



Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager, Release 11.0(1)

First Published: 2015-06-08

Last Modified: 2018-11-05

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



CONTENTS

CHAPTER 1

Overview of this Integration 1

- Basic Federated Network 1
- Intercluster and Multinode Deployments 3
 - SIP Federation Deployments 3
 - XMPP Federation Deployments 4
- High Availability and Federation 4
 - High Availability for SIP Federation 4
 - High Availability for XMPP Federation 5
- Cisco Adaptive Security Appliance Deployment Options 6
- Presence Subscriptions and Blocking Levels 8
- Availability State Mappings 10
 - Availability State Mappings for Microsoft OCS 10
 - Availability State Mappings for Microsoft Lync 12
 - Availability State Mappings for XMPP Federation 13
- Instant Messaging 15
 - Instant Message Flow for SIP Federation 15
 - Availability and Instant Message Flow for XMPP Federation 16
- Federation in Deployments with Multiple Domains 18
- Federation and Subdomains 18

CHAPTER 2

Preparations for this Integration 21

- Supported Interdomain Federation Integrations 21
 - Presence Web Service API Support 22
- Hardware Requirements 22
- Software Requirements 22
- Integration Preparation 23

- Routing Configuration 23
- Public IP Address 24
- Public FQDN 24
- Redundancy/High Availability 25
- DNS Configuration 25
- Certificate Authority Server 27
- Prerequisite Configuration Tasks for this Integration 28
 - Configure the IM and Presence Service for Integration 28
 - Configure the Cisco Adaptive Security Appliance for Integration 28

CHAPTER 3

Configuration Workflows for Interdomain Federation 31

- Microsoft Lync Workflow (Intracompany via Expressway) 31
- Microsoft Lync Workflow (Business to Business via ASA) 32
- Microsoft OCS Workflow (Direct Federation) 33
- Microsoft OCS Workflow (Business to Business via ASA) 34
- Cisco Adaptive Security Appliance for SIP Federation Workflow 34
- XMPP Federation Workflow 35

CHAPTER 4

IM and Presence Service Configuration for SIP Federation 37

- Add a SIP Federated Domain 37
- Routing Configuration on IM and Presence Service 38
 - DNS Configuration for SIP Federation 38
 - Configure Static Routes Using TLS 39
- Configure Federation Routing Parameters 40
- Configuration of Security Settings on IM and Presence Service 41
 - Create a New TLS Peer Subject 41
 - Add TLS Peer to Selected TLS Peer Subjects List 42
- Turn On the SIP Federation Service 42

CHAPTER 5

SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance 45

- Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance 45
 - Generate Key Pair and Trustpoints on the Cisco Adaptive Security Appliance 45
 - Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance 46

| | |
|--|---|
| Import Self-Signed Certificate onto the IM and Presence Service | 47 |
| Generate a New Certificate on the IM and Presence Service | 47 |
| Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance | 48 |
| Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA | 49 |
| CA Trustpoints | 49 |
| Configure a Certificate on the Cisco Adaptive Security Appliance Using SCEP | 50 |
| Configure a Certificate on the Cisco Adaptive Security Appliance Using Manual Enrollment | 51 |
| Certificate Configuration for the External Access Edge Interface | 53 |
| Download CA Certification Chain | 53 |
| Install a CA Certification Chain | 53 |
| Request Certificate from CA Server | 54 |
| Download Certificate from CA Server | 55 |
| Upload a Certificate onto Access Edge | 55 |
| Create Custom Certificate for Access Edge Using Enterprise Certificate Authority | 56 |
| Create and Issue a Custom Certificate Template | 56 |
| Request Site Server Signing Certificate | 57 |
| Security Certificate Configuration on Lync Edge Server for TLS Federation | 58 |
| | |
| CHAPTER 6 | Cisco Adaptive Security Appliance Configuration for SIP Federation |
| | 59 |
| Cisco Adaptive Security Appliance Unified Communication Wizard | 59 |
| External and Internal Interface Configuration | 59 |
| Configure Static IP Routes | 60 |
| Port Address Translation (PAT) | 61 |
| Port Address Translation for This Integration | 61 |
| PAT for Private to Public Requests | 63 |
| Static PAT for New Requests | 64 |
| NAT Rules in ASDM | 64 |
| Sample Static PAT Commands | 65 |
| PAT Configuration for Routing the IM and Presence Service Node | 65 |
| PAT Configuration for Intercluster or Intracluster IM and Presence Service Nodes | 67 |
| Cisco Adaptive Security Appliance Upgrade Options for Existing Deployments | 68 |
| | |
| CHAPTER 7 | TLS Proxy Configuration on the Cisco Adaptive Security Appliance |
| | 71 |

| | |
|--|----|
| TLS Proxy | 71 |
| Access List Configuration Requirements | 72 |
| Configure TLS Proxy Instances | 73 |
| Associate Access List with TLS Proxy Instance Using Class Maps | 74 |
| Enable TLS Proxy | 75 |
| Configure Cisco Adaptive Security Appliance for an Intercluster Deployment | 76 |

CHAPTER 8**Interdomain Federation to Microsoft Lync 77**

| | |
|---|----|
| Interdomain Federation to Microsoft Lync within an Enterprise | 77 |
| Configuration Task Flow for Microsoft Lync Federation | 78 |
| Add a Microsoft Lync Domain Within Enterprise | 79 |
| Configure Static Routes from IM and Presence to Lync | 79 |
| Configure Expressway Gateway for Microsoft Lync Federation | 80 |
| Configure Static Route from Lync to Expressway Gateway | 80 |
| Configure a Static Route from Lync to IM and Presence | 82 |
| Configure Trusted Applications on Lync Server | 84 |
| Publish Topology | 86 |
| Set up Certificates on IM and Presence for Federation with Lync | 86 |

CHAPTER 9**Interdomain Federation to Microsoft OCS 89**

| | |
|---|----|
| Interdomain Federation to Microsoft OCS within an Enterprise | 89 |
| Configuration Task Flow for Microsoft OCS Federation | 89 |
| Add a Microsoft OCS Domain Within Enterprise | 91 |
| Configure Static Route on IM and Presence Service for Microsoft Servers | 92 |
| Configure Static Routes on OCS to Point to the IM and Presence Service | 93 |
| Verify Peer Authentication Listener | 94 |
| Adding a Host Authorization Entry for the IM and Presence Service Node on OCS | 94 |
| Configure Certificates on OCS for Interdomain Federation | 95 |
| Enable Port 5060/5061 on the OCS Server | 95 |
| Configure OCS to use FIPS | 96 |
| Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS | 97 |

CHAPTER 10**External Server Component Configuration for SIP Federation 99**

Microsoft Component Configuration for SIP Federation 99

CHAPTER 11

Load Balancer Configuration for Redundancy for SIP Federation 103

About the Load Balancer 103

IM and Presence Service Node Updates 103

Cisco Adaptive Security Appliance Updates 104

Static PAT Message Updates 105

Access List Updates 106

TLS Proxy Instance Updates 108

CA-Signed Security Certificate Updates 109

Security Certificate Configuration Between the Load Balancer and Cisco Adaptive Security Appliance 109

Security Certificate Configuration Between the Load Balancer and IM and Presence Service Node 109

Microsoft Component Updates 110

CHAPTER 12

IM and Presence Service Configuration for XMPP Federation 111

External XMPP Federation through Cisco Expressway 111

Configure General Settings for XMPP Federation 113

XMPP Federation Overview 113

Important Notes about Restarting Services for XMPP Federation 113

Turn On XMPP Federation on a Node 114

Configure Security Settings for XMPP Federation 114

DNS Configuration for XMPP Federation 115

DNS SRV Records for XMPP Federation 115

DNS SRV Records for Chat Feature for XMPP Federation 118

Configure DNS SRV Record for Chat Node for XMPP Federation 119

Policy Settings Configuration for XMPP Federation 121

Policy Exception Configuration 121

Configure Policy for XMPP Federation 122

Configure the Cisco Adaptive Security Appliance for XMPP Federation 122

Turn On XMPP Federation Service 124

CHAPTER 13

Security Certificate Configuration for XMPP Federation 125

Security Certificate Configuration for XMPP Federation 125

Local Domain Validation for XMPP Federation 125

Multi-Server Certificate Overview 126

Use a Self-Signed Certificate for XMPP Federation 126

Use of a CA Signed Certificate for XMPP Federation 127

 Generate a Certificate Signing Request for XMPP Federation 127

 Upload a CA-Signed Certificate for XMPP Federation 128

Import a Root CA Certificate for XMPP Federation 130

CHAPTER 14

Email Address for Federation Configuration 131

Email for Federation Enablement 131

Email Address for Federation Considerations 131

 Email Address for Federation Support of Multiple Domains 132

 Email Domain Configuration Overview 132

 Information to Provide to the Administrator of an External Domain 133

 Information to Provide IM and Presence Service Users 133

 Email Domain Management Interactions and Restrictions 133

Email Address for Federation Configuration and Email Domain Management 134

 Turn On Email for Federation 134

 View Email Domains 134

 Add or Update Email Domain 135

 Delete an Email Domain 136

CHAPTER 15

Serviceability Configuration for Federation 137

Use of Logging for Federation 137

 Location of Log Files for SIP Federation 137

 Location of Log File for XMPP Federation 137

 Turn On Logging for Federation 137

How to Restart the Cisco XCP Router 138

 Cisco XCP Router 138

 Restart Cisco XCP Router 138

CHAPTER 16

Federation Integration Verification 139

 Verify SIP Federation Configuration 139

Verify XMPP Federation Configuration 140

CHAPTER 17

Troubleshooting a SIP Federation Integration 143

Common Cisco Adaptive Security Appliance Problems and Recommended Actions 143

Certificate Configuration Problems 143

Certificate Failure Between the IM and Presence Service and Cisco Adaptive Security Appliance 143

