLS**.

Step 7 Click **OK** to close the **Edit Connection** window. The Transport associated with Port 5061 should now be **MTLS**.

Step 8 Click **OK** to close the **Properties** window.

What to Do Next

Install Certificate Authority Root Certificates on OCS, on page 76

Related Topics

Integration Troubleshooting, on page 121

Install Certificate Authority Root Certificates on OCS

To support TLS encryption between IM and Presence Service and OCS, each OCS server must have a signed security certificate. This signed certificate, along with the root certificate of the Certificate Authority (CA) that signed the certificate, must be installed on each OCS server.

Cisco recommends that OCS and IM and Presence Service nodes share the same CA. If not, the root certificate of the CA that signed the IM and Presence Service certificates must also be installed on each OCS server.

Generally, the root certificate of the OCS CA is already installed on each OCS server. Therefore, if OCS and IM and Presence Service share the same CA, there may be no need to install a root certificate. However, if a root certificate is required, see the following details.

If you are using Microsoft Certificate Authority, refer to the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for information about installing the root certificate from the Microsoft Certificate Authority onto OCS:

- Downloading the CA Certification Chain
- Installing the CA Certification Chain

If you are using an alternative CA, the following procedure is a generic procedure for installing root certificates onto OCS servers. The procedure for downloading the root certificate from the CA differs depending on your chosen CA.

Before You Begin

Download the root certificate or certificate chain from your CA and save it to the hard disk of your OCS server.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.

Step 2 Enter `mmc` and click **OK**.

Step 3 From the File menu, choose **Add/Remove Snap-in**.

Step 4 From the Add/Remove Snap-in dialog box, click **Add**.

Step 5 From the list of Available Standalone Snap-ins, choose **Certificates**, and then click **Add**.

Step 6 Choose **Computer Account**, and then click **Next**.

Step 7 In the Select Computer dialog box, check the check box for **<Local Computer> (the computer this console is running on)**, and then click **Finish**.

Step 8 Click **Close**, and then click **OK**.

Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

Step 10 Expand **Trusted Root Certification Authorities**.

Step 11 Right-click **Certificates**, and choose **All Tasks**.

Step 12 Click **Import**.

Step 13 In the **Import** wizard, click **Next**.

Step 14 Click **Browse** and navigate to where you saved the root certificate or certificate chain.

Step 15 Choose the file and click **Open**.

Step 16 Click **Next**.

Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears under the Certificate store.

Step 18 Click **Next**, and then click **Finish**.

Step 19 Repeat Step 11 to Step 18 as necessary for other CAs.

Note The *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* document refers to the Access Edge Server. For partitioned intradomain federation, you can replace references to the Access Edge Server with OCS Standard Edition server or Enterprise Edition front-end server.

What to Do Next

Validate Existing OCS Signed Certificate, on page 78

Related Topics

Integration Troubleshooting, on page 121
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Validate Existing OCS Signed Certificate

To support TLS encryption between IM and Presence Service and OCS, each OCS server must have a signed security certificate that supports Client Authentication. If a signed certificate is already installed on the OCS server, the following procedure describes how to check if that existing signed certificate supports Client Authentication.

Note
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.
Step 2 Enter `mmc` and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal** and choose **Certificates**.
Step 11 Find the signed certificate currently used by OCS in the right pane.
Step 12 Ensure that **Server and Client Authentication** is listed in the Intended Purposes column.

What to Do Next

Signed Certificate Request from the Certificate Authority for the OCS Server, on page 79

Related Topics

Integration Troubleshooting, on page 121

Signed Certificate Request from the Certificate Authority for the OCS Server

This section describes how to install a signed certificate on a Microsoft Office Communicator Server (OCS) and how to choose the installed certificate for TLS negotiation.

Note The procedures in this topic are only necessary if no signed certificate exists on an OCS or the existing certificate does not support Client Authentication.

To support TLS encryption between IM and Presence Service and OCS, each OCS must have a signed security certificate that supports Client Authentication. If that is not the case on any OCS, the following procedures outline how to request a newly signed certificate from the Certificate Authority and install it onto that specific OCS.

The Subject Common Name (CN) used in Certificate Signing Requests (CSR) from the OCS differs depending on the OCS deployment:

- For Standard Edition servers, use the FQDN of the Standard Edition server as the Subject CN.
- For Enterprise Edition front-end servers, use the FQDN of the pool to which the front-end server belongs as the Subject CN.

Standalone Microsoft Certificate Authority

If you are using a Standalone Microsoft Certificate Authority, see the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to request a signed certificate from the CA for the OCS:

- Requesting a Certificate from the CA Server
- Downloading the Certificate from the CA Server

Note This document refers to the Access Edge Server. For Partitioned Intradomain Federation, you can replace references to the Access Edge Server with an OCS Standard Edition or Enterprise Edition front-end server.

Enterprise Microsoft Certificate Authority

If you are using an Enterprise Microsoft Certificate Authority, see the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to generate the required template on the CA and request a signed certificate from the CA for the OCS:

- Creating a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

- Requesting the Site Server Signing Certificate

Alternative Certificate Authority

If you are using an alternative CA, the following is a generic procedure for installing signed certificates onto the OCS. The procedure for requesting a signed certificate differs depending on your chosen CA.

Related Topics

Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Install Signed Certificate on the OCS Server

Before You Begin

Download the signed certificate from your CA and save it to the hard disk of your OCS server.

Procedure

Step 1 On your OCS server, choose **Start** > **Run**.
Step 2 Enter **mmc** and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal**.
Step 11 Right-click **Certificates**, and then choose **All Tasks**.
Step 12 Click **Import**.
Step 13 In the **Import** wizard, click **Next**.
Step 14 Click **Browse** and navigate to where you saved the signed certificate.
Step 15 Choose the file and click **Open**.
Step 16 Click **Next**.
Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Personal** appears under the Certificate store.
Step 18 Click **Next**, and then click **Finish**.

What to Do Next

Select Installed Certificate for TLS Negotiation, on page 81

Related Topics

Integration Troubleshooting, on page 121

Select Installed Certificate for TLS Negotiation

Regardless of which CA is used, after the signed certificate is installed onto the OCS server, you must perform the following procedure to select the installed certificate for use by OCS in TLS negotiation withIM and Presence Service.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Properties** > **Front End Properties**.

Step 3 Choose the **Security** tab and choose **Select Certificate**.

Step 4 From the list of installed certificates, choose the newly signed certificate and click **OK** to close the **Select Certificate** window.

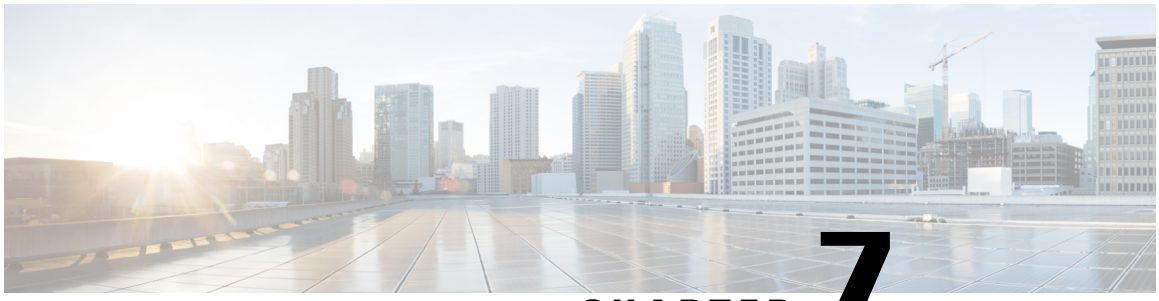
Step 5 Click **OK** to close the **Properties** window.

What to Do Next

Restart Services on OCS Front-End Servers, on page 74

Related Topics

Integration Troubleshooting, on page 121



CHAPTER 7

Configuration of Microsoft Live Communications Server for Partitioned Intradomain Federation

- Domain Verification for LCS Servers, page 83
- Enable Port 5060 on LCS Server, page 83
- Configure a LCS Static Route to Point to the IM and Presence Service, page 84
- Add Host Authorization on LCS for IM and Presence Service, page 85
- Restart Services on LCS Servers, page 86
- TLS Encryption Configuration for Microsoft LCS Servers, page 87

Domain Verification for LCS Servers

Before you proceed to set up the IM and Presence Service for Partitioned Intradomain Federation, verify that there are matching domains configured on the Microsoft LCS servers and all nodes in the IM and Presence Service cluster.

Enable Port 5060 on LCS Server

If you wish to use unencrypted TCP connections for SIP traffic between the IM and Presence Service and Microsoft Live Communications Server (LCS), then LCS must be configured to listen on TCP SIP port 5060. The following procedure describes how to enable port 5060 on LCS servers.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Properties**.

Step 3 Choose the **General** tab.

Step 4 If port 5060 is not listed under Connections, click **Add**.

Step 5 Choose **All available IP Addresses**.

Step 6 Choose **TCP** as the Transport Value.

Step 7 Choose **5060** as the Port Value and click **OK** to close the **Add Connection** window. Port 5060 should now be listed under the Connections list.

Step 8 Click **OK** to close the **Properties** window.

What to Do Next

Configure a LCS Static Route to Point to the IM and Presence Service, on page 84

Related Topics

Integration Troubleshooting, on page 121

Configure a LCS Static Route to Point to the IM and Presence Service

To allow LCS to route requests to the IM and Presence Service, you must configure a static route on LCS servers. The static route points to an IM and Presence Service node.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the Enterprise Edition pool name or Standard Edition server name, as appropriate.

Step 3 Choose **Properties**.

Step 4 Choose the **Routing** tab and click **Add**.

Step 5 Enter * (asterisk) as the User value.

Step 6 Enter the domain of the IM and Presence Service node, for example, foo.com.

Step 7 Ensure that the check box for **Phone URI** is unchecked.

Step 8 If you are entering an FQDN, choose **Network Address** and enter the FQDN of the IM and Presence Service node. For example, cup1.foo.com.

Step 9 If you are entering an IP address, choose **IP Address** and enter the IP address of the IM and Presence Service node. For example, 10.x.x.x.

Step 10 Choose **TCP** for the Transport value.

Step 11 Enter **5060** for the Port value.

Step 12 Ensure that the check box for **Replace host in request URI** is unchecked and click **OK**. The new static route should appear in the Routing list.

Step 13 Click **OK** to close the Properties window.

What to Do Next

Add Host Authorization on LCS for IM and Presence Service, on page 85

Related Topics

Integration Troubleshooting, on page 121

Add Host Authorization on LCS for IM and Presence Service

To allow LCS to accept SIP requests from the IM and Presence Service without being prompted for authorization, you must configure host authorization entries on LCS for each IM and Presence Service node.

If you are configuring TLS encryption between LCS and the IM and Presence Service, you must add two host authorization entries for each IM and Presence Service node, as follows:

- The first entry must contain the FQDN of the IM and Presence Service node.
- The second entry must contain the IP address of the IM and Presence Service node.

If you are not configuring TLS encryption, you add only one host authorization entry for each IM and Presence Service node. This host authorization entry must contain the IP address of the IM and Presence Service node.

The following procedure describes how to add the required host authorization entries.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all pools.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the Enterprise Edition pool name or Standard Edition server name, as appropriate.

Step 3 Choose **Properties**.

Step 4 Choose the **Host Authorization** tab and click **Add**.

Step 5 If you are entering an FQDN, choose **Network Address** and enter the FQDN of the IM and Presence Service node. For example, cup1.foo.com.

Step 6 If you are entering an IP address, choose **IP Address** and enter the IP address of the IM and Presence Service node. For example, 10.x.x.x.

Step 7 Ensure that the check box for **Outbound Only** is unchecked.

Step 8 Check the **Throttle as Server** check box.

Step 9 Check the **Treat as Authenticated** check box.

Step 10 Click **OK** to close the **Add Authorized Host** window.

Step 11 Repeat Step 4 to Step 10 for each IM and Presence Service node.

Step 12 After you enter all the Host Authorization entries, click **OK** to close the **Properties** window.

What to Do Next

Restart Services on LCS Servers, on page 86

Related Topics

Integration Troubleshooting, on page 121

Restart Services on LCS Servers

After you complete all the configuration steps on LCS, you must restart the LCS services to ensure that the configuration takes effect.

Note

- Cisco recommends that you perform this procedure during a scheduled maintenance window.
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Stop**.

Step 3 After the services stop, right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Start**.