Certificate Failure Between the Cisco Adaptive Security Appliance and Microsoft Access Edge 143

Certificate Error in SSL Handshake 143

Error When Submitting a Certificate Signing Request to VeriSign 144

SSL Errors when an IM and Presence Service Domain or Hostname is Changed 144

Errors When Creating TLS Proxy Class Maps 144

Subscriptions Do Not Reach Access Edge 145

Problems with Cisco Adaptive Security Appliance after Upgrade 145

Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008 146

Common Integration Problems and Recommended Actions 146

Unable to Get Availability Exchange 146

Problems Sending and Receiving IMs 147

Losing Availability and IM Exchange after a Short Period 148

Delay in Availability State Changes and IM Delivery Time 149

403 FORBIDDEN Returned Following an Availability Subscription Attempt 149

Time Out on NOTIFY Message 149

IM and Presence Service Certificate not Accepted 150

Problems Starting Front-End Server on OCS 151

Unable to Remote Desktop to Access Edge 151

CHAPTER 18

Troubleshooting an XMPP Federation Integration 153

Check System Troubleshooter 153

CHAPTER 19

Sample Cisco Adaptive Security Appliance Configuration 155

Sample PAT Commands and Access List Configuration for SIP Federation 155

Sample Access List Configuration for XMPP Federation 158

Sample NAT Configuration for XMPP Federation 159

CHAPTER 20**Security Certificate Exchange Between the Cisco Adaptive Security Appliance and Microsoft Access Edge Using VeriSign 161**

Security Certificate Configuration on Cisco Adaptive Security Appliance 161

Delete Old Certificates and Trustpoints 161

Generate New Trustpoint for VeriSign 162

Import Root Certificate 163

Generate Certificate Signing Request 164

Submit Certificate Signing Request to VeriSign 164

Delete Certificate Used for Certificate Signing Request 165

Import Intermediate Certificate 166

Create a Trustpoint for Root Certificate 167

Import a Root Certificate 167

Import Signed Certificate 168

Import VeriSign Certificates onto Microsoft Access Edge 169

CHAPTER 21**Integration Debugging Information 171**

Debugging Information for the Cisco Adaptive Security Appliance 171

Cisco Adaptive Security Appliance Debugging Commands 171

Capture Output on Internal and External Interfaces 173

TLS Proxy Debugging Commands 174

Access Edge and OCS Server Debugging 175

Initiate Debug Session on OCS/Access Edge 175

Verify DNS Configuration on Access Edge 175



CHAPTER 1

Overview of this Integration

- [Basic Federated Network, on page 1](#)
- [Intercluster and Multinode Deployments, on page 3](#)
- [High Availability and Federation, on page 4](#)
- [Cisco Adaptive Security Appliance Deployment Options, on page 6](#)
- [Presence Subscriptions and Blocking Levels, on page 8](#)
- [Availability State Mappings, on page 10](#)
- [Instant Messaging, on page 15](#)
- [Federation in Deployments with Multiple Domains, on page 18](#)
- [Federation and Subdomains, on page 18](#)

Basic Federated Network

This integration enables the IM and Presence Service users from within any domain that IM and Presence Service manages to exchange availability information and Instant Messaging (IM) with users in external domains. The IM and Presence Service uses different protocols to federate with different external domains.

The IM and Presence Service uses the standard Session Initiation Protocol (SIP RFC 3261) to federate with:

- Microsoft Lync 2010 and 2013, Standard Edition and Enterprise Edition
- Microsoft Office Communications Server Release 2 (OCS R2), OCS 2007



Note IM and Presence Service Release 9.0 or later supports interdomain federation with Microsoft Lync. For IM and Presence Service Release 9.0 or later, any reference to interdomain federation with OCS also includes Microsoft Lync, unless explicitly stated otherwise.

IM and Presence Service uses the Extensible Messaging and Presence Protocol (XMPP) to federate with:

- IBM Sametime Server 8.2 and 8.5
- Cisco WebEx Messenger
- IM and Presence Service 9.x and up
- Any other server that is XMPP Standards compliant

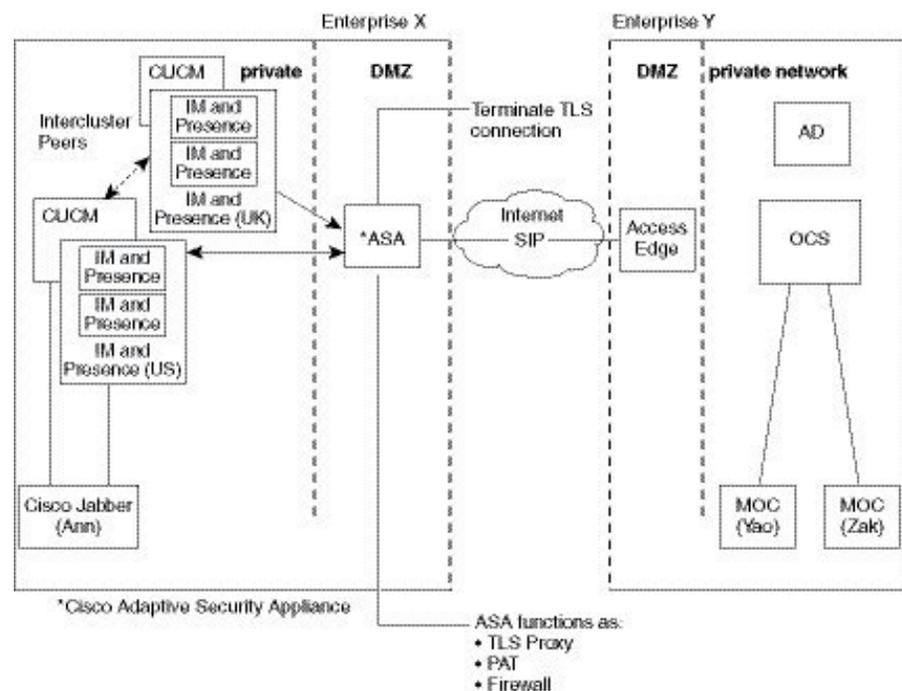


Note If you wish to enable XMPP federation with an external domain, ensure that the external domain was not previously configured as a SIP federated domain on the IM and Presence Service.

Example: An IM and Presence deployment with example.com was historically configured as a SIP based federation. But example.com has now added XMPP support, so the local administrator instead wishes to enable an XMPP based federation. To allow this, the local administrator must first delete example.com as a SIP federated domain on the IM and Presence Service.

The following figure provides an example of a SIP federated network between IM and Presence Service enterprise deployment and Microsoft OCS enterprise deployment.

Figure 1: Basic SIP Federated Network Between IM and Presence Service and Microsoft OCS

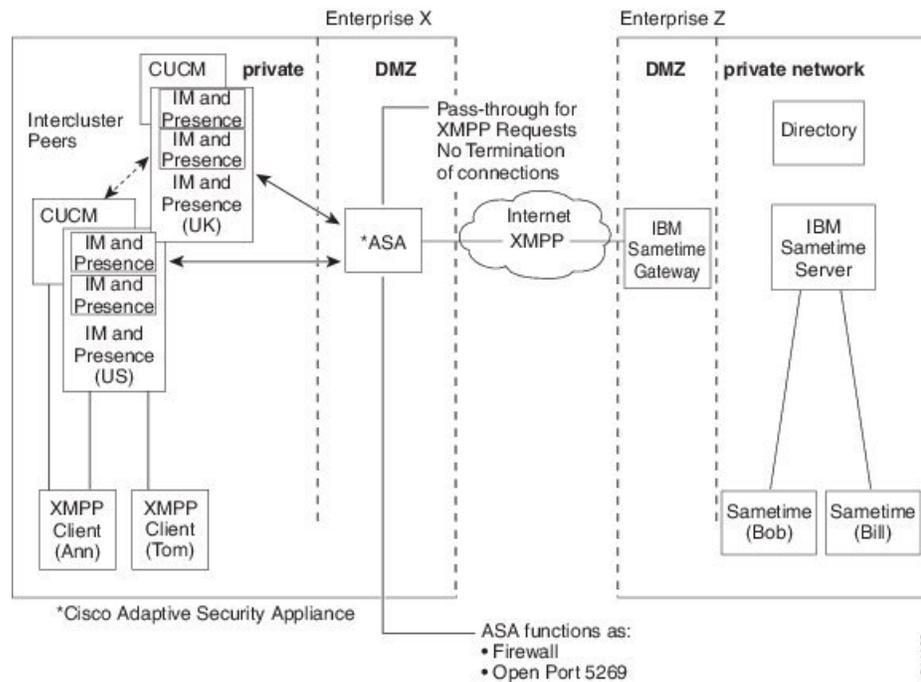


This example shows the messaging flows for a multi-cluster IM and Presence Service deployment where SIP Federation is enabled in one cluster only. A single routing node receives all incoming IMs from the ASA and reroutes the IM to the correct node in either cluster. Outgoing IMs can be sent to the ASA from any node in either cluster.

In the figure, each internal enterprise domain interconnects over the public internet using its DMZ edge server using a secure TLS connection. Within the internal IM and Presence Service enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT), and TLS proxy functionality. The Cisco Adaptive Security Appliance routes all incoming traffic initiated from the external domain to a designated IM and Presence Service node.

The following figure provides an example of a multi-cluster XMPP federated network between IM and Presence Service enterprise deployment and an IBM Sametime enterprise deployment. TLS is optional for XMPP federation. Cisco Adaptive Security Appliance acts only as a firewall for XMPP federation; it does not provide TLS proxy functionality or PAT for XMPP federation. IMs can be sent and received from any node that has Federation enabled. However, Federation must be configured in parallel in both clusters.

Figure 2: Basic XMPP Federated Network Between IM and Presence Service and IBM Sametime



There are two DNS servers within the internal IM and Presence Service enterprise deployment. One DNS server hosts the IM and Presence Service private address. The other DNS server hosts the IM and Presence Service public address and DNS SRV records for SIP federation (`_sipfederationtls`), and XMPP federation (`_xmpp-server`) with the IM and Presence Service. The DNS server that hosts the IM and Presence Service public address is located in the local DMZ.

Intercluster and Multinode Deployments



Note Any configuration procedures in this document that relate to intercluster IM and Presence Service deployments, you can also apply these procedures to multinode IM and Presence Service deployments.

SIP Federation Deployments

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external domain initiates a new session, Cisco Adaptive Security Appliance routes all 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 through intercluster communication to the appropriate IM and Presence Service node within the cluster. The system routes all responses that are associated with this request through the routing IM and Presence Service node.

Any IM and Presence Service node can initiate a message to an external domain through Cisco Adaptive Security Appliance. On OCS, when the external domain replies to these messages, the replies are sent directly back to the IM and Presence Service node that initiated the message through the Cisco Adaptive Security

Appliance. You enable this behavior when you configure Port Address Translation (PAT) on the Cisco Adaptive Security Appliance. We recommend that you configure PAT on the Cisco Adaptive Security Appliance as PAT is required for the 200 OK response messages.

Related Topics

[Port Address Translation \(PAT\)](#), on page 61

XMPP Federation Deployments

For a single cluster, you only need to enable XMPP federation on one node in the cluster. A single DNS SRV record is published for the enterprise in the public DNS. This DNS SRV record maps to the IM and Presence Service node that is enabled for XMPP Federation. All incoming requests from external domains are routed to the node running XMPP federation, based on the published SRV record. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service also routes all outgoing requests through the node running XMPP federation.

You can also publish multiple DNS SRV records, for example, for scale purposes, or if you have multiple IM and Presence Service clusters and you must enable XMPP federation at least once per cluster. Unlike SIP federation, XMPP federation does not require a single point of entry for the IM and Presence Service enterprise domain. As a result, the IM and Presence Service can route incoming requests to any one of the published nodes that you enable for XMPP federation.

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external XMPP federated domain initiates a new session, it performs a DNS SRV lookup to determine where to route the request. If you publish multiple DNS SRV records, the DNS lookup returns multiple results; IM and Presence Service can route the request to any of the servers that DNS publishes. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation within the cluster.

If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, the IM and Presence Service routes all incoming requests through that single node, rather than load balancing the incoming requests across the nodes running XMPP federation. The IM and Presence Service load-balances outgoing requests and sends outgoing requests to any of the nodes running XMPP federation within the cluster.

High Availability and Federation

High Availability for SIP Federation



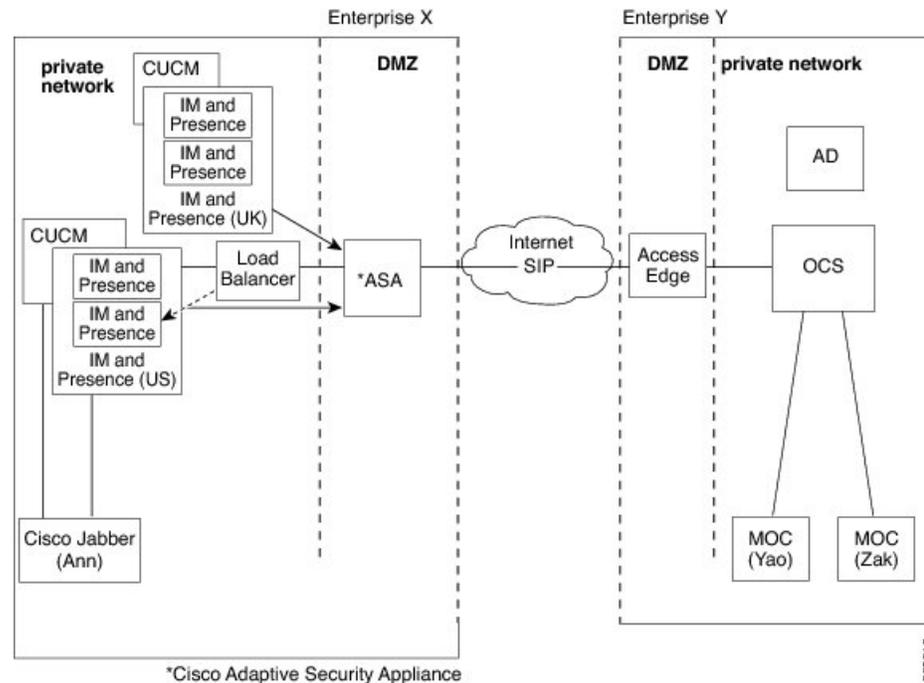
Note Only the IM and Presence Service, Release 8.5 or later supports high availability.

If you are federating with a Microsoft OCS enterprise, the Microsoft Access Edge server only supports the return of a single hostname and server address in the DNS SRV lookup. Also the Microsoft Access Edge server only supports the manual provisioning of a single IP address.

Therefore, in order to achieve high availability when federating with Microsoft OCS, you must incorporate a load balancer between the IM and Presence Service node and Cisco Adaptive Security Appliance, as shown in the following figure. The load balancer terminates incoming TLS connections from Cisco Adaptive Security

Appliance, and initiates a new TLS connection to route the content to the appropriate backend IM and Presence Service.

Figure 3: Federated Network Between the IM and Presence Service and Microsoft OCS with High Availability



Related Topics

[Load Balancer Configuration for Redundancy for SIP Federation](#), on page 103

High Availability for XMPP Federation

High availability for XMPP federation differs from the high availability model for other IM and Presence Service features because it is not tied to the two node sub-cluster model.

To provide high availability for XMPP federation, you must enable two or more IM and Presence Service nodes in your cluster for XMPP federation; having multiple nodes enabled for XMPP federation not only adds scale but it also provides redundancy in the event that any node fails.

High Availability for Outbound Request Routing

The IM and Presence Service evenly load balances outbound requests from users within that cluster across all the XMPP federation enabled nodes in the cluster. If any node fails, the IM and Presence Service dynamically spreads the outbound traffic across the remaining active nodes within the cluster.

High Availability for Inbound Request Routing

An additional step is required to provide high availability for inbound request routing. To allow an external domain to discover the local IM and Presence Service deployment, a DNS SRV record must be published on a public DNS server. This record resolves to an XMPP federation enabled node. The external domain then connects to the resolved address.

To provide high availability in this model, multiple DNS SRV records must be published for the local IM and Presence Service deployment. Each of these records resolve to one of the XMPP Federation enabled nodes within the local IM and Presence Service deployment.

These records provide a choice of DNS SRV records for the local deployment. If an XMPP federation enabled node fails, the external system has other options from which to connect to the local IM and Presence Service deployment.