Related Topics

Integration Troubleshooting, on page 121

TLS Encryption Configuration for Microsoft LCS Servers

You must complete the procedures in this section to configure TLS encryption between the IM and Presence Service and Microsoft LCS servers.

After the TLS configuration is complete, you must restart services on LCS servers, see Restart Services on LCS Servers, on page 86.

Enable Federal Information Processing Standard Compliance on LCS

To support TLS encryption between the IM and Presence Service and LCS, you must enable TLSv1 on LCS servers. TLSv1 is included as part of the Federal Information Processing Standard (FIPS) compliance on Windows servers. The following procedure describes how to enable FIPS compliance.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On the LCS server, choose **Start** > **Programs** > **Administrative Tools** > **Local Security Policy**.

Step 2 From the console tree, choose **Local Policies**.

Step 3 Choose **Security Options**.

Step 4 Double-click **System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing**.

Step 5 Enable the security setting.

Step 6 Click **OK**.

Step 7 Close the **Local Security Settings** window.

What to Do Next

Configure Mutual TLS Authentication on LCS, on page 88

Related Topics

Integration Troubleshooting, on page 121

Configure Mutual TLS Authentication on LCS

To configure TLS encryption between the IM and Presence Service and LCS, you must configure port 5061 on the LCS servers for Mutual TLS authentication. The following procedure describes how to configure port 5061 for Mutual TLS authentication.

Note

- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise front-end server and choose **Properties**.

Step 3 Choose the **General** tab.

Step 4 If the Transport associated with Port 5061 is **Mutual TLS**, go to Step 8.

Step 5 If the Transport associated with Port 5061 is not **Mutual TLS**, click **Edit**.

Step 6 Check the **Authenticate remote server (Mutual TLS)** check box.

Step 7 Click **OK** to close the **Edit Connection** window. The Transport associated with Port 5061 should now be **Mutual TLS**.

Step 8 Click **OK** to close the Properties window.

What to Do Next

Install Certificate Authority Root Certificates on LCS, on page 88

Related Topics

Integration Troubleshooting, on page 121

Install Certificate Authority Root Certificates on LCS

To support TLS encryption between the IM and Presence Service and LCS, each LCS server must have a signed security certificate. This signed certificate, along with the root certificate of the Certificate Authority (CA) that signed the certificate, must be installed on each LCS server.

Cisco recommends that LCS and the IM and Presence Service nodes share the same CA. If not, the root certificate of the CA that signed the IM and Presence Service certificates must also be installed on each LCS server.

Generally, the root certificate of the LCS CA is already installed on each LCS server. Therefore, if LCS and the IM and Presence Service share the same CA, there may be no need to install a root certificate. However, if a root certificate is required, see the following details.

If you are using Microsoft Certificate Authority, refer to the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for information about installing the root certificate from the Microsoft Certificate Authority onto LCS:

- Downloading the CA Certification Chain
- Installing the CA Certification Chain

If you are using an alternative CA, the following procedure is a generic procedure for installing root certificates onto LCS servers. The procedure for downloading the root certificate from the CA differs depending on your chosen CA.

Before You Begin

Download the root certificate or certificate chain from your CA and save it to the hard disk of your LCS server.

Procedure

Step 1 On your LCS server, choose **Start** > **Run**.

Step 2 Enter **mmc** and click **OK**.

Step 3 From the File menu, choose **Add/Remove Snap-in**.

Step 4 In the Add/Remove Snap-in dialog box, click **Add**.

Step 5 From the list of Available Standalone Snap-ins, choose **Certificates**, and then click **Add**.

Step 6 Choose **Computer Account**, and then click **Next**.

Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.

Step 8 Click **Close**, and then click **OK**.

Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

Step 10 Expand **Trusted Root Certification Authorities**.

Step 11 Right-click **Certificates** and choose **All Tasks**.

Step 12 Click **Import**.

Step 13 In the **Import** wizard, click **Next**.

Step 14 Click **Browse** and navigate to where you saved the root certificate or certificate chain.

Step 15 Choose the file and click **Open**.

Step 16 Click **Next**.

Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears under the Certificate store.

Step 18 Click **Next**, and then click **Finish**.

Step 19 Repeat Step 11 to Step 18 as necessary for other CAs.

Note The *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* document refers to the Access Edge Server. For Partitioned Intradomain Federation, you can replace references to the Access Edge Server with LCS Standard Edition server or Enterprise Edition front-end server.

What to Do Next

Validate Existing LCS Signed Certificate, on page 90

Related Topics

Integration Troubleshooting, on page 121
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Validate Existing LCS Signed Certificate

To support TLS encryption between the IM and Presence Service and LCS, each LCS server must have a signed security certificate that supports Client Authentication. If a signed certificate is already installed on the LCS server, the following procedure describes how to check if that existing signed certificate supports Client Authentication.

Note
- For Standard Edition, you must perform this procedure on all Standard Edition servers.
- For Enterprise Edition, you must perform this procedure on all front-end servers.

Procedure

Step 1 On your LCS server, choose **Start** > **Run**.
Step 2 Enter `mmc` and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates** and click **Add**.
Step 6 Choose **Computer Account** and click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal** and choose **Certificates**.
Step 11 Find the signed certificate currently used by LCS in the right pane.
Step 12 Ensure that **Client Authentication** is listed in the Intended Purposes column.

What to Do Next

Signed Certificate Requests from Certificate Authority for LCS Server, on page 91

Related Topics

Integration Troubleshooting, on page 121

Signed Certificate Requests from Certificate Authority for LCS Server

This section describes how to install a signed certificate on an LCS server and how to choose the installed certificate for TLS negotiation.

Note The procedures in this section are necessary only if no signed certificate exists on an LCS server or the existing certificate does not support Client Authentication.

To support TLS encryption between the IM and Presence Service and LCS, each LCS server must have a signed security certificate that supports Client Authentication. If that is not the case on any LCS server, the following procedures outline how to request a newly signed certificate from the Certificate Authority and install it onto that specific LCS server.

The Subject Common Name (CN) used in Certificate Signing Requests (CSR) from LCS differs depending on LCS deployment:

- For Standard Edition servers, use the FQDN of the Standard Edition server as the Subject CN.
- For Enterprise Edition front-end servers, use the FQDN of the pool to which the front-end server belongs as the Subject CN.

Standalone Microsoft Certificate Authority

If you are using a Standalone Microsoft Certificate Authority, see the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to for instructions to request a signed certificate from the CA for the LCS server:

- Requesting a certificate from the CA server
- Downloading the certificate from the CA server

Note This document refers to the Access Edge Server. For Partitioned Intradomain Federation, you can replace references to the Access Edge Server with LCS Standard Edition server or Enterprise Edition front-end server.

Enterprise Microsoft Certificate Authority

If you are using an Enterprise Microsoft Certificate Authority, see the following procedures in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* to generate the required template on the CA and request a signed certificate from the CA for the LCS server:

- Creating a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

- Requesting the Site Server Signing Certificate

Alternative Certificate Authority

If you are using an alternative CA, the following is a generic procedure for installing signed certificates onto LCS servers. The procedure for requesting a signed certificate differs depending on your chosen CA.

Related Topics

Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Install Signed Certificate on LCS Server

Before You Begin

Download the signed certificate from your CA and save it to the hard disk of your LCS server.

Procedure

Step 1 On your LCS server, choose **Start** > **Run**.
Step 2 Enter `mmc` and click **OK**.
Step 3 From the File menu, choose **Add/Remove Snap-in**.
Step 4 From the Add/Remove Snap-in dialog box, click **Add**.
Step 5 From the list of Available Standalone Snap-ins, choose **Certificates**, and then click **Add**.
Step 6 Choose **Computer Account**, and then click **Next**.
Step 7 In the Select Computer dialog box, check the **<Local Computer> (the computer this console is running on)** check box and click **Finish**.
Step 8 Click **Close**, and then click **OK**.
Step 9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.
Step 10 Expand **Personal**.
Step 11 Right-click **Certificates** and choose **All Tasks**.
Step 12 Click **Import**.
Step 13 In the **Import** wizard, Click **Next**.
Step 14 Click **Browse** and navigate to where you saved the signed certificate.
Step 15 Choose the file and click **Open**.
Step 16 Click **Next**.
Step 17 Leave the default value **Place all certificates in the following store** and ensure that **Personal** appears under the Certificate store.
Step 18 Click **Next**, and then click **Finish**.

What to Do Next

Select Installed Certificate for TLS Negotiation, on page 93

Related Topics

Integration Troubleshooting, on page 121

Select Installed Certificate for TLS Negotiation

Regardless of which CA is used, after the signed certificate is installed onto the LCS server, you must perform the following procedure to select the installed certificate for use by LCS in TLS negotiation with the IM and Presence Service.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005**.

Step 2 Right-click the FQDN of the Standard Edition server or Enterprise Edition front-end server and choose **Properties**.

Step 3 Choose the Security tab and choose **Select Certificate**.

Step 4 From the list of installed certificates, choose the newly signed certificate and click **OK** to close the **Select Certificate** window.

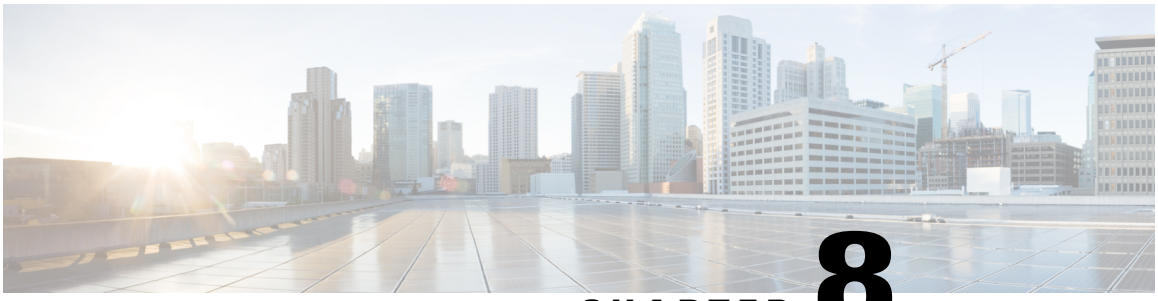
Step 5 Click **OK** to close the **Properties** window.

What to Do Next

Restart Services on LCS Servers, on page 86

Related Topics

Integration Troubleshooting, on page 121



CHAPTER 8

User Migration

- Cisco User Migration Tools, page 95
- Recommendations before Migration, page 96
- Provision of Microsoft Server Users on Cisco Unified Communications Manager, page 99
- Backups of User Microsoft Server Contact List Information, page 99
- Export of Contact Lists for Migrating Users, page 100
- Disable Users on Microsoft Servers, page 106
- Delete User Data from Database for Migrating Users, page 108
- Import Contact Lists for Migrating Users into IM and Presence, page 110
- Deploy an IM and Presence Service Supported Client on Users Desktop, page 112
- Reset Maximum Contact List Size and Maximum Watcher Size, page 112

Cisco User Migration Tools

Cisco provides the following tools to aid the user migration process from Lync/OCS/LCS to IM and Presence Service:

- Export Contact List tool—allows you to export contact lists in bulk from the Microsoft server for migrating users
- Disable Account tool—allows you to disable the Microsoft server account of migrating users
- Delete Account tool—allows you to delete migrating users from the Microsoft server so that presence requests for these users are later routed to IM and Presence Service

These user migration tools can be collectively downloaded as a zip file from the IM and Presence Service Download Software page on cisco.com at http://software.cisco.com/download/release.html?mdfid=286269517&flowid=50462&softwareid=282074312&release=UTILS&relind=AVAILABLE&rellifecycle=&reltype=latest.

The zip file contains the three tools and a text file called version.txt. The text file contains the current version number of the tools and must be saved in the same folder as the tools. If the tools are stored in different folders,

you must store a copy of the text file in each location. If the text file is not in the same folder when you run a tool, you receive an error and the tool does not run.

Tip

While attempting to run any of the user migration tools you may receive the following error: "Application failed to initialize properly". The reason for this error is that you are attempting to run the user migration tools without the .NET 1.1 Framework installed. Each of the user migration tools that Cisco provides requires that at least version 1.1 of the .NET Framework is installed on the server where you are running the tool.