**Note**

- Each published DNS SRV records must have the same priority and weight. This allows a spread of load across all published records, and also allows the external system to correctly reconnect to one of the other nodes with a DNS SRV record in the event of a failure.
- DNS SRV records may be published for all or just a subset of XMPP federation enabled nodes. The greater the number of records published, the greater the redundancy in the system for inbound request handling.
- If you configure the Chat feature on an IM and Presence Service node in an XMPP federation deployment, you can publish multiple DNS SRV records for chat node aliases also. This allows the external system to find another inbound route to that specific chat node through another XMPP federation node, should any XMPP Federation enabled node fail. Note that this is not high availability for the Chat feature itself, but an extension of the XMPP Federation high availability feature for inbound requests addressed to chat node aliases.

IBM Sametime Federation

IM and Presence Service Release 9.0 does not support high availability for Interdomain federation between an IM and Presence Service enterprise and an IBM Sametime enterprise and an IBM Sametime enterprise. This is because IBM Sametime does not retry other records that are returned in a DNS SRV lookup. It only tries the first DNS SRV record found, and if the connection attempt fails, it does not retry to lower weighted nodes.

**Note**

There is one situation where XMPP Federation high availability may appear to occur on the IM and Presence Service in an IBM Sametime federation deployment. If users have failed over to the backup node due to critical services failing, but the Cisco XCP XMPP Federation Connection Manager remains running on the primary node. In this case, incoming traffic is still directed to the primary node, and then redirected to the backup node using the router to router connection. However, in this scenario XMPP Federation has not failed and can continue to operate as normal.

Related Topics

[DNS Configuration for XMPP Federation](#), on page 115

[Turn On XMPP Federation on a Node](#), on page 114

Cisco Adaptive Security Appliance Deployment Options

Within the internal IM and Presence Service enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT) and TLS proxy functionality in the DMZ to terminate the incoming connections from the public internet, and permit traffic from specific federated domains.

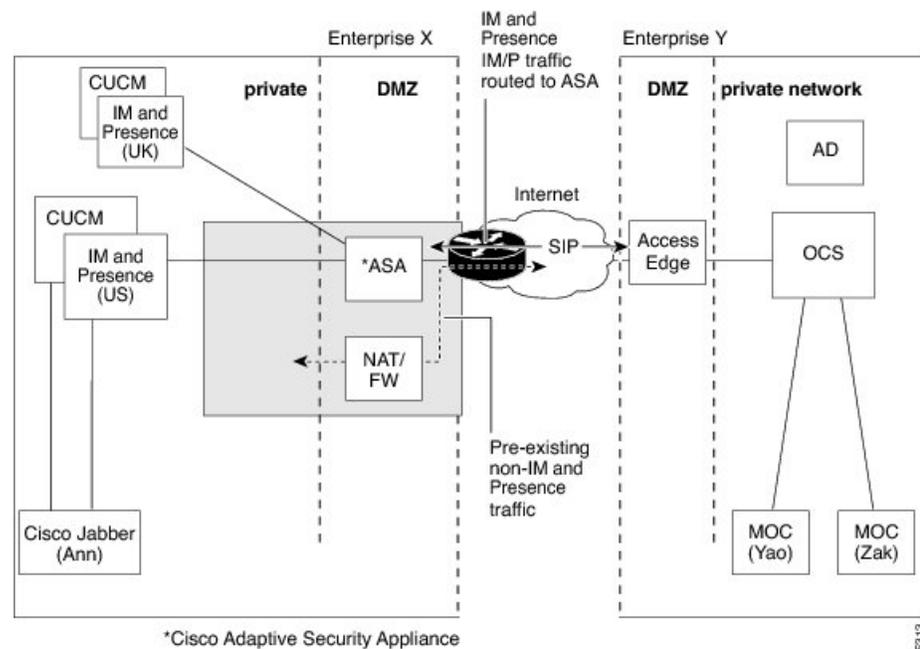


Note In an XMPP federation deployment, Cisco Adaptive Security Appliance provides firewall functionality only. If you already deploy a firewall, you do not require an extra Cisco Adaptive Security Appliance for XMPP federation.

You can deploy the Cisco Adaptive Security Appliance in a number of different ways, depending on your existing network and the type of firewall functionality you want to deploy. This section contains only an overview of the deployment models we recommend. For further details please refer to the deployment guidelines in the Cisco Adaptive Security Appliance documentation. The Cisco Adaptive Security Appliance deployment options we describe here apply to SIP federation only.

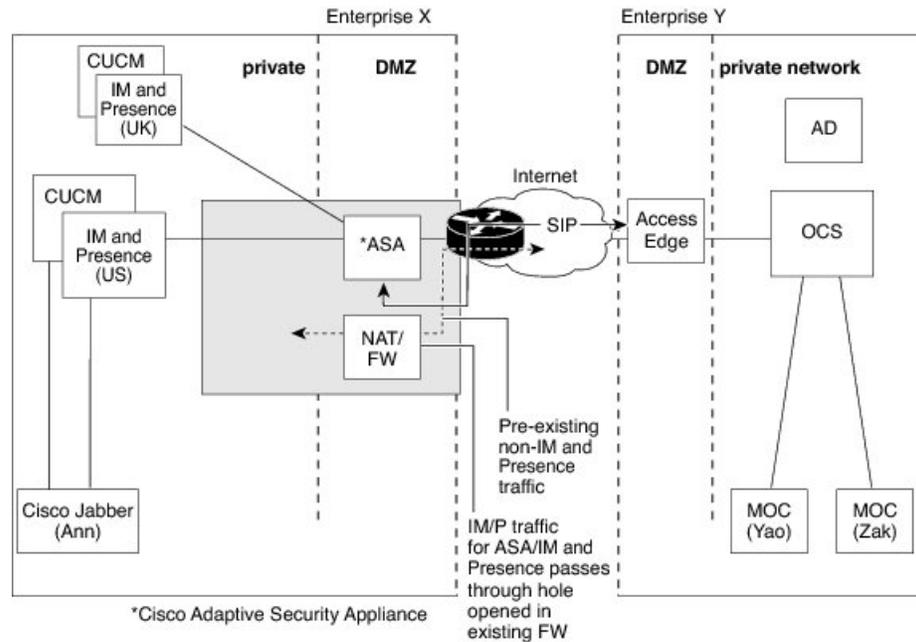
You can deploy the Cisco Adaptive Security Appliance as the enterprise firewall that protects Instant Messaging (IM) traffic, Availability traffic, and other traffic as illustrated in the following figures. This is the most cost-effective deployment, and the one we recommend for new and existing networks. You can also deploy the Cisco Adaptive Security Appliance in parallel to the existing firewall, as illustrated in the following figure. In this deployment Cisco Adaptive Security Appliance handles the IM and Presence Service traffic between IM and Presence Service and the public internet, and the pre-existing traffic continues to use any existing firewall. In the following figure Cisco Adaptive Security Appliance is also deployed as a gateway for the IM and Presence Service node, which means that you do not require a separate router to direct traffic to Cisco Adaptive Security Appliance.

Figure 4: Cisco ASA 5500 Deployed in Parallel to Existing NAT/Firewall



You can also deploy the Cisco Adaptive Security Appliance behind an existing firewall. In this case, you configure the existing firewall to allow traffic destined for the IM and Presence Service to reach the Cisco Adaptive Security Appliance, as illustrated in the following figure. In this type of deployment the Cisco Adaptive Security Appliance is functioning as a gateway for the IM and Presence Service node.

Figure 5: Cisco ASA 5500 Deployed Behind Existing NAT/Firewall



Presence Subscriptions and Blocking Levels

All new presence subscriptions from `x@externaldomain.com` to `user@local.com` are sent by the Cisco Adaptive Security Appliance, as shown in the following figure. The Cisco Adaptive Security Appliance checks the inbound SIP subscriptions against the list of permitted external domains. If the domain is not permitted, the Cisco Adaptive Security Appliance denies the presence subscription.



Note In an XMPP federation deployment, the Cisco Adaptive Security Appliance does not perform any domain checks.

On receipt of the inbound subscription, the IM and Presence Service verifies that the external domain is one of the permitted federated domains that you define at the administration level on the IM and Presence Service node. For SIP federation, you configure a federated domain. For XMPP federation, you define the administrator policy for XMPP federation. If the subscription is not from a permitted domain, the IM and Presence Service denies the subscription (without contacting the local user).

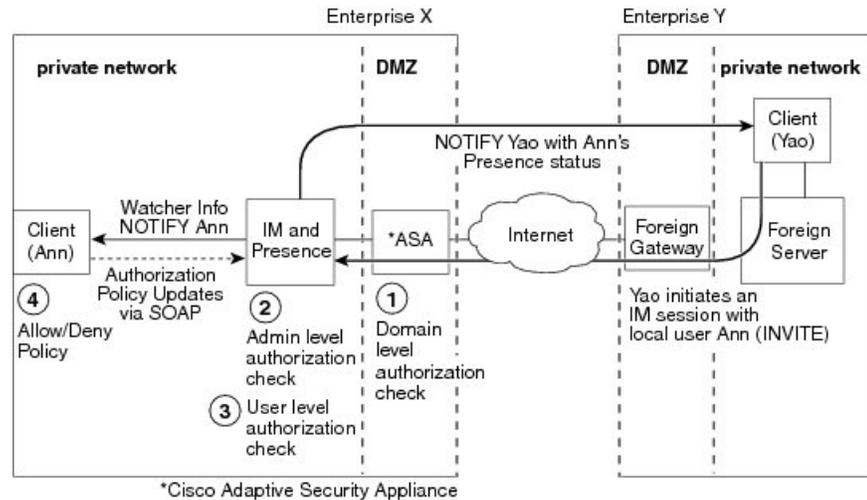
If the subscription is from a permitted domain, the IM and Presence Service checks the authorization policies of the local user to verify that the local user has not previously blocked or allowed either the federated domain or the user sending the presence subscription. The IM and Presence Service then accepts the incoming subscription and places it in a pending state.

The IM and Presence Service notifies the local user that `x@externaldomain.com` wants to watch their presence by sending the client application a notification message for the subscription. This triggers a dialog box on the client application that enables the local user to allow or deny the subscription. Once the user has made an authorization decision, the client application communicates that decision back to the IM and Presence Service. The authorization decision is added to the policy list of the user stored on the IM and Presence Service.

A deny decision is handled using polite blocking, which means that the presence state of the user appears offline on the external client. If the local user allows the subscription, the IM and Presence Service sends presence updates to the external watcher.

The user can also block subscriptions on a per user and a per domain basis. This can be configured by the Cisco Jabber client.

Figure 6: Inbound SIP Presence Message Flow



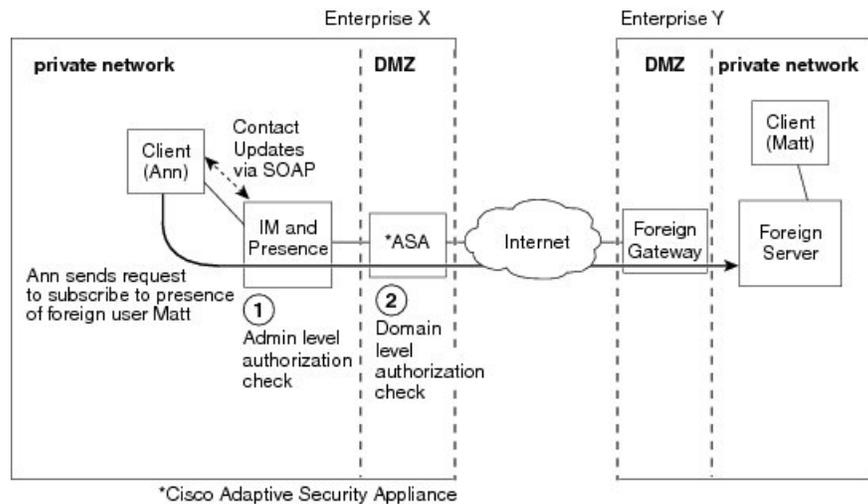
The IM and Presence Service sends all outgoing subscriptions through the Cisco Adaptive Security Appliance, the Cisco Adaptive Security Appliance then forwards these subscriptions to the external domain. The IM and Presence Service sends an outgoing subscription even if an active subscription already exists between a different local user to the same external user in the same external domain. The following figure illustrates an outgoing presence subscription flow.

The external user is added to the contact list on the client application and the **IM and Presence Service User Options** interface as `user@externaldomain.com`.



Note The domain level authentication check is not applied on the Cisco Adaptive Security Appliance for XMPP federation.

Figure 7: Outbound Presence Request Flow

**Note**

- Microsoft OCS performs a refresh subscribe every one hour and 45 minutes. Therefore, if an IM and Presence Service node restarts, the maximum duration a Microsoft Office Communicator client is without the presence status of the IM and Presence Service contacts is approximately two hours.
- If Microsoft OCS restarts, the maximum duration an IM and Presence Service client is without presence status of Microsoft Office Communicator contacts is approximately two hours.

Related Topics

[Availability State Mappings](#), on page 10

[Instant Messaging](#), on page 15

Availability State Mappings

Availability State Mappings for Microsoft OCS

The following table shows the availability mapping states from Microsoft Office Communicator to the IM and Presence Service, third-party XMPP clients and Cisco Jabber.

Table 1: Availability Mapping States from Microsoft Office Communicator

| Microsoft Office Communicator Setting | Third-party XMPP Client Setting (connected to IM and Presence Service) | Cisco Jabber Release 8.x Setting |
|---------------------------------------|--|----------------------------------|
| Available | Available | Available |
| Busy | Away | Busy |
| Do Not Disturb | Away | Busy |

| Microsoft Office Communicator Setting | Third-party XMPP Client Setting (connected to IM and Presence Service) | Cisco Jabber Release 8.x Setting |
|---------------------------------------|--|----------------------------------|
| Be Right Back | Away | Away |
| Away | Away | Away |
| Offline | Offline | Offline |

In the table, Microsoft Office Communicator "Busy" and "Do Not Disturb" states map to "Away" with a status text of "Busy" on a third-party XMPP client. XMPP clients differ in how they render this "Away" status, for example, certain XMPP clients show the "Away" icon with no text. Other XMPP clients render the "Away" icon with "Busy" text annotation alongside.

The following table shows the availability mapping states from Cisco Jabber Release 8.x to Microsoft Office Communicator.

Table 2: Availability Mapping States from Cisco Jabber Release 8.x

| Cisco Jabber Release 8.x Setting | Microsoft Office Communicator Setting |
|----------------------------------|---------------------------------------|
| Available | Available |
| Busy | Busy |
| Do Not Disturb | Busy |
| Offline | Offline |

The following table shows the availability mapping states from third-party XMPP clients that are connected to IM and Presence Service to Microsoft Office Communicator.

Table 3: Availability Mapping States from Third-party XMPP Client

| Third-party XMPP Client Setting (connected to IM and Presence Service) | Microsoft Office Communicator Setting |
|--|---------------------------------------|
| Available | Available |
| Away | Away |
| Extended Away | Away |
| Do Not Disturb | Busy |
| Offline | Offline |

Related Topics

[Presence Subscriptions and Blocking Levels](#), on page 8

Availability State Mappings for Microsoft Lync

The following table shows the availability mapping states from Microsoft Lync to the IM and Presence Service, third-party XMPP clients and Cisco Jabber.

Table 4: Availability Mapping States from Microsoft Lync

| Microsoft Lync Setting | Third-party XMPP Client Setting (connected to IM and Presence Service) | Cisco Jabber Release 8.x Setting |
|-------------------------------|---|---|
| Available | Available | Available |
| Busy | Away | Busy |
| Do Not Disturb | Away | Busy |
| Be Right Back | Away | Away |
| Away | Away | Away |
| Offline | Offline | Offline |

In the table, Lync Client "Busy" and "Do Not Disturb" states map to "Away" with a status text of "Busy" on a third-party XMPP client. XMPP clients differ in how they render this "Away" status, for example, certain XMPP clients show the "Away" icon with no text. Other XMPP clients render the "Away" icon with "Busy" text annotation alongside.

The following table shows the availability mapping states from Cisco Jabber Release 8.x to a Lync client.

Table 5: Availability Mapping States from Cisco Jabber Release 8.x

| Cisco Jabber Release 8.x Setting | Microsoft Lync Setting |
|---|-------------------------------|
| Available | Available |
| Busy | Busy |
| Do Not Disturb | Busy |
| Offline | Offline |

The following table shows the availability mapping states from third-party XMPP clients, that are connected to the IM and Presence Service, to a Lync client.

Table 6: Availability Mapping States from a Third-party XMPP Client

| Third-party XMPP Client Setting (connected to IM and Presence Service) | Microsoft Lync Setting |
|---|-------------------------------|
| Available | Available |
| Away | Away |

| Third-party XMPP Client Setting (connected to IM and Presence Service) | Microsoft Lync Setting |
|---|-------------------------------|
| Extended Away | Away |
| Do Not Disturb | Busy |
| Offline | Offline |

Related Topics

[Presence Subscriptions and Blocking Levels](#), on page 8

Availability State Mappings for XMPP Federation

The following table shows the availability mapping states from IBM Sametime 8.2 to a third-party XMPP client on the IM and Presence Service, and to Cisco Jabber.