Recommendations before Migration

Cisco recommends that you perform the following tasks before you begin to migrate users from Lync/OCS/LCS to IM and Presence Service:

- Set unlimited contact lists and watchers
- Enable automatic authorization of subscription requests
- Disable new subscriber notification pop-ups on Microsoft Lync

Set Unlimited Contact Lists and Watchers

Before you migrate users from Lync/OCS/LCS to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service to unlimited. This ensures that each migrated user contact list is fully imported to IM and Presence Service.

After all users have been migrated to IM and Presence Service, reset the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service to the desired values. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers size.

The following procedure describes how to set unlimited values for the Maximum Contact List Size and Maximum Watchers settings.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. When you change Presence settings, they are applied to all nodes in the cluster; therefore you need to set them only on the IM and Presence Service database publisher node within any given cluster.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Settings**.

Step 2 For **Maximum Contact List Size (per user)**, check the **No Limit** check box.

Step 3 For **Maximum Watchers (per user)**, check the **No Limit** check box.

Step 4 Click **Save**.

Step 5 Restart the Cisco XCP Router on all IM and Presence Service nodes in the cluster. To restart the Cisco XCP Router, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Network Services**.

Enable Automatic Authorization of Subscription Requests

To improve user experience during migration, Cisco recommends that you allow automatic authorization of subscription requests before you begin the migration process. Otherwise, each IM and Presence Service user is forced to manually authorize subscription requests each time they are imported as a contact into the IM and Presence Service. This setting should only be disabled, if desired, after all migrations are complete.

The following procedure describes how to enable automatic authorization of subscription requests.

Note This setting is enabled by default on IM and Presence Service.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. When you change Presence settings, they are applied to all nodes in the cluster; therefore you need to set them only on the IM and Presence database publisher node within any given cluster.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Settings**.

Step 2 Check the check box for **Allow users to view the availability of other users without being prompted for approval**.

Step 3 Click **Save**.

Step 4 Restart the Cisco XCP Router on all IM and Presence Service nodes in the cluster. To restart the Cisco XCP Router, log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center – Network Services**.

Subscriber Notification Pop-ups

When you migrate users from Microsoft Lync to IM and Presence Service, users that remain on Lync may receive subscription notification pop-ups from some of those migrated users. Such a notification only occurs when:

- the migrated user has the Microsoft Lync user in their contact list

  and

- the Microsoft Lync user does not have that same migrated user in their contact list

If the Microsoft Lync user has the migrated contact in their contact list also, then there is no notification pop-up. When an individual notification pop-up has been handled by the Microsoft Lync user, it will not re-appear.

If you do not want Lync users to receive new subscriber notification pop-ups you can disable Lync pop-ups. You have two options when disabling these notification pop-ups:

- you can disable pop-ups for the entire duration of user migration
- you can disable pop-ups only during the migration of a batch of users

If you disable pop-ups, then all pop-ups for all Lync users will be disabled until you re-enable them.

Note Disabling and enabling Microsoft Lync pop-ups requires a restart of the Lync front-end services.

Disable Microsoft Lync Pop-ups

If you want to disable all pop-ups for all Microsoft Lync users, complete the following procedure before you begin the user migration or the migration of a batch of users.

Procedure

Step 1 On the Lync front-end server choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Management Shell**.

Step 2 Enter the following powershell command:

```
Set-CSClientpolicy -EnableNotificationForNewSubscriber $False
```

Step 3 Choose **Start** > **Programs** > **Administrative Tools** > **Services**.

Step 4 Right-click the service **Lync front end server** and click **Restart**.

Restore Microsoft Lync Pop-up Behavior

To restore the previous client behavior for notification pop-ups for Microsoft Lync users complete the following procedure after user migration is complete or after the migration of a batch of users is complete.

Procedure

Step 1 Enter the following command to restore client pop-up behavior on Lync:
```
Set-CSClientpolicy -EnableNotificationForNewSubscribers $Null
```

Step 2 Choose **Start** > **Programs** > **Administrative Tools** > **Services**.

Step 3 Right-click the service **Lync front end server** and choose **Restart**.

Provision of Microsoft Server Users on Cisco Unified Communications Manager

The first step in migrating users from Microsoft Lync, Microsoft Office Communications Server (OCS), or Microsoft Live Communications Server (LCS) to IM and Presence Service is to provision the Microsoft server users on Cisco Unified Communications Manager and license them for IM and Presence Service and an IM and Presence Service supported client.

Note After users are provisioned on Cisco Unified Communications Manager and IM and Presence Service, Cisco recommends that you complete the full user migration process during the same maintenance window. Leaving users provisioned on both IM and Presence Service and on the Microsoft servers for any time period disrupts message routing for those users.

See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for information about configuring new users in Cisco Unified Communications Manager and the license requirements for IM and Presence Service and supported clients.

What To Do Next

Backups of User Microsoft Server Contact List Information

Related Topics

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

Backups of User Microsoft Server Contact List Information

The Lync/OCS/LCS provides a tool called dbimpexp.exe. Cisco recommends that you use this tool to back up the Microsoft server user contact list information so that you can restore this information on the Microsoft server at a later date, if needed.

For the purpose of migrating Microsoft server users to an IM and Presence Service supported client, you can use this tool to back up the contact list for an individual Microsoft server user or all users.

Related Topic

Usage of the dbimpexp.exe tool: http://www.ocspedia.com/Misc/Explore_Dbimpexp.aspx?ArticleID=41

What To Do Next

Export of Contact Lists for Migrating Users, on page 100

Export of Contact Lists for Migrating Users

Cisco provides an Export Contact List tool (ExportContacts.exe) to allow an administrator to export contact lists in bulk from Lync/OCS/LCS for migrating users. The tool uses the Microsoft server application programming interfaces (APIs) to export contact lists and output to a comma-separated values (CSV) file. This file can then be used by the IM and Presence Service Bulk Administration Tool (BAT) to import these same contact lists into IM and Presence Service at a later point in the migration.

Note

- You can run this tool against all the supported Microsoft server platforms.
- You can run the tool on any Standard Edition server or Enterprise Edition front-end server.
- To export contact lists for Lync users, the Export Contact List tool requires read access to the Lync RTC database and also read access to LDAP. You must also ensure that dbo execution account privileges are granted to the RTC database.
- Running this tool has no affect on the capabilities of other Microsoft server users who are signed into Microsoft Lync or Microsoft Office Communicator. However, Cisco recommends that you run this tool during a scheduled maintenance window to reduce the load on the Microsoft server and Active Directory system.

After you run the tool, a file that contains the exported contact lists is created in the same directory as the tool. The filename is ExportedContacts<Timestamp>.csv. A time stamp is appended to the filename when the file is created; therefore, each time you run the Export Contact List tool, it creates a unique output file.

The Export Contact List tool also creates a second file that contains the Microsoft server SIP URI of each user that you specify for the contact list export. The filename is UserList<Timestamp>.txt and it is also created in the same directory as the tool.

Note You can use the UserList<Timestamp>.txt file as input to the Disable Account tool and the Delete Account tool.

Log File

The Export Contact List tool also creates a unique time-stamped log file in the same directory as the output file each time you run the tool. The filename for the log file is ExportContactsLog<Timestamp>.txt.

It is good practice to check the log file each time you run the Export Contact List tool. You can then scan through the log file to fix any issues. At the bottom of each log file, the following information is summarized:

- Number of users that were successfully processed
- Number of users that were not found
- Number of users that were not processed due to errors
- Largest contact list size

- Total number of contacts that were found
- Average contact list size

Run Modes

The Export Contact List tool has two run modes; NORMAL and STATSONLY. NORMAL is the standard way to run the tool. In this mode, three files are created: the CSV file that contains the exported contacts, the log file and the users' Lync/OCS/LCS SIP URI file. In STATSONLY mode, the Export Contact List tool creates only the log file. This allows you to run the tool to discover any errors that you can fix before you create the exported contacts CSV file and the Microsoft server SIP URI file.

Input File Formats

The Export Contact List tool (`ExportContacts.exe`) allows you to specify an input file containing the list of migrating users. The tool then retrieves the contact lists for the users that are specified in that input file. Alternatively, you can specify a command line parameter to export contact lists for all users in the local Lync/OCS/LCS database.

Note If you use choose to export all users with the Export Contact List tool, the resulting `UserList<Timestamp>.txt` file contains the contact lists of all Microsoft server-enabled users in the domain, regardless of whether they are migrating to IM and Presence Service. If you later use the `UserList<Timestamp>.txt` file as input to the Disable Account tool and the Delete Account tool, be aware that all user accounts in the domain are affected by the Disable Account and Delete Account tools.

If you are using an input file, the following input file formats are supported:

Input File Format 1: Microsoft server SIP URIs

Note the following:

- Each line in the input file represents a contact list owner.
- The contact list owner is represented by the owner's Microsoft server SIP URI, for example, sip:bobjones@foo.com.
- The following is a sample input file:

```
sip:ann@foo.com
sip:bob@foo.com
sip:joe@foo.com
sip:chuck@foo.com
```

Input File Format 2: Users by Organizational Unit in Active Directory

In this input file format, you can specify the Organizational Unit (OU) in Active Directory that contains the users that you want to migrate. The input file must have the following format:

```
DN:OU=OrgUnit1,OU=OrgUnit2,DC=DomainComp1,DC=DomainComp2
```

where OrgUnit1 is an OU in the OrgUnit2 OU and DomainComp1 and DomainComp2 are the domain components. Domains usually have two domain components in AD, for example cisco and com for the cisco.com domain.

You can also specify multiple distinguished names (DNs) in a single input file to export contact lists for users from different OUs. The format of an input file with multiple DNs is as follows:

```
DN:OU=firstOU,DC=DomainComp1,DC=DomainComp2
DN:OU=secondOU,DC=DomainComp1,DC=DomainComp2
DN:OU=thirdOU,DC=DomainComp1,DC=DomainComp2
```

Input File Format 3: IM and Presence Service User IDs

Note the following:

- You can obtain a file in this format using the IM and Presence Service BAT Subcluster Export tool.
- This format is a comma-separated values (CSV) format, in which each line in the input file represents IM and Presence Service subcluster assignment data on the contact list owner.
- The contact list owner is represented by the owner's IM and Presence Service user ID, for example, bobjones. The user ID (configured on Cisco Unified Communications Manager) must match the user portion of the SIP URI in the Microsoft server domain; if the user ID does not match, you must use one of the other input file formats instead.
- The following is a sample input file with user IDs in bold type:

  ```
  UserID,Subcluster Name,Node Name
  ann,CUPSubcluster1,CUPServer1
  bob,CUPSubcluster1,CUPServer1
  joe,CUPSubcluster1,CUPServer1
  chuck,CUPSubcluster1,CUPServer1
  ```

  The Export Contact List tool ignores the Subcluster Name and Node Name information and uses only the UserID value.
- If you use this file format, you must provide the domain of the IM and Presence Service server when you run the tool. The tool uses the domain to format the user's SIP URI as follows: sip:userID@domain.

The following procedure describes how to export contact lists in bulk from the Microsoft server for migrating users.

Procedure

Step 1 Copy and extract the zip file containing the Cisco user migration tools to the Standard Edition server or Enterprise Edition front-end server.

Note After extraction, if you move any of the Cisco user migration tools to a different location on the Microsoft server, you must also copy the `version.txt` file to the new location to ensure that the tool prints out its current version.

Step 2 Open a command prompt and change directory to the location of the Export Contact List tool.

Step 3 At the command prompt, run the tool as follows:

If you want to...	Enter this command
Export the contact list for a list of users as specified in a Microsoft server SIP URI input file or Export the contact list for a list of users in an Organizational Unit in AD, as specified in a Users by Organizational Unit in AD input file	**ExportContacts.exe -s/***LDAPServer* **-f/***input_file* **-l/***logLevel* **-r/***run_mode* **-i/***database_instance* where: • *LDAPServer*—The IP or FQDN of the AD server where Microsoft server users are stored • *input_file*—A text file that contains a list of Microsoft server SIP URIs, or, a text file that contains a list of distinguished names for AD Organizational Units that contain the users that you want to migrate • *logLevel*—The logging level, which must be one of the following: ◦ error ◦ info ◦ debug (recommended) • *run_mode*—The run mode, which must be one of the following: ◦ NORMAL ◦ STATSONLY • *database_instance*—The Lync datastore instance name. This parameter is required only when you are exporting contacts for Lync users. Sample entries are as follows: ◦ Lync 2010 Standard Edition server: `localhost\rtc` ◦ Lync 2010 Enterprise Edition server: `LyncDatastoreFqdn\rtc`

If you want to...	Enter this command
Export the contact list for all Microsoft server-enabled users in the domain	**ExportContacts.exe -s/***LDAPServer* **-f/ALL -l/***logLevel* **-r/***run_mode* **-i/***database_instance* where: • *LDAPServer*—The IP or FQDN of the AD server where Microsoft server users are stored • *logLevel*—The logging level, which must be one of the following: ◦ error ◦ info ◦ debug (recommended) • *run_mode*—The run mode, which must be one of the following: • NORMAL • STATSONLY • *database_instance*—The Lync datastore instance name. This parameter is required only when you are exporting contacts for Lync users. **Note** This command exports the contact lists for all Microsoft server enabled users in the specified domain, regardless of whether they are migrating to IM and Presence Service. If you use the `UserList<Timestamp>.txt` file, which is created from this command, as input to the Disable Account tool and the Delete Account tool, be aware that all user accounts in the domain are affected by the Disable Account and Delete Account tools.

If you want to...	Enter this command
Export the contact list for a list of users as specified in an IM and Presence Service User ID input file	**ExportContacts.exe -s/***LDAPServer* **-f/***input_file* **-l/***logLevel* **-d/***Domain* **-r/***run_mode* **-i/***database_instance* where: • *LDAPServer*—The IP or FQDN of the AD server where Microsoft server users are stored • *input_file*—A text file that contains a list of IM and Presence Service user IDs • *logLevel*—The logging level, which must be one of the following: ◦ error ◦ info ◦ debug (recommended) • *Domain*—The domain in which the IM and Presence Service server resides. • *run_mode*—The run mode, which must be one of the following: ◦ NORMAL ◦ STATSONLY • *database_instance*—The Lync datastore instance name. This parameter is required only when you are exporting contacts for Lync users. Sample entries are as follows: ◦ Lync Standard Edition server: `localhost\rtc` ◦ Lync Enterprise Edition server: `LyncDatastoreFqdn\rtc`

Note To ensure correct contact list migration, the owners of the exported contact lists must be completely disabled on the Microsoft server before you import the contacts lists into IM and Presence Service.

What to Do Next

Disable Users on Microsoft Servers

Related Topics

Export Contact List Tool, on page 132

Disable Users on Microsoft Servers

This section describes procedures on how to disable a Lync/OCS/LCS account for migrating users and how to verify that Active Directory updates are synchronized to the Microsoft server.

Disable Microsoft Server Account for Migrating Users

Cisco provides a tool to disable the Lync/OCS/LCS account of migrating users. This tool (DisableAccount.exe) connects to Active Directory (AD) and updates the users' Microsoft server attributes to disable their account. Running the Disable Account tool is the first step in a two-step process that must take place to disable a migrating user on the Microsoft server:

1. Disable the Microsoft server user account for migrating user.
2. Delete the Microsoft server user data for migrating user.

After you disable the account for migrating user, wait until the Microsoft server's LDAP changes are synchronized before proceeding with the Delete utility. The LDAP synchronization can take up to 30 minutes.

Note

- You can run this tool on all supported Microsoft server platforms.
- You can run this tool on any Standard Edition server or Enterprise Edition front-end server.
- Running this tool has no affect on the capabilities of other Microsoft server users who are signed into Microsoft Lync or Microsoft Office Communicator. However, Cisco recommends that you run this tool during a scheduled maintenance window to reduce the load on the Microsoft server and Active Directory system.

The Disable Account tool accepts three inputs:

- The IP or FQDN of the AD server on which the Microsoft server users exist
- An input file containing the list of Microsoft server user accounts to disable
- The logging level, which should be one of error, info, or debug (debug is the recommended setting)

The Disable Account tool reads the list of users to disable from an input file. Each line in the input file represents a contact list owner. The contact list owner is represented by the owner's Microsoft server SIP URI, for example, sip:bobjones@cisco.com. The following is a sample input file:

```
sip:ann@cisco.com
sip:bob@cisco.com
sip:joe@cisco.com
sip@chuck@cisco.com
```

You can create your own input file based on the above format. however, Cisco recommends that you use the UserList<Timestamp>.txt file as the input file for the Disable Account tool. The UserList<Timestamp>.txt file does not contain any duplicate, disabled, or nonexistent users.

After you run the Disable Account tool, the tool generates a unique, time-stamped log file called DisableAccountLog<Timestamp>.txt in the same directory as the tool. The log file contains details about any failures or errors that occurred.

Before You Begin

You must have read/write permission to AD to run this tool.

Procedure

Step 1 Copy and extract the zip file containing the Cisco user migration tools to the Standard Edition server or Enterprise Edition front-end server.

Note After extraction, if you move any of the Cisco user migration tools to a different location on the Microsoft servers, you must also copy the version.txt file to the new location to ensure that the tool prints out its current version.

Step 2 Open a command prompt and change directory to the location of the Disable Account tool.

Step 3 At the command prompt, enter the following command:

`DisableAccount.exe -s/LDAPServer -f/`*`input_file`* **`-l/logLevel`**

where:

- **`LDAPServer`**—The IP or FQDN of the AD server on which the users exist
- *`input_file`*—The file containing the list of Microsoft server user accounts to disable, UserList<Timestamp>.txt
- **`logLevel`**—The logging level, which must be one of error, info or debug (debug is the recommended setting)

Step 4 Check the DisableAccountLog<Timestamp>.txt log file after each execution of the Disable Account tool to ensure that all users were successfully disabled.

What to Do Next

Verify That Active Directory Updates Synchronized to Microsoft Servers, on page 107

Verify That Active Directory Updates Synchronized to Microsoft Servers

After the Active Directory updates are made to disable the Lync/OCS/LCS accounts, the next step is to verify that those updates have synchronized to the Microsoft server. Verification takes place on the Standard Edition server or Enterprise Edition pool where the disabled Microsoft server account was provisioned. You must wait until the Microsoft server LDAP changes are synched before proceeding with the Delete utility.

Note Depending on your Microsoft server deployment, it may take up to 30 minutes for these changes to synchronize to the Microsoft server.

Procedure

Step 1 Depending on your deployment, do one of the following:

- If you are using Lync Server 2010, choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Control Panel**.
- If you are using OCS 2007 R2, choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2Start > Programs > Administrative Tools > Office Communications Server 2007 R2**.
- If you are using LCS 2005, choose **Start** > **Programs** > **Administrative Tools** > **Live Communications Server 2005Start > Programs > Administrative Tools > Live Communications Server 2005**.

Step 2 Depending on your deployment, check the following:

- For Lync, choose **Users** and ensure that the disabled user no longer appears in the list of users.
- For OCS/LCS, choose **Users** and ensure that the disabled user no longer appears in the list of enabled OCS/LCS users.

What to Do Next

Delete User Data from Database for Migrating Users, on page 108

Related Topics

Disable Account Tool, on page 134

Delete User Data from Database for Migrating Users

Note To delete user data from the Lync/OCS/LCS database for migrating users, you must have read/write access to the Microsoft server database.

The Microsoft server provides an administrative way to delete a user from the Microsoft server database. However, if you delete a user from the database in this way, the user is removed from other users' contact lists. To prevent the user being removed from the contact lists of other Microsoft Lync or Microsoft Office Communicator users, Cisco provides an alternative means of deleting the user from the Microsoft server database.

This alternative tool (`DeleteAccount.exe`) allows you to delete migrating users so that availability requests for these users are later routed to IM and Presence Service. This tool also ensures that the deleted users are not removed from the contact list of any users that remain on the Microsoft server. Running the Delete Account tool is the second step in a two-step process to disable a migrating user on the Microsoft server. The two-step process is as follows:

1. Disable the Microsoft server account for migrating user.
2. Delete the Microsoft server user data for migrating user.

After you disable the account for migrating user, wait until the Microsoft server's LDAP changes are synchronized before proceeding with the Delete utility. The LDAP synchronization can take up to 30 minutes.

Note

- You can run this tool on all supported Microsoft server platforms.
- You can run this tool on any Standard Edition server or Enterprise Edition pool.
- Running this tool has no affect on the capabilities of other Microsoft server users who are signed into Microsoft Lync or Microsoft Office Communicator. However, Cisco recommends that you run this tool during a scheduled maintenance window to reduce the load on the Microsoft server and Active Directory system.

The Delete Account tool reads the list of users to delete from an input file. Each line in the input file represents a contact list owner. The contact list owner is represented by the owner's Microsoft server SIP URI, for example, sip:bobjones@cisco.com. The following is a sample input file:

```
sip:ann@cisco.com
sip:bob@cisco.com
sip:joe@cisco.com
sip@chuck@cisco.com
```

You can create your own input file based on the above format. however, Cisco recommends that you use the UserList<Timestamp>.txt file as the input file for the Delete Account tool. The `UserList<Timestamp>.txt` file does not contain any duplicate, disabled, or nonexistent users.

Running the Delete Account Tool on Standard Edition Deployments

When deleting data for a list of users, you must run this tool once on each Standard Edition server. The database is coresident on the Standard Edition server.

Running the Delete Account Tool on Enterprise Edition Deployments

When deleting data for a list of users, you must run this tool once on each Enterprise Edition pool. The LCS SQL server name or Lync/OCS database instance name to which the Microsoft server's front-end connects must be specified when running the tool.

Caution For Lync Enterprise Edition, you must run this tool first on the back-end database server and then on each front-end server. The Lync database instance name to which the Lync front-end connects must be specified in both options. The name of the database for the front-end servers is rtclocal. The default name of the database for the back-end server is rtc, but that can be changed during system installation.

For LCS/OCS Enterprise Edition, the tool must be run on only the back-end database server.

Procedure

Step 1 Ensure that you have read/write access to the Microsoft server database before you run this tool.

Step 2 Copy and extract the zip file containing the Cisco user migration tools to the Standard Edition server or one of the Enterprise Edition pool servers (front-end or back-end).

Note After extraction, if you move any of the Cisco user migration tools to a different location on the Microsoft server, you must also copy the `version.txt` file to the new location to ensure that the tool prints out its current version.

Step 3 Open a command prompt and change directory to the location of the Delete Account tool.

Step 4 At the command prompt, enter the command as follows:

```
DeleteAccount.exe -s/database_instance -f/input_file -l/logLevel
```

where:

- *database instance*—The database instance name of the Lync/OCS pool or the SQL server instance of the LCS pool
- *input_file*—The file containing the list of Microsoft server user accounts to delete, UserList<Timestamp>.txt
- *logLevel*—The logging level, which must be one of error, info, or debug (debug is the recommended setting)

Note After the command executes, the Delete Account tool generates a unique, time-stamped log file called `DeleteAccountLog<Timestamp>.txt` in the same directory as the tool. The log file contains details about any failures or errors that have occurred.

Step 5 For each Standard Edition server or Enterprise Edition pool, repeat Steps 1 to 3.
For troubleshooting tips, see Delete Account Tool, on page 135

Step 6 If you are deleting user data from a Lync database you must also repeat Steps 2 to 4 on each front-end server. To access the front-end server database, the command in Step 4 must be run locally on the front-end server. In addition, you must use *front-end_server_hostname*`\rtclocal` as the value for the database instance parameter.

What to Do Next

Import Contact Lists for Migrating Users into IM and Presence, on page 110

Import Contact Lists for Migrating Users into IM and Presence

You can use the IM and Presence Service Bulk Administration Tool (BAT) to import Lync/OCS/LCS user contact lists into IM and Presence Service.

Complete the following steps to import the Microsoft server user contact lists into the IM and Presence Service:

1. Upload the CSV File Using BAT.
2. Create a New Bulk Administration Job.
3. Check Results of Bulk Administration Job.

Note The default contact list import rate is based on the server hardware type. You can change the contact list import rate by logging in to the **Cisco Unified IM and Presence Administration** user interface and choosing **System** > **Service Parameters** > **Cisco Bulk Provisioning Service**, then change the variable under Import Users Contact Rate. However, if you increase the default import rate, this results in a higher CPU and Memory usage on IM and Presence Service.

Before You Begin

The procedure to import the Microsoft server user contact lists is one of the final steps in the user migration process. Before you import the Microsoft server user contact lists, you must complete the following procedures:

1. Provision the Microsoft server users on Cisco Unified Communications Manager.

2 Ensure that the Microsoft server users are licensed and assigned to IM and Presence Service.

3 Ensure that the IM and Presence Service Maximum Contact List Size and Maximum Watchers settings are set to unlimited to ensure all contact lists are fully imported. See Set Unlimited Contact Lists and Watchers, on page 96.