Table 7: Availability Mapping States from IBM Sametime 8.2 Client

| IBM Sametime Client Setting | Third-party XMPP Client Setting (connected to IM and Presence Service) | Cisco Jabber Setting Release 8.x |
|--------------------------------------|---|---|
| Available | Available | Available with status message |
| Do Not Disturb | Do Not Disturb | Do Not Disturb with status message |
| Available with status “In a meeting” | Available with status “In a meeting” | Available with status message |
| Away | Away | Away with status message |
| Offline | Offline | Offline |

The following table shows the availability mapping states from webex Connect to a third-party XMPP client on the IM and Presence Service, and to Cisco Jabber.

Table 8: Availability Mapping States from Webex Connect

| Webex Connect Setting | Third-party XMPP Client Setting (connected to IM and Presence Service) | Cisco Jabber Setting Release 8.x |
|---------------------------------|---|---|
| Available | Available | Available |
| Do Not Disturb | Do Not Disturb | Do Not Disturb |
| Away with status “In a meeting” | Available with status “In a meeting” | Away with status “In a meeting” |
| Away | Away | Away |
| Offline | Offline | Offline |

The following table shows the availability mapping states from Cisco Jabber Release 8.x to other federated clients.

Table 9: Availability Mapping States from Cisco Jabber Release 8.x

| Cisco Jabber Release 8.x Setting | Federated Cisco Jabber Release 8.x Setting | Federated Third-party XMPP Client Setting (connected to IM and Presence Service) | Webex Connect Client Setting | IBM Sametime Client Server |
|---|---|---|-------------------------------------|-----------------------------------|
| Available | Available | Available | Available | Available |
| Do Not Disturb | Do Not Disturb | Do Not Disturb | Do Not Disturb | Do Not Disturb |
| Busy | Busy | Away | Idle | Away |
| Idle | Idle | Idle | Idle | Idle |
| Offline | Offline | Offline | Offline | Offline |

The following table shows the availability mapping states from a third-party XMPP client on the IM and Presence Service to other federated clients.

Table 10: Availability Mapping States from XMPP Client Connected to the IM and Presence Service

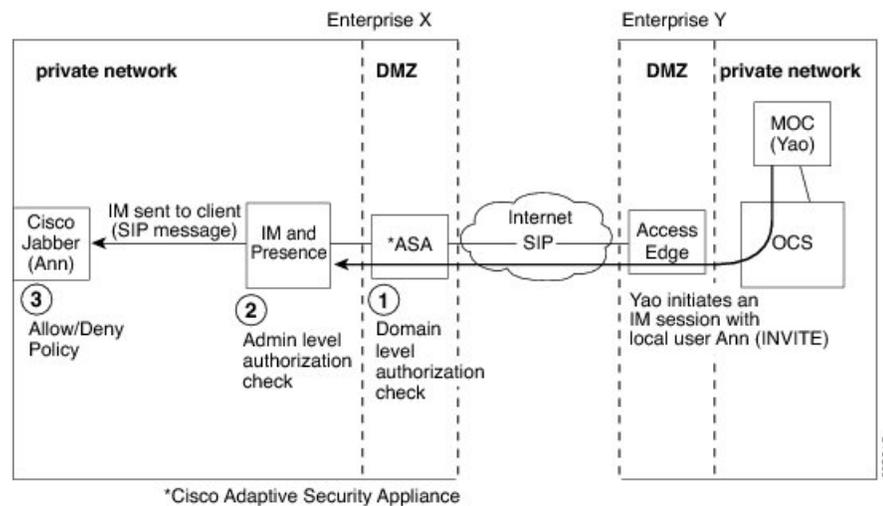
| Third-party XMPP Client Setting (connected to IM and Presence Service) | Federated Cisco Jabber Release 8.x Setting | Federated XMPP Client Setting (connected to IM and Presence Service) | Webex Connect Client Setting | IBM Sametime Client Server |
|---|---|---|-------------------------------------|-----------------------------------|
| Available | Available | Available | Available | Available |
| Do Not Disturb | Do Not Disturb | Do Not Disturb | Do Not Disturb | Do Not Disturb |
| Away | Away | Away | Away | Away |
| Extended Away | Away | Extended Away | Extended Away | Away |
| Away with status "Idle" | Idle | Away with status "Idle" | Away with status "Idle" | Away with status "Idle" |
| Offline | Offline | Offline | Offline | Offline |

Instant Messaging

Instant Message Flow for SIP Federation

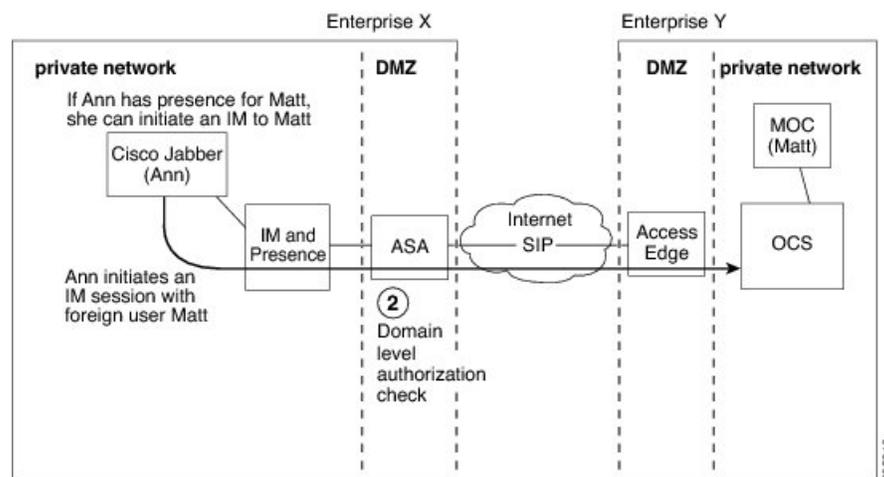
Instant Messages (IMs) that are sent between two enterprise deployments use Session Mode. When a user in an external domain sends an IM to a local user in the IM and Presence Service domain, the external server sends an INVITE message, as illustrated in the following figure. The Cisco Adaptive Security Appliance forwards the INVITE message to IM and Presence Service. The IM and Presence Service replies with a 200 OK message to the external server, and the external server sends a SIP MESSAGE containing the text data. The IM and Presence Service forwards the text data to the client application of the local user, using the appropriate protocol.

Figure 8: Inbound Instant Messaging Flow



When a local user in the IM and Presence Service domain sends an IM to a user in an external domain, the IM is sent to the IM and Presence Service node. If no existing IM session is established between these two users, the IM and Presence Service sends an INVITE message to the external domain to establish a new session. The following figure illustrates this flow. The IM and Presence Service uses this session for any subsequent MESSAGE traffic from either of these two users. Note that users of Cisco Jabber and third-party XMPP clients can initiate an IM even if they do not have availability.

Figure 9: Outbound Instant Message Flow



Note The IM and Presence Service does not support a three-way IM session (group chat) with a Microsoft OCS contact.

Availability and Instant Message Flow for XMPP Federation

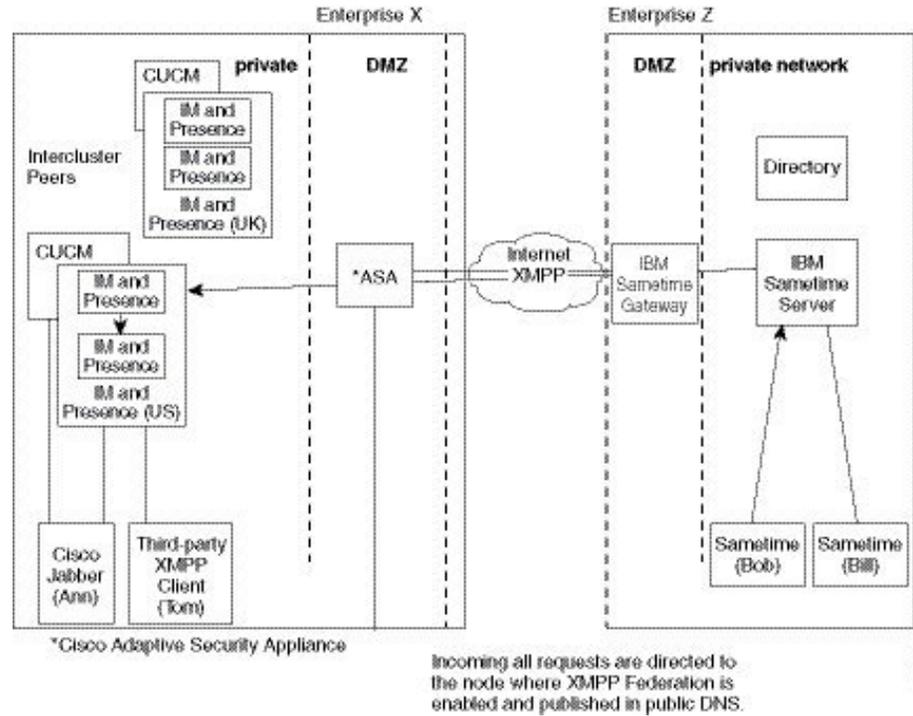
The flow of incoming and outgoing availability and IM requests for XMPP federation can vary in a multinode IM and Presence Service deployment.

In a multinode deployment, you can enable XMPP federation on each node in the cluster, or just on a single node in a cluster. In addition, you can decide to publish only a single DNS SRV record, or publish multiple DNS SRV records (one record for each node on which you enable XMPP Federation).

If you only publish a single DNS SRV record, the system routes all inbound requests to that single node, and internally the IM and Presence Service routes the traffic to the correct node using intercluster routing, as illustrated in the following figure. If you publish multiple DNS SRV records, depending on how you configure the SRV records, the system could load-balance inbound requests across each node.

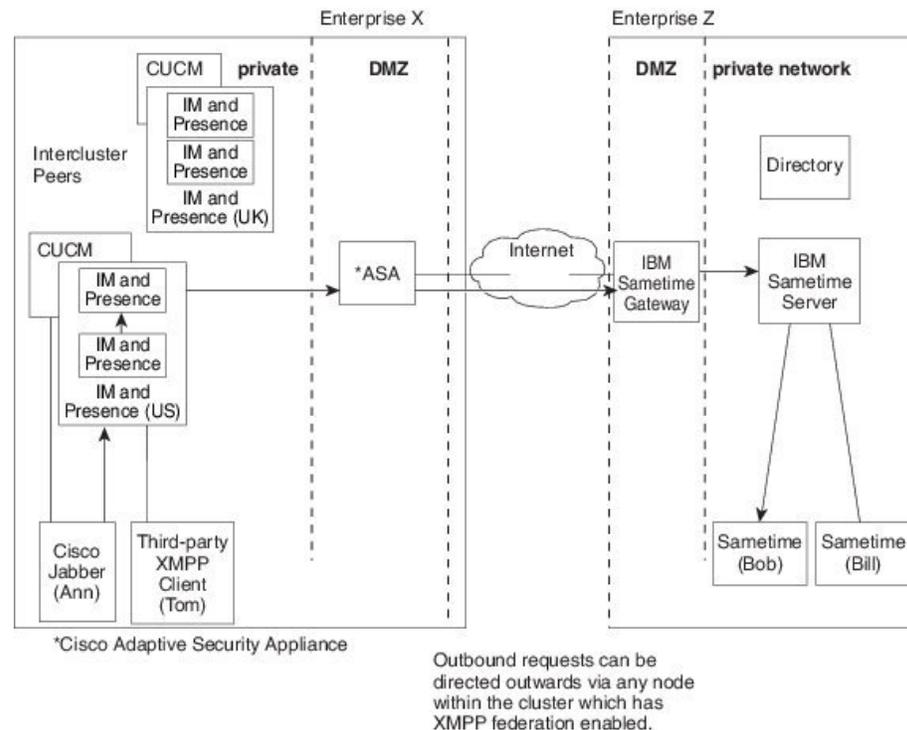
In this diagram, which shows the inbound message flow for a multi-cluster XMPP Federated network, Federation is enabled in both clusters. The inbound message goes directly to a Federation-enabled node in the destination cluster. The Federation-enabled node reroutes the message to the appropriate cluster node.

Figure 10: XMPP Inbound Request Flow



The IM and Presence Service routes outbound requests to any node in the cluster on which you enable XMPP Federation, even if that node is not the home node for the user that initiates the request, as illustrated in the following figure. In this diagram, Federation is enabled in both peer clusters, but the outbound flow does not hit the peer cluster.

Figure 11: XMPP Outbound Request Flow



Federation in Deployments with Multiple Domains

Federation is fully supported in IM and Presence Service deployments with multiple domains provided the remote domain is not managed by the local IM and Presence Service deployment.

You must create DNS records for all local domains to enable Federation for all users in the local cluster.

For XMPP federation, the cup-xmpp security certificate must have all local domains included as Subject Alt Names.

Federation and Subdomains

The IM and Presence Service supports the following subdomain scenarios:

- The IM and Presence Service belongs to a subdomain of the external domain. For example, the IM and Presence Service belongs to the subdomain "imp.cisco.com". The IM and Presence Service federates with an external enterprise that belongs to the domain "cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@imp.cisco.com", and the external user has the URI "foreignuser@cisco.com".
- The IM and Presence Service belongs to a parent domain, and the external enterprise belongs to a subdomain of that parent domain. For example, the IM and Presence Service belongs to the domain "cisco.com". The IM and Presence Service federates with an external enterprise that belongs to the

subdomain "foreign.cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@cisco.com", and the external user is assigned the URI "foreignuser@foreign.cisco.com".

- The IM and Presence Service and the external enterprise each belong to different subdomains, but both of these subdomains belong to the same parent domain. For example, the IM and Presence Service belongs to the subdomain "cup.cisco.com" and the external enterprise belongs to the subdomain "foreign.cisco.com". Both of these subdomains belong to the parent domain "cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@cup.cisco.com" and the external user is assigned the URI "foreignuser@foreign.cisco.com".

If you federate with subdomains, you only need to configure separate DNS domains; there is no requirement to split your Active Directory. If you configure federation within the enterprise, the IM and Presence Service users or external users can belong to the same Active Directory domain. For example, in the third scenario above, the Active Directory can belong to the parent domain "cisco.com". You can configure all users under the "cisco.com" domain in Active Directory, even though a user may belong to the subdomain "imp.cisco.com" or "foreign.cisco.com", and may have the URI "impuser@imp.cisco.com" or "foreignuser@foreign.cisco.com".

Note that even though an LDAP search from Cisco Jabber may return users in the other domain, or subdomain, a Cisco Jabber user cannot add these federated users from the LDAP lookup on Cisco Jabber. The Cisco Jabber user must add these users as external (federated) contacts so that the IM and Presence Service applies the correct domain and not the local domain.



Note The IM and Presence Service also supports the scenarios above if you configure federation between two IM and Presence Service enterprise deployments.



CHAPTER 2

Preparations for this Integration

- [Supported Interdomain Federation Integrations](#), on page 21
- [Hardware Requirements](#), on page 22
- [Software Requirements](#), on page 22
- [Integration Preparation](#), on page 23
- [Prerequisite Configuration Tasks for this Integration](#), on page 28

Supported Interdomain Federation Integrations

This document describes the configuration steps for setting up a federated network between the IM and Presence Service node and an external domain.

The supported external domains that an IM and Presence Service node can federate with are:

- Microsoft Office Communications Server Releases 2007, R2, Microsoft Lync 2010 and 2013 over SIP



Note The IM and Presence Service, supports interdomain federation with Microsoft Lync. Any reference to interdomain federation with OCS also includes Microsoft Lync, unless explicitly stated otherwise.

- Cisco WebEx Messenger over XMPP
- IBM Sametime Server Release 8.2, 8.5 over XMPP
- IM and Presence Service Release 9.x and later over XMPP



Note If you federate between one IM and Presence Service enterprise and another, follow the procedures that describe how to configure XMPP Federation.

Related Topics

- [Hardware Requirements](#), on page 22
- [Software Requirements](#), on page 22

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 restrictions about Presence Web Service API support:

- For interdomain federation over SIP, you can use the Presence Web Service API to obtain rich presence information from non-Cisco clients, but basic presence for non-Cisco clients is not supported.
- For interdomain federation over XMPP, 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>.

Hardware Requirements

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 Cisco Unified Communications Manager compatibility matrix
- Two DNS servers within the IM and Presence Service enterprise
- Cisco Adaptive Security Appliance 5500 Series
- We only recommend the Cisco Adaptive Security Appliance for SIP federation as it provides the TLS proxy functionality. For XMPP federation, any firewall is sufficient.
- When selecting a Cisco Adaptive Security Appliance model, go to: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html. The TLS proxy component is available on all 5500 models.
- Make sure you use the correct version of Cisco Adaptive Security Appliance software for your deployment. If you are configuring a new interdomain federation deployment, refer to the IM and Presence Service compatibility matrix for the correct version of Cisco Adaptive Security Appliance software.

Related Topics

[Software Requirements](#), on page 22

Software Requirements

Cisco Software

- IM and Presence Service
- Cisco Unified Communications Manager

- Cisco Adaptive Security Appliance v8.3(1) or later
- Cisco Adaptive Security Device Manager (ASDM) v6.3 or later
- Supported XMPP clients:
 - 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

Microsoft Software for SIP Federation

- Microsoft Lync 2013 or 2010, Standard Edition or Enterprise Edition
- Microsoft OCS 2007 Release 2 Server Standard or Enterprise
- Microsoft Office Communicator 2007 Release 2

Software for XMPP Federation

- Cisco WebEx Messenger
- IBM Sametime Server Release 8.2

Related Topic

[Hardware Requirements, on page 22](#)

Integration Preparation

It is essential that you plan carefully for this integration. Read the items in this section before you commence any configuration for this integration.