4 Run the Export Contact List tool to produce the `ExportedContacts<Timestamp>.csv` file. See Export of Contact Lists for Migrating Users, on page 100.

5 Ensure that the Microsoft server users have been fully disabled on the Microsoft server. See Disable Users on Microsoft Servers, on page 106.

CSV File Upload Using BAT

You must upload the ExportedContacts<Timestamp>.csv file to IM and Presence Service using the BAT. See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for instructions on how to upload the CSV file.

Related Topic

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

What To Do Next

Creation of a New Bulk Administration Job, on page 111

Creation of a New Bulk Administration Job

After you upload the CSV file, you must create a new bulk administration job in the **Cisco Unified CM IM and Presence Administration** user interface to update the user contact lists. See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for instructions on how to create a new bulk administration job.

Related Topic

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

What To Do Next

Results of Bulk Administration Job, on page 111

Results of Bulk Administration Job

When the bulk administration job is complete, the IM and Presence Service Bulk Administration Tool writes the results of the contact list import job to a log file. See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for instructions on how to check the results of the bulk administration job.

What To Do Next

Deploy an IM and Presence Service Supported Client on Users Desktop, on page 112

Related Topics

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager
User Migration Troubleshooting, on page 132

Deploy an IM and Presence Service Supported Client on Users Desktop

After you provision the Lync/OCS/LCS users on Cisco Unified Communications Manager and license them for IM and Presence Service and an IM and Presence Service supported client, you can install the client software on the users' desktops. See *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* for information about deploying IM and Presence Service supported clients.

Related Topics

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

Reset Maximum Contact List Size and Maximum Watcher Size

Before migrating users from Lync/OCS/LCS to IM and Presence Service, Cisco recommends that you set the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service to unlimited. This ensures that each migrated user contact list is fully imported to IM and Presence Service.

After all users have been migrated to IM and Presence Service, reset the Maximum Contact List Size and Maximum Watchers settings on IM and Presence Service to the desired values. The system default value is 200 for Maximum Contact List Size and 200 for Maximum Watchers size.

Note If you are performing a phased migration of users from the Microsoft server to IM and Presence Service, do not reset the Maximum Contact List Size and Maximum Watchers values until all users have been migrated.

The following procedure describes how to set values for the Maximum Contact List Size and Maximum Watchers settings.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. When you change Presence settings, they are applied to all nodes in the cluster; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

Procedure

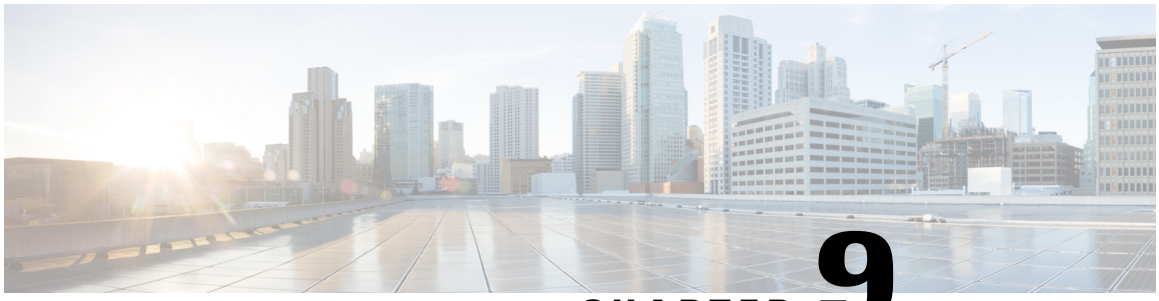
Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Settings**.

Step 2 For **Maximum Contact List Size (per user)**, uncheck the check box for **No Limit** and enter the desired limit.

Step 3 For **Maximum Watchers (per user)**, uncheck the check box for **No Limit** and enter the desired limit.

Step 4 Click **Save**.

Step 5 Restart the Cisco XCP Router on all IM and Presence Service nodes in the cluster. To restart the Cisco XCP Router, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools** > **Control Center – Network Services**.



CHAPTER 9

Interdomain Federation and Intradomain Federation Deployment Integration

- IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers, page 115
- IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers, page 116
- Remote Domain Setup for Interdomain Federation through Intradomain Federation Connections on Microsoft Servers, page 116
- Configure a Static Route for a Remote Domain, page 117
- Remove IM and Presence Service Integration with Microsoft Server Interdomain Federation Capability, page 119

IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers

You can integrate IM and Presence Service with the interdomain federation capability of Microsoft servers.

Microsoft servers support interdomain federation with remote enterprises or public IM providers. This interdomain federation capability is still available to Microsoft Lync or Microsoft Office Communicator users when partitioned intradomain federation is configured between the Microsoft server and IM and Presence Service.

Furthermore, you can configure IM and Presence Service so that users who migrate to an IM and Presence Service supported client can still use the interdomain federation capability that is configured on the Microsoft server.

For information about configuring interdomain federation on IM and Presence Service, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.

Interactions and Restrictions

- Do not use email for federation when you have an integrated interdomain and partitioned intradomain federation deployment. Email address for federation is not supported in deployments where partitioned intradomain federation is configured. Email address for federation is also not supported for interdomain federation if your deployment uses the interdomain federation capabilities of Lync/OCS/LCS. Confirm that email address for federation is not enabled anywhere in the deployment in these deployment scenarios.
- When partitioned intradomain federation with the Microsoft server is enabled, it is also possible to configure both SIP-based and XMPP-based interdomain federation to remote domains on IM and Presence Service. However, this federation capability is available to users on IM and Presence Service supported clients only.

IM and Presence Service Integration with Interdomain Federation Capability of Microsoft Servers

You can integrate IM and Presence Service with the interdomain federation capability of Microsoft servers.

Microsoft servers support interdomain federation with remote enterprises or public IM providers. This interdomain federation capability is still available to Microsoft Lync or Microsoft Office Communicator users when partitioned intradomain federation is configured between the Microsoft server and IM and Presence Service.

Furthermore, you can configure IM and Presence Service so that users who migrate to an IM and Presence Service supported client can still use the interdomain federation capability that is configured on the Microsoft server.

For information about configuring interdomain federation on IM and Presence Service, see *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*.

Remote Domain Setup for Interdomain Federation through Intradomain Federation Connections on Microsoft Servers

IM and Presence Service users can communicate with external domains using either the existing Lync/OCS/LCS interdomain federation connections or using connections to those external domains that you configure directly on IM and Presence Service.

When you configure interdomain federation through existing Microsoft server intradomain federation connections, all requests to the remote domain are routed through the SIP interface between IM and Presence Service and the Microsoft server. You must configure the remote domain on IM and Presence Service to be a Microsoft server SIP Federation domain before you proceed to configure interdomain federation through existing intradomain federation connections. Do this for each remote domain.

See procedures related to adding a SIP federated domain in the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for detailed instructions on how to configure a SIP federation domain.

Choose the following options when you configure a SIP Federation domain for interdomain federation using existing intradomain connections that are configured on Microsoft servers:

- For Domain Name, enter the remote domain.
- For Integration Type, choose **Inter-domain to OCS/Lync**
- Ensure that **the Direct Federation** check box is checked.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on theIM and Presence Service database publisher node within any given cluster.

What To Do Next

Configure a Static Route for a Remote Domain, on page 117

Related Topics

Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Integration Troubleshooting, on page 121

Configure a Static Route for a Remote Domain

When you integrate IM and Presence Service with Lync/OCS/LCS interdomain federation capability, you must configure static routes on IM and Presence Service for each remote domain.

Caution Email address for federation is not supported in deployments where partitioned intradomain federation is configured. Email address for federation is also not supported for interdomain federation if your deployment uses the interdomain federation capabilities of Microsoft servers. Confirm that email address for federation is not enabled anywhere in the deployment in these deployment scenarios.

For Standard Edition Microsoft servers, the static routes must point to the IP address of a specific Standard Edition server.

For Enterprise Edition Microsoft servers, the static routes must point to a specific Enterprise Edition front-end server.

If you are using a Microsoft server's front-end load balancer, note the following:

- See the following URL for a list of load balancers: http://technet.microsoft.com/en-us/office/ocs/cc843611. It is your responsibility to ensure that those load balancers are deployed and managed correctly. Cisco does not support the configuration of static routes to point to such load balancers.
- Cisco recommends that you configure static routes to bypass the front-end load balancer.

For High Availability purposes, you can configure additional backup static routes for each remote domain. The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service publisher node within any given cluster.

Procedure

Step 1 Lin to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Presence** > **Routing** > **Static Routes**.

Step 2 Click **Add New**.

Step 3 Enter the destination pattern value so that the domain, or FQDN, is reversed. For example, if the domain is remote.com, the Destination Pattern value must be .com.remote

Step 4 Choose **domain** for the Route Type.

Step 5 In the Next Hop field, enter the IP address of the next hop.

Step 6 Set the Next Hop Port and the Protocol Type as follows:

- For TLS Encryption:
  - Next Hop Port number is **5061**
  - Protocol Type is **TLS**
- For TCP:
  - Next Hop Port number is **5060**
  - Protocol Type is **TCP**

Step 7 Enter the Priority value as follows:

- For primary static routes, enter the default Priority value of **1**.
- For backup static routes, enter a Priority value of greater than 1. (The lower the value, the higher the priority of the static route.)

Step 8 Leave the default values for all other parameters.

Step 9 Click **Save**.

Related Topics

Integration Troubleshooting, on page 121

Remove IM and Presence Service Integration with Microsoft Server Interdomain Federation Capability

At some stage, you may want to configure IM and Presence Service for interdomain federation with one of the remote domains that you previously configured on Lync/OCS/LCS. The most likely scenario for this is when all Microsoft Lync or Microsoft Office Communicator users have been migrated to IM and Presence Service. At this point, the Microsoft server deployment can be shut down, and any interdomain federation capability can instead be enabled directly from IM and Presence Service.

To remove an IM and Presence Service integration with Microsoft server interdomain federation capability, you must complete Remove Static Route for Remote Domain, on page 119 and Remove the SIP Federation Domain, on page 119.

Remove Static Route for Remote Domain

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Routing** > **Static Routes**.

Step 2 Choose the appropriate static route from the list provided. If no list is shown, click **Find**.

Step 3 Click **Delete Selected**.

Step 4 Click **OK** to confirm the deletion.

What to Do Next

Remove the SIP Federation Domain, on page 119

Remove the SIP Federation Domain

Note If you have a multicluster deployment, you must perform this procedure on each cluster. These settings are cluster-wide; therefore you need to set them only on the IM and Presence Service database publisher node within any given cluster.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Inter-Domain Federation** > **SIP Federation**.

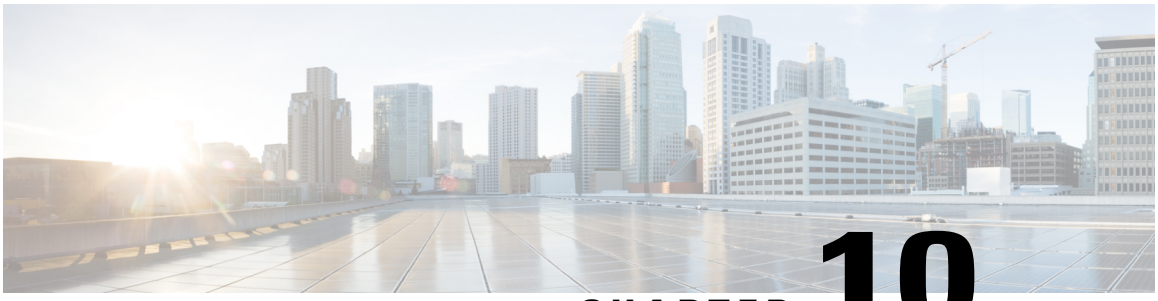
Step 2 Choose the domain from the list provided. If no list is shown, click **Find**.

Step 3 Click **Delete Selected**.

Step 4 Click **OK** to confirm the deletion.

What to Do Next

After you remove the static route to the remote domain and remove the SIP federation domain, you can proceed to configure IM and Presence Service for interdomain federation with the remote domain. See *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager* for more information.



CHAPTER 10

Integration Troubleshooting

- IM and Presence Service Tracing, page 121
- Microsoft Server SIP Tracing, page 124
- Common Integration Problems, page 125
- User Migration Troubleshooting, page 132

IM and Presence Service Tracing

On the IM and Presence Service node, the SIP Proxy is responsible for SIP request routing, while the XCP SIP Federation Connection Manager is responsible for SIP Protocol Translation between Microsoft SIP and native XMPP. Therefore, these services are central to the SIP partitioned intradomain federation integration between IM and Presence Service and Lync/OCS/LCS.

The XCP Router is a core service of IM and Presence Service. It determines whether the request recipient is a Microsoft server user or an IM and Presence Service user.

The locations of the log files are as follows:

- Logs for XCP SIP Federation Connection Manager: `/var/log/active/epas/trace/xcp/log/sip-cm-3_000*.log`
- Logs for SIP Proxy: `/var/log/active/epas/trace/esp/sdi/esp000*.log`
- Logs for XCP Router: `var/log/active/epas/trace/xcp/log/rtr-jsm-1_000*.log`

Example of SIP Proxy Logging

```
2:26:18.719 |PID(25333) sip_protocol.c(5964) Received 536 bytes TCP packet
 from 10.53.56.17:34282SUBSCRIBE sip:ysam@implync.net SIP/2.0^M
From:
<sip:fbear@implync.net>;tag=a4cdaec0-1138350a-13d8-45026-4d755b8a-2162aa7a-4d755b8a^M

To: <sip:ysam@implync.net>^M
Call-ID: a30386f0-1138350a-13d8-45026-4d755b8a-2c25871c-4d755b8a^M
CSeq: 1 SUBSCRIBE^M
Via: SIP/2.0/TCP
10.53.56.17:5080;branch=z9hG4bK-4d755b8a-926d95b4-3c330144^M
```

```
Expires: 7446^M
Accept: application/pidf+xml, application/cpim-pidf+xml^M
User-Agent: Cisco-Systems-Partitioned 8.0^M
Max-Forwards: 70^M
Event: presence^M
Contact: <sip:10.53.56.17:5080;transport=TCP>^M
Content-Length: 0^M
…
22:26:18.719 |ID(25333) sip_sm.c(4977) SIPGW Partitioned Fed UA Header
found in this request
22:26:18.719 |ID(25333) sip_sm.c(5010) This is a partitioned federation
request, skip User Location DB lookup
22:26:18.719 |ID(25333) sip_sm.c(5200) This is an outbound Partitioned
federation request.
 22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1435)
 Routing: dipping for cuplcs.net
22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1473)
 Routing: Found domain route for cuplcs.net:10.53.56.18:5061;TLS pwf 1:1:5
22:26:18.719 |ID(25333) sip_dns.c(811) "A" Query for 10.53.56.18
successful, Got 1 IP addresses
22:26:18.719 |ID(25333) sip_dns.c(139) A Record : 10.53.56.18
```

Example of SIP Federation Connection Manager Logging

The following is a extract from an outbound request log:

```
21:48:44.277 |SIPGWDir.cpp:463: [FROM XMPP] <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'/>...
...
21:48:44.743 |SIPGWController.cpp:622: Skipping DNS lookup: <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWController.cpp:704: Entering _handleOutContinue:
<presence from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWController.cpp:989: _findSession (JID):
local(fbear@implync.net) remote(ysam@implync.net)
21:48:44.743 |SIPGWController.cpp:999: _findSession: Session not found
21:48:44.743 |SIPHostInfo.cpp:82: hostinfo(0x09a10ce8) refInc: 3
cuplcs.net:cuplcs.net
21:48:44.743 |SIPGWSession.cpp:58: Creating SIPGWSession sess=0x09a5a090
 local=fbear@implync.net remote=ysam@implync.net
21:48:44.743 |SIPGWController.cpp:1017: _findSession: Made new session:
sess=0x09a5a090 local(fbear@implync.net) remote(ysam@implync.net)
21:48:44.743 |SIPGWSession.cpp:990: sess=0x09a5a090 Entering handleOut:
<presence from='fbear@implync.net' to='ysam@implync.net' type='probe'/>
21:48:44.743 |SIPGWSession.cpp:1090: _createOutgoingSubs
local=fbear@implync.net, remote=ysam@implync.net
48:44.744 |SIPSubs.cpp:1037: from=<sip:fbear@implync.net>
to=<sip:ysam@implync.net> local_contact=sip:10.53.56.17:5080;transport=TCP
 remote_contact=sip:ysam@implync.net
```

Example of XCP Router Logging

```
12:29:24.762 |debug sdns_plugin-1.gwydlvm453 sdns_plugin handling:<presence
 type='subscribed' to='ysam@implync.net'
from='bbird@implync.net'><status>Already Subscribed</status></presence>
12:29:24.762 |debug ConnectionPool.cpp:166 connection pool checkout:
ccm2/dbuser (success)
```

```
12:29:24.762 |debug IdsODBC.cpp:648 Performing SQL operation select userid,
 jsmid from enduser, enterprisenode where my_lower(xep106userid) =
my_lower(?) and primarynodeid=id
12:29:24.763 |debug ODBCConnection.cpp:315 (elapsed 0.002407) select
userid, jsmid from enduser, enterprisenode where my_lower(xep106userid)
= my_lower(?) and primarynodeid=id
12:29:24.763 |debug CUPDatabaseAlgorithm.cpp:311 This is probably a
Partitioned OCS user ... redirecting to cm-3-sip-fed-s2s.gwydlvm453
component
12:29:24.763 |debug IdsODBC.cpp:229 (elapsed 0.000137) rollback
12:29:24.763 |debug ConnectionPool.cpp:207 connection pool checkin:
ccm2/dbuser (success)
12:29:24.763 |debug sdns_plugin-1.gwydlvm453 sdns_plugin redirecting to:
 cm-3-sip-fed-s2s.gwydlvm453
```

You can enable debug tracing for the SIP Proxy, XCP SIP Federation Connection Manager and XCP Router on the Cisco Unified IM and Presence Service Serviceability user interface.

Configure Tracing on the IM and Presence Service

The following procedure describes how to configure tracing for the SIP Proxy, XCP SIP Federation Connection Manager and XCP Router services on the Cisco Unified IM and Presence Serviceability GUI. Repeat this procedure for each service that you want to configure for tracing.

Caution Debug level tracing can affect system performance. Enable debug level tracing only when required and reset to default log settings after the investigation is complete.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace** > **Configuration**.

Step 2 Choose the IM and Presence Service node, and click **Go**.

Step 3 Choose **IM and Presence Services** from the **Service Group** drop-down list, and click **Go**.

Step 4 From the Service drop-down list, choose one of the following options and click **Go**:

a) Cisco SIP Proxy
b) Cisco XCP SIP Federation Connection Manager
c) Cisco XCP Router

Step 5 Check the check box for **Trace On**.

Step 6 In the Trace Filter Settings area, choose the Debug Trace Level from the drop-down list. If you want to enable debug level tracing on the traces choose **Debug**.

Step 7 When you configure tracing for the SIP Proxy, there are a number of trace options under Trace Filter Settings. Check the check boxes for the following traces:

a) Enable SIP TCP Trace
b) Enable SIP TLS Trace
c) Enable Server Trace
d) Enable SIP Message and State Machine Trace
e) Enable Method/Event Routing Trace

f) Enable Routing Trace

Step 8 Click **Save**.
See the Cisco Unified IM and Presence Serviceability Online Help for more information about initiating debug tracing for each of these services.

Related Topics

Microsoft Server SIP Tracing, on page 124

Microsoft Server SIP Tracing

The Lync/OCS/LCS SIP Proxy component is responsible for all SIP request routing. To debug any routing issues, you can enable debug tracing on the Microsoft server (Standard Edition or Enterprise Edition) using the method that is specific to your Microsoft server.

Enable SIP Tracing on Lync

The following procedure describes how to enable SIP tracing on Lync.

Procedure

Step 1 Choose **Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Logging Tool**.
Step 2 In the Components area, check the **SIPStack** check box.
Step 3 Set Logging Level to All and click **Start Logging**.
Step 4 When you are ready to stop the trace click **Stop Logging**.
Step 5 Choose **Analyze Log Files** to view the logs.
Step 6 For a more structured analysis of the logs, download the Snooper tool and use it to view the log files.

Related Topics

IM and Presence Service Tracing, on page 121
Snooper Tool

Enable SIP Tracing on OCS

The following procedure describes how to enable SIP tracing on OCS.

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Office Communications Server 2007 R2**.
Step 2 Do one of the following depending on the edition:

a) If you are using Standard Edition, right-click on the OCS server name and choose **Logging Tool** > **New Debug Session**.
b) If you are using Enterprise Edition, right-click OCS pool name and choose **Logging Tool** > **New Debug Session**.

Step 3 In the Components area, check the **SIPStack** check box and in the Level area, click **All**.
Step 4 When you are ready to begin logging, click **Start Logging**.
Step 5 When you are ready to stop logging, click **Stop Logging**.
Step 6 Click **Analyze Log Files** to view the OCS SIP Proxy log analysis.

Related Topics

IM and Presence Service Tracing, on page 121
Snooper Tool

Enable SIP Tracing on LCS

The following procedure describes how to enable SIP tracing on LCS.

Procedure

Step 1 Choose **Start > Programs > Administrative Tools > Live Communications Server 2005**.
Step 2 Right-click the LCS server FQDN and choose **Properties**.
Step 3 Choose the **Logging** tab and check the **Enable Logging** check box.
Step 4 Set Logging Level to **4** (Debug).
Step 5 Choose a location to store the log files.
Step 6 Accept all other defaults and click **OK** to close the Properties window and enable logging.
Step 7 When you are ready to stop logging, choose the LCS server FQDN and choose **Properties** again.
Step 8 Choose the **Logging** tab and choose **Force Rollover Now**.
Step 9 Uncheck the **Enable Logging** check box and click **OK** to close the Properties window.
Step 10 Open the latest log file in your chosen location.
Step 11 For a more structured analysis of the logs, download the Snooper tool and use it to view the log files.

Common Integration Problems

This section describes some common integration problems.

Microsoft Server User Does Not Receive Pop-up when Added to IM and Presence Service Contact List

Troubleshooting Steps

1. If a valid availability state is shown for the contact, check whether the Microsoft Lync or Microsoft Office Communicator user previously accepted a subscription from the IM and Presence Service client user.

   Microsoft server subscription authorization is permanent, which means that if an IM and Presence Service client user removes and re-adds a Microsoft Lync or Microsoft Office Communicator user, no second pop-up appears.

2. If the "Waiting for Confirmation" state is shown for the contact, perform the remaining troubleshooting steps as required.

   - Ensure that the contact has a valid MOC SIP URI.
   - Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.
   - Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
   - Check that the partitioned federation routing mode applies to the chosen deployment.
   - Advanced Routing is supported only in single-cluster IM and Presence Service deployments.
   - Ensure that the IM and Presence Service static routes are correctly configured to route requests to the Microsoft server. To do this, check the SIP Proxy logs on the IM and Presence Service user home node to see whether the SIP Proxy returns a SIP 408 Request Timeout error for the SIP NOTIFY request to the Microsoft server.
   - If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
   - If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 131.
   - Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP NOTIFY.
   - At the very least, there must be an IP address entry for each IM and Presence Service node.
   - If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

Microsoft Server User Receives a Pop-up when Added to an IM and Presence Service Contact List but Has No Availability after Accepting

Troubleshooting Tip

Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Lync/OCS/LCS servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.

IM and Presence Service User Does Not Receive a Pop-up when a Microsoft Lync or Microsoft Office Communicator User Adds the User to their Contact List

Troubleshooting Steps

1. If a valid availability state is shown, check whether IM and Presence Service is configured to automatically approve subscription requests from users within the local presence domain. If this feature is enabled, IM and Presence Service automatically approves the request without a pop-up to the IM and Presence Service user.
2. Otherwise, if "Status Unknown" or "Presence Unknown" is shown for the contact, perform the remaining troubleshooting steps as required.
3. Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.
4. Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
5. Check that the partitioned federation routing mode applies to the chosen deployment.

   Advanced Routing is supported only in single-cluster IM and Presence Service deployments.
6. If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
7. If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 131.
8. Ensure that a static route that points to the routing IM and Presence Service node is configured on each Lync/OCS/LCS Standard Edition server or Enterprise Edition pool.
9. Ensure that each IM and Presence Service node is resolvable by Domain Name Service (DNS) from the Microsoft server deployment.
10. Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP NOTIFY message.
    a. At the very least, there must be an IP address entry for each IM and Presence Service node.
    b. If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

11 Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Microsoft servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.

12 If this is a multicluster IM and Presence Service deployment, ensure that inter-cluster peering is correctly configured.

   a Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Inter-Clustering** on the publisher node of the cluster that contains the designated routing IM and Presence Service node.
   b Ensure that the list of inter-cluster peers includes a peer for the cluster on which the IM and Presence Service user is provisioned and that the number of Associated Users for that peer is greater than 0.
   c Choose the inter-cluster peer to validate the Inter-cluster Peer Status.
   d Ensure that there are no errors highlighted.

Microsoft Server User Does Not Receive IMs Sent by an IM and Presence Service User

Troubleshooting Steps

1 Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Service node.

2 Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.

3 Check that the partitioned federation routing mode applies to the chosen deployment.

   Advanced routing is supported only in single-cluster IM and Presence Service deployments.

4 Ensure that IM and Presence Service static routes are correctly configured to route requests to Lync/OCS/LCS. To do this, check the SIP Proxy logs on the IM and Presence Service user home node to see whether the SIP Proxy returns a SIP 408 Request Timeout error for the SIP INVITE request to the Microsoft server.

5 If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.

6 If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 131.

7 Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP INVITE request.

   a At the very least, there must be an IP address entry for each IM and Presence Service node.
   b If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.

IM and Presence User Does Not Receive IMs Sent by a Microsoft Server User

Troubleshooting Steps

1. Ensure that the Cisco SIP Proxy and Cisco SIP Federation Connection Manager services are running on each IM and Presence Server node.
2. Ensure that partitioned intradomain federation is enabled on each IM and Presence Service cluster.
3. Check that the partitioned federation routing mode applies to the chosen deployment.

   Advanced routing is supported only in single-cluster IM and Presence Service deployments.
4. For Microsoft Lync, ensure that TLS encryption is configured.
5. If TLS encryption is configured, use Wireshark or an equivalent monitoring tool to verify that the TLS handshake is successful.
6. If the TLS handshake is still failing, for more TLS troubleshooting steps see TLS Handshake Errors between the IM and Presence Service and Microsoft Servers, on page 131.
7. Ensure that a static route that points to the routing IM and Presence Service node is configured on each Lync/OCS/LCS Standard Edition server or Enterprise Edition pool.
8. Ensure that each IM and Presence Service node is resolvable by DNS from the MIcrosoft server deployment.
9. Ensure that a Microsoft server Host Authorization entry exists for the IM and Presence Service node that is sending the SIP INVITE.
   a. At the very least, there must be an IP address entry for each IM and Presence Service node.
   b. If TLS encryption is configured, a second FQDN entry is also required for each IM and Presence Service node.
10. Ensure that the IM and Presence Service Access Control List (ACL) allows requests from all Microsoft servers/pools. If there is an ACL issue, the following entry appears in the SIP Proxy logs of the routing IM and Presence Service node: ACL – upstream not trusted – need to authenticate.
11. If this is a multicluster IM and Presence Service deployment, ensure that inter-cluster peering is correctly configured.
    a. Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Presence** > **Inter-Clustering** on the publisher node of the cluster that contains the designated routing IM and Presence Service node.
    b. Ensure that the list of inter-cluster peers includes a peer for the cluster on which the IM and Presence Service user is provisioned and that the number of Associated Users for that peer is greater than 0.
    c. Click the inter-cluster peer to validate the Inter-cluster Peer Status.
    d. Ensure that there are no errors highlighted.

Microsoft Server User Updates and IMs Take up to 40 Seconds to Appear

Troubleshooting Steps

The most common reason for such delays is missing DNS configuration within the deployment. IM and Presence Service performs a reverse DNS lookup of the Lync/OCS/LCS IP address from which it received the inbound SIP requests. If the IP address does not resolve to a hostname, the reverse lookup times out after approximately 20 seconds. If this occurs, the following log is generated in the SIP Proxy logs: incoming ACL check took over 2 seconds – check DNS.

To solve this problem, ensure that a DNS Pointer (PTR) record exists for each Microsoft server IP address.

When Advanced Routing Is Enabled, No Availability Is Exchanged Between IM and Presence Service and Microsoft Server

Troubleshooting Steps

1. Verify that Cisco Unified Communications Manager is synchronizing user data from Active Directory for all Lync/OCS/LCS users.

   Advanced Routing is dependent on the Microsoft server SIP URI being synchronized to Cisco Unified Communications Manager from Active Directory.
2. Verify that Advanced Routing is enabled only if this is a single-cluster IM and Presence Service deployment.

IM and Presence Service User Does Not Appear in the Microsoft Server Address Book

Troubleshooting Steps

1. Ensure that a full synchronization by the Lync/OCS/LCS Address Book Service has taken place since the IM and Presence Service user was migrated from the Microsoft server. This synchronization happens nightly by default.
2. Request the Microsoft Lync or Microsoft Office Communicator user to sign out and sign in to trigger a download of the new address book. By default, it may take more than an hour to download the new address book from the Microsoft server.
3. If the IM and Presence Service user was previously a Microsoft Lync or Microsoft Office Communicator user, ensure that the IM and Presence Service user still has their old Microsoft server SIP URI populated in Active Directory (msRTCSIP-PrimaryUserAddress).
4. If the IM and Presence Service user was not previously a Microsoft Lync or Microsoft Office Communicator user or if their old Microsoft server SIP URI has been cleared from Active Directory, you must manually populate the Active Directory msRTCSIP-PrimaryUserAddress field to ensure that the IM and Presence Service user appears in the Microsoft server address book. You must enter sip:user's_uri in the msRTCSIP-PrimaryUserAddress field.

IM and Presence Service Unable to Route Interdomain Federation Requests through Microsoft Server Deployment

Troubleshooting Steps

1. Verify that the Lync/OCS/LCS deployment is correctly configured for interdomain federation. To do this, ensure that Microsoft server users can federate.
2. Ensure that the Cisco SIP Proxy and the Cisco SIP Federation Connection Manager are running on each IM and Presence Service node.
3. Ensure that IM and Presence Service is configured for interdomain federation to the external domain and that Direct Federation is enabled.
4. Ensure that a static route is configured on IM and Presence Service for the external domain and that the static route points to the Microsoft server.
5. Ensure that the external domain is included in the IM and Presence Service Access Control List (ACL).

TLS Handshake Errors between the IM and Presence Service and Microsoft Servers

Troubleshooting Steps

1. Verify that Lync/OCS/LCS has been configured to listen for mutual TLS connections on port 5061.
2. Verify that the IM and Presence Service Application Listeners have been configured such that the Presence Peer Authentication Port is set to 5061.
3. Verify that the IM and Presence Service certificate is signed by the same certificate authority as the Microsoft server.
4. Verify that none of the Microsoft server or IM and Presence Service certificates have expired.
5. Verify that the Microsoft server certificate is configured for both Server Authentication and Client Authentication.
   - Such certificates have an OID value of "1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2"
   - If the certificate is configured for Server Authentication only, it has an OID value of "1.3.6.1.5.5.7.3.1"
6. Verify that the IM and Presence Service TLS Peer Subjects list contains the Subject Common Name (CN) used in certificates provided by the Microsoft server during TLS handshaking.
7. Verify that the IM and Presence Service TLS Peer Authentication TLS Context is configured correctly and that all TLS Peer Subjects have been chosen.

Incorrect SIP URI Specified for Microsoft Lync or Microsoft Office Communicator Users when Added to Cisco Unified Personal Communicator Contact List

Troubleshooting Step

Verify that the Cisco Unified Personal Communicator registry configuration is correct, in particular the LDAP_AttributeName_uri and LDAP_UriSchemeName subkeys. For more information see the chapter for Configuring Active Directory for in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* .

Display Names not Shown for Microsoft Lync or Microsoft Office Communicator Contacts on Cisco Unified Personal Communicator

Troubleshooting Step

Verify that the Cisco Unified Personal Communicator registry configuration is correct, in particular the LDAP_AttributeName_uri and LDAP_UriSchemeName subkeys. For more information, see topics related to configuring Active Directory in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

User Migration Troubleshooting

This section describes user migration tracing and common user migration problems.

User Migration Tracing

This section describes tools used for user migration tracing.

Export Contact List Tool

The Export Contact List tool allows an administrator to export contact lists in bulk from Lync/OCS/LCS for migrating users. With each run the tool generates a log file called ExportContactsLog<Timestamp>.txt. The log file contains details about any failures or errors that have occurred. The log file is saved to the same location as the tool itself.

Some common reasons why errors can occur include:

- Incorrect input filename specified
- Misspellings in input file
- Users specified are not associated with the Microsoft server/pool that the tool is being run against

The following is an example of a log file for the Export Contact List tool:

```
>>------------------- 18/05/2011 16:59:38 ------------------->>Version:
2.1
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Current line item is: sip:ExampleUser@dtstfedcup2.com
[DEBUG] Exit>>
ExportContacts.ExportContactsUtilities.getAllSipUriFromStandardFile
[DEBUG] Enter>>
ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[DEBUG] Total number of users found is: 1
[DEBUG] Processing user number: 1
[INFO]  Preparing to get contacts for User
[sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Searching for userInstanceId [SELECT * FROM MSFT_SIPESUserSetting
 WHERE PrimaryURI = 'sip:ExampleUser@dtstfedcup2.com']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com,
InstanceId : {7D777FD5-A8F6-8243-B4D6-7F331008C58C}
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Searching for contacts [SELECT * FROM MSFT_SIPESUserContactData
WHERE UserInstanceID = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found contact:  SIPURI : [SIP:lyncContact@dtstfedcup2.com] with
GroupId: [1]
[DEBUG] Found contact:  SIPURI : [SIP:ExampleUser@dtstfedcup2.com] with
GroupId: [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getGroups
[DEBUG] Searching for groups [SELECT * FROM MSFT_SIPESUserContactGroupData
 WHERE UserInstanceID = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found group:  groupName : [General] with GroupId: [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getGroups
[INFO]  User Processed Successfully
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>>
ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[INFO]  Summary:
[INFO]  1 users successfully processed
[INFO]  0 users not found
[INFO]  0 users could not be processed due to errors
<<------------------- 18/05/2011 16:59:41 -------------------<<
```

Related Topics

IM and Presence Service BAT Contact List Import, on page 137

Disable Account Tool

The Disable Account tool connects to Active Directory (AD) and updates the users' Lync/OCS/LCS attributes to disable their Microsoft server account. With each run the tool generates a log file called DisableAccountLog<Timestamp>.txt. The log file contains details about any failures or errors that have occurred. The log file is saved to the same location as the tool itself.

Some common reasons why errors can occur with this tool include:

- Incorrect input filename specified
- Misspellings in input file
- User does not exist in the Microsoft server database
- The administrator who is running the tool does not have read/write permissions for the AD
- The administrator did not allow enough time for the changes applied to AD by this tool to propagate down to the Microsoft server database. The migration may fail if the administrator moves on to the next migration step without validating that the changes have taken effect in the Microsoft server database.

The following is an example of a log file for the Disable Account tool:

```
>>------------------- 18/05/2011 17:02:07 ------------------->>Version:
2.0
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.AccountDisable.DisableUsersInFile
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.GetSipUriFromLine
[INFO]  Preparing to Disable Communications Server Account for User
[sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> DisableAccount.LdapConnection.DisableAccount
[INFO]  Searching for user [sip:ExampleUser@dtstfedcup2.com]
[INFO]  Search results returned
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[INFO]  Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com,
DisplayName : Example User, Enabled : True
[DEBUG] Committed changes to the AD
[INFO]  User Account Disabled
[DEBUG] Exit>> DisableAccount.LdapConnection.DisableAccount
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.DisableUsersInFile
[INFO]  Summary:
[INFO]  1 users successfully processed
[INFO]  0 users not found
```

```
[INFO]  0 users could not be processed due to errors
<<------------------- 18/05/2011 17:02:08 -------------------<<
```

For more information about using the Disable Account tool, see topics related to disabling Microsoft server accounts for migrating users.

Delete Account Tool

The Delete Account tool allows you to delete migrating users so that presence requests for these users are later routed to IM and Presence Service while ensuring the deleted users are not removed from the contact list of any users that remain on Lync/OCS/LCS. After you run the Delete Account tool, the tool generates a log file called `DeleteAccountLog<Timestamp>.txt` to the same directory as the tool. The log file contains details about any failures or errors that have occurred.

Some common reasons why errors can occur with this tool include:

- Incorrect input filename specified
- Incorrect database instance name specified
- Misspellings in the input file
- User does not exist in the Microsoft server database

The following is an example of a log file for the Delete Account tool:

```
>>------------------- 02/12/2013 15:13:50 ------------------->>
Version: 10.x.x-xx
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Attempting to Open connection with String :
Server=lyncServer\rtclocal;Database=rtc;Trusted_Connection=yes;
[DEBUG] Connection Opened Ok
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Resource']
[DEBUG] Found id [1077578877]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the Resource Table, appears to be a valid Communications
Server Database
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Endpoint']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Container']
[DEBUG] Found id [1202103323]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'HomedResource']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'CertificateStore']
[DEBUG] Found id [1826105546]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the CertificateStore table, dealing with a version of Lync.
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
```

```
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'ForestDirectory']
[DEBUG] Found id [853578079]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO]  Found the ForestDirectory table, Creating Lync2013 Connection
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.CheckConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.CheckConnection
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DisableUsersInFile
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[INFO]  Preparing to Delete Communications Server Data for User
[lyncUser@lyncDomain.net]
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[INFO]  Found user [lyncUser06@cork.com] with ResourceId [1010], proceeding
 to delete data
[DEBUG] Enter>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Ran dbo.RtcpDeleteHomedResourceTransaction for resource [1010]
[DEBUG] Deleted CachedContainerMember for resource [1010]
[DEBUG] Deleted ContainerMemberUser for resource [1010]
[DEBUG] Deleted PromptedSubscriber for resource [1010]
[DEBUG] Deleted Delegate for resource [1010]
[DEBUG] Ran RtcpDeleteConferenceParticipantByEnterpriseId for resource
[1010]
[DEBUG] Deleted UserPolicy for resource [1010]
[DEBUG] Deleted ResourcePhone for resource [1010]
[DEBUG] Deleted RtcItem for resource [1010]
[DEBUG] Deleted PUIDDirectory for resource [1010]
[DEBUG] Deleted ResourceDirectory for resource [1010]
[DEBUG] Committing transaction for resource [1010]
[INFO]  Completed Updates for resource [1010]
[DEBUG] Exit>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DisableUsersInFile


Summary:
 Users successfully processed:      1
 Users not found:                   0
 Users not processed due to errors: 0
<<------------------- 02/12/2013 15:13:50 -------------------<<
```

For more information about using the Delete Account tool, see topics related to deleting user data from the database for migrating users.

IM and Presence Service BAT Contact List Import

The IM and Presence Service Bulk Administration Tool (BAT) tool writes the results of the contact list import job to a log file. The log file contains the following information:

- The number of contacts that were successfully imported.
- The number of internal server errors that were encountered while trying to import the contacts.
- The number of contacts that were not imported (ignored). The log file lists a reason for each ignored contact at the end of the log file.
- The number of contacts in the CSV file that were unprocessed due to an error that caused the BAT job to finish early. This error rarely occurs.

To access this log file, complete the following procedure:

1. Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Bulk Administration** > **Job Scheduler**.
2. Click **Find**, and then choose the Job ID of the contact list import job.
3. Click the **Log File Name** link to open the log.

If you require further detail on any BAT job, see the Bulk Provisioning Service debug logs. You can access these logs at the following location: `/var/log/active/cm/trace/bps/log4j/bps000*.txt`

You can enable debug logging for the Bulk Provisioning Service on the **Cisco Unified IM and Presence Serviceability** user interface.

Configure Bulk Provisioning Service Logging on the IM and Presence Service

The following procedure describes how to configure Bulk Provisioning Service logging on IM and Presence Service.

Caution Debug level tracing can affect system performance. Enable debug level tracing only when required and reset to default log settings after the investigation is complete.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace** > **Configuration**.

Step 2 Choose the IM and Presence Service node and click **Go**.

Step 3 Choose **Database and Admin Services** from the Service Group drop-down list and click **Go**.

Step 4 Choose the **Bulk Provisioning Service** from the Service drop-down list and click **Go**.

Step 5 Choose **Trace On**.

Step 6 In the Trace Filter Settings, choose the Debug Trace Level. If you want to enable debug level on the traces, choose **Debug**.

Step 7 Click **Save**.

Related Topics

Export Contact List Tool, on page 132

Common User Migration Problems

This section describes some common user migration problems.

Application Failed to Initialize Properly - Error Occurs When Running Any of the User Migration Tools

Troubleshooting Steps

While attempting to run any of the user migration tools you may receive the following error: "Application failed to initialize properly". The reason for this error is that you are attempting to run the user migration tools without the .NET 1.1 Framework installed. Each of the user migration tools that Cisco provides requires that at least version 1.1 of the .NET Framework is installed on the server where you are running the tool.

Export Contact List Tool does not Produce an Output File for Lync Users

Troubleshooting Steps

To export contact lists from a Lync server you must include the database instance parameter. If you omit the database instance parameter or enter an incorrect database parameter, an error is written to the Export Contact List log. Check the log to determine whether you omitted the database parameter or entered an incorrect parameter.

Follow these steps to find the database instance for each server/pool:

1. Open a powershell window on a front-end server in the pool.
2. Run the following cmdlet:

```
Get-CsManagementConnection
```

The database instance name is the value of the Data Source parameter in the command output.

Export Contact List Tool Log Shows getAndPrintContactsForUsers Error

Troubleshooting Steps

If you run the export tool for Lync users and see the following error in the log, “Error occurred in getAndPrintContactsForUsers”, then the Export Contact List tool cannot connect to the Lync database. Verify that the user account running the tool has the appropriate read permissions for the Lync database. Verify that dbo execution account privileges are granted to the RTC database. If this doesn't solve the issue, verify that there are no typographic errors in the database instance name.

Export Contact List Tool - Log Summary Shows Several Users as Not Found

Troubleshooting Steps

1. If you are using an IM and Presence Service exported file as the input, check that the correct domain is being used for the -d/ parameter and that there are no typographic errors in the file.
2. If you are using a SIP URI file as the input, check that the users are valid (exist in Active Directory [AD] and Lync/OCS/LCS) and that they are entered correctly in the input file with the "sip:" prefix.
3. If you are not using an IM and Presence Service exported file or a SIP URI file as the input, or if you are using the OU input file, the user accounts are most likely disabled in AD. Re-enable the user accounts and run the tool again.

Export Contact List Tool - Tool Does Not Show the Progress Bar and Does Not Produce an Output File of Exported Contacts when Run in Normal Mode

Troubleshooting Steps

1. Check for the following error in the Export Contact List log: "Unable to connect to LDAP using IP/FQDN/Hostname: [some_ip_or_hostname]."
   a. If the error exists, check that the address supplied for the Active Directory (AD) server is correct.
   b. If the address supplied is valid, then ping the AD server to check that there is network connectivity between it and the Lync/OCS/LCS server.
   c. If there is connectivity, ensure that the user has the required privileges to access the AD server.
2. Check for the following error in the Export Contact List log: "Failed to open file…."
   a. If the error exists, the filename used for the -f/ parameter is misspelled or invalid.
   b. Check also that the input file does not contain spaces or special characters in its filename.
3. If you are running the Export Contact List Tool on OCS or LCS, ensure that you did not enter the database instance parameter. The database instance parameter is needed to export contacts from Lync only.

Disable Account Tool - Log Shows Unable to Connect to LDAP Using IP/FQDN/Hostname

Troubleshooting Steps

1. Check that the address supplied for the Active Directory (AD) server is correct.
2. If the address supplied is valid, ping the AD server to check that there is network connectivity between it and the Lync/OCS/LCS server.
3. If there is connectivity, ensure that user has the required privileges to access the AD server.

Delete Account Tool - Unable to Find the Microsoft Server Database or Server Instance

Troubleshooting Steps

1. The Delete Account tool must be run against each database instance (Lync/OCS) and SQL server instance (LCS) to ensure that the account is correctly deleted.
2. For OCS, follow these steps to find the database instance for each server/pool:
   a. On the OCS management console, choose the pool name under the Enterprise Pools (Enterprise Edition) or the server name under Standard Edition Servers (Standard Edition).
   b. In the right pane, choose the **Database** tab.
   c. The database instance name is the first item under **General Settings**.
3. For LCS, follow these steps to find the SQL server instance for each server/pool:
   a. Choose the pool name under **Forest** > **Domains** > **[domain name]** > **Live Communications servers and pools** > **[pool name]**.
   b. In the right pane, choose the **Status** tab.
   c. The first item is the SQL server instance.
4. For Lync, follow these steps to find the database instance for each server/pool:
   a. Open a powershell window on a front-end server in the pool.
   b. Run the following cmdlet:

      ```
      Get-CsManagementConnection
      ```

      The database instance name is the value of the Data Source parameter in the returned output.

Delete Account Tool - Log Shows Error While Connecting to the SQL Server

Troubleshooting Steps

1. Check the Delete Account tool logs to see the reason for this error. If the error is “The user is not associated with a trusted SQL Server connection”, the user running the tool does not have the required privileges to write to the Lync/OCS/LCS database.
2. Rerun the tool with a user account that has the required privileges.

BAT Contact List Update - Uploaded Contact List File Not in Drop-Down List

Troubleshooting Steps

1. Log in to the **Cisco Unified Communications Manager IM and Presence Administration** user interface. Choose **Bulk Administration** > **Upload/Download Files** and click **Find**.
2. Check that the file exists and that its function type is Import Users' Contacts – Custom File.

3 If a file exists with the incorrect function type, delete the file. If you deleted the file, or there is no file, upload the file again and ensure that its target is Contact Lists and its transaction type is Import Users' Contacts – Custom File.

BAT Contact List Update - No Log file Exists on Results Page after BAT Job

Troubleshooting Steps

If the log for the BAT import contacts job is missing from the job result page, the BAT job was run from a subscriber node. The log is accessible only from the publisher node. Log in to **Cisco Unified Communications Manager IM and Presence Administration** on the publisher node to view the log.

BAT Contact List Update - A User's Contacts Are Not Imported During BAT Job

Troubleshooting Steps

1 Check the job results log file for any specific errors.

2 Ensure that the user is licensed for IM and Presence.

3 Ensure that the user is assigned to a node within this cluster.

4 Ensure that the contact's domain is valid.

BAT Contact List Update - A User's Contacts Are Partially Imported During BAT Job

Troubleshooting Steps

1 Check the job results log file for any specific errors.

2 Ensure that the missing contacts are in a valid format in the CSV file.

3 Check that the user’s number of contacts does not exceed the Maximum Contact List Size on the system.

4 Check that the user’s number of watchers does not exceed the Maximum Watchers on the system.

BAT Contact List Update - No Contacts are Imported During BAT Job

Troubleshooting Steps

1 Check the job results log file for any specific errors.

2 Ensure that the import file is in a valid format.

3 Ensure that all the users are licensed for IM and Presence Service.

4 Ensure that all the users are assigned on the local cluster.

5 Ensure that the Cisco Presence Engine service is running on all nodes within the cluster.

Migrating User Status Appears as Status Unknown or Presence Unknown to Microsoft Server Users during the Migration Process

Troubleshooting Steps

1. Ensure that contacts have been fully migrated to IM and Presence Service as described in this document.

   There is a period during the migration process when availability of migration contacts is not visible to Microsoft Lync or Microsoft Office Communicator users. Cisco recommends that user migration takes place during a scheduled maintenance window to reduce the occurrence of such issues.

2. Request Microsoft Lync or Microsoft Office Communicator users to sign out and sign in again.

   After the migrated contacts are imported into IM and Presence Service, Microsoft server users do not see availability for these contacts until they have signed out and back in to their clients.

3. If the problem persists, ensure that the migration steps were correctly followed, as defined in this document.
   - Verify that the updates that were applied by the Disable Account tool were synchronized to Lync/OCS/LCS before you ran the Delete Account tool.
   - Ensure that you ran the Delete Account tool on all Standard Edition Microsoft servers or Enterprise Edition pools.
   - If these steps were not performed correctly, then repeat to resolve this issue as follows:
     - Run the Disable Account tool.
     - Verify that the AD updates made by the Disable Account tool have synchronized to the Microsoft server.
     - Run the Delete Account tool.

4. If migrated contacts are still appearing with a state of “Presence Unknown” there may be an issue with the integration between the IM and Presence Service and the Microsoft server. To help troubleshoot integration issues, see Common Integration Problems, on page 125.