Routing Configuration

Consider how you are going to set up routing in your federated network. Consider how you route messages that are destined for an external domain address from IM and Presence Service through the Cisco Adaptive Security Appliance to the external domain. You could consider deploying a routing entity (router, switch or gateway) between the IM and Presence Service enterprise deployment and Cisco Adaptive Security Appliance. The routing entity routes messages to the Cisco Adaptive Security Appliance, and Cisco Adaptive Security Appliance routes these messages to the external domain.

You can also deploy Cisco Adaptive Security Appliance as a gateway between the IM and Presence Service and the external domain. If you use the Cisco Adaptive Security Appliance as a gateway for the IM and Presence Service, within your local enterprise deployment, you must consider how the Cisco Unified

Communications Manager, and the IM and Presence Service client access the IM and Presence Service node. If the Cisco Unified Communications Manager and the IM and Presence Service clients are in a different subnet from the IM and Presence Service, they must access the IM and Presence Service using the Cisco Adaptive Security Appliance.

If you deploy the Cisco Adaptive Security Appliance behind an existing firewall in your network, consider how you route traffic to the Cisco Adaptive Security Appliance and to the IM and Presence Service. On the existing firewall, configure routes and access lists to route traffic to the public IM and Presence Service address. You must also configure routes to the external domain using the existing firewall.

Related Topics

[Cisco Adaptive Security Appliance Deployment Options](#), on page 6

[Cisco Adaptive Security Appliance Configuration for SIP Federation](#), on page 59

Public IP Address

For SIP federation, you require a publicly accessible IP address for the public IM and Presence Service address. If you do not have an IP address that you can assign, use the outside interface of the Cisco Adaptive Security Appliance as the public IM and Presence Service address (once you only use the Cisco Adaptive Security Appliance for availability and IM traffic).

For SIP federation with Microsoft OCS R2, you require a single public IP address, even if you deploy multiple IM and Presence Service nodes. Cisco Adaptive Security Appliance routes the requests from OCS to the correct IM and Presence Service node using Port Address Translation (PAT).

For XMPP federation, you can choose to either expose a public IP address for each IM and Presence Service node on which you enable XMPP federation, or expose a single public IP address:

- If you expose multiple IP addresses, you use NAT on Cisco Adaptive Security Appliance to convert the public addresses to private addresses. For example, you can use NAT to convert the public addresses `x.x.x.x:5269` and `y.y.y.y:5269` to the private addresses `a.a.a.a:5269` and `b.b.b.b:5269` respectively.
- If you expose a single IP address, you use PAT on Cisco Adaptive Security Appliance to map to the correct IM and Presence Service node. For example, the public IP address in your deployment is `x.x.x.x`, and there are multiple DNS SRV records for `_xmpp-server`. Each record has a different port, but all records resolve to `x.x.x.x`. The external servers sends requests to `x.x.x.x:5269`, `x.x.x.x:15269`, `x.x.x.x:25269` through the Cisco Adaptive Security Appliance. The Cisco Adaptive Security Appliance performs PAT on the IP addresses, whereby it maps each address to the corresponding internal IP address for each IM and Presence Service node.

For example, the public IP address `x.x.x.x:5269` maps to the private IP address `a.a.a.a:5269`, the public IP address `x.x.x.x:15269` maps to the private IP address `b.b.b.b:5269`, and the public IP address `x.x.x.x:25269` maps to the private IP address `c.c.c.c:5269`, and so on. All IP addresses map internally to the same port (5269) on the IM and Presence Service.

Related Topics

[External and Internal Interface Configuration](#), on page 59

[DNS Configuration](#), on page 25

Public FQDN

For SIP federation, request messages are routed based on the FQDN. Therefore, the FQDN of the routing IM and Presence Service node (publisher) must be publicly resolvable.

Redundancy/High Availability

You need to consider how you are going to configure redundancy in your federated network. The Cisco Adaptive Security Appliance supports redundancy by providing the Active/Standby (A/S) deployment model.

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

DNS Configuration

In the local IM and Presence Service enterprise deployment, the IM and Presence Service must publish a DNS SRV record for the IM and Presence Service domain to make it possible for other domains to discover the IM and Presence Service node through DNS SRV. The DNS SRV records reside on the DNS server in the enterprise DMZ.

If the local IM and Presence Service deployment is managing multiple domains, you must publish a DNS SRV record for each local domain. The DNS SRV record you publish for each local domain should resolve to the same public FQDN IP address.

For SIP federation with Microsoft OCS R2, you must publish the DNS SRV record "_sipfederationtls". The Microsoft enterprise deployment requires this record because you configure the IM and Presence Service as a Public IM Provider on the Access Edge server. In the external enterprise deployment, in order for the IM and Presence Service to discover the Microsoft domain, a DNS SRV record must exist that points to this external domain. If the IM and Presence Service node cannot discover the Microsoft domain using DNS SRV, you must configure a static route on the IM and Presence Service that points to the public interface of this external domain.

See the following figure for a sample DNS configuration for the DNS SRV record "_sipfederationtls_tcp.example.com".

Figure 12: DNS SRV for "_sipfederationtls"

The screenshot shows a dialog box titled "_sipfederationtls Properties" with a "Security" tab selected. The "Service Location (SRV)" section contains the following fields:

- Domain: example.com
- Service: _sipfederationtls
- Protocol: _tcp
- Priority: 0
- Weight: 0
- Port number: 5061
- Host offering this service: hostname.example.com

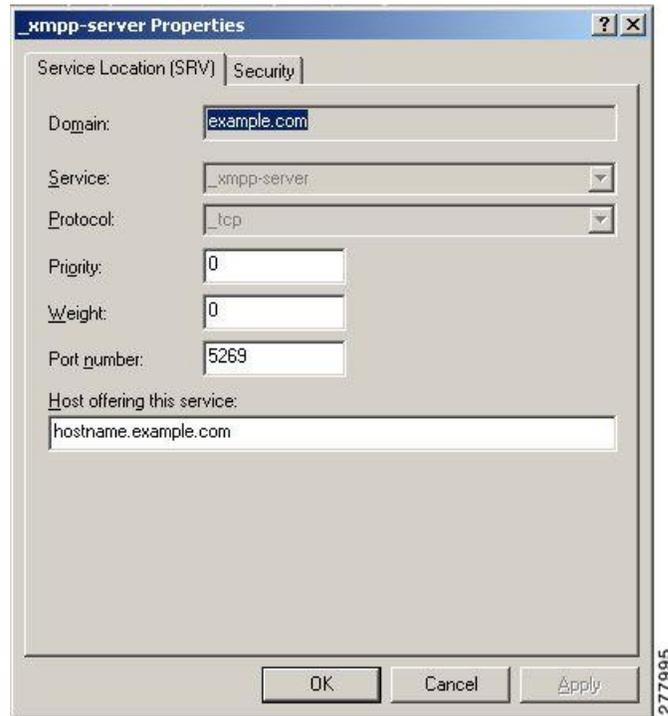
At the bottom of the dialog are buttons for "OK", "Cancel", "Apply", and "Help". A small number "350770" is visible in the bottom right corner of the dialog box.

Because DNS SRV records are publicly resolvable, if you turn on DNS forwarding in the local enterprise, DNS queries retrieve information about public domains outside of the local enterprise. If the DNS queries rely completely on DNS information within the local enterprise (you do not turn on DNS forwarding in the local enterprise), you must publish DNS SRV record/FQDN/IP address that points to the external domain. Alternatively, you can configure static routes.

For XMPP federation, you must publish the DNS SRV record "_xmpp-server". This record enables federated XMPP domains to discover the IM and Presence Service domain so users in both domains can exchange IM and availability information over XMPP. Similarly, external domains must publish the _xmpp-server record in their public DNS server to enable the IM and Presence Service to discover the external domain.

See the following figure for a sample DNS configuration for the DNS SRV record "_xmpp-server".

Figure 13: DNS SRV for "_xmpp-server"



Certificate Authority Server

For SIP federation, the Cisco Adaptive Security Appliance in the IM and Presence Service enterprise deployment, and the external enterprise deployment, share IM and availability over a secure SSL/TLS connection.

Each enterprise deployment must present a certificate that is signed by an external Certificate Authority (CA), however each enterprise deployment may use a different CA. Therefore each enterprise deployment must download the root certificate from the external CA of the other enterprise deployment to achieve a mutual trust between the two enterprise deployments.

For XMPP federation, you can choose whether or not to configure a secure TLS connection. If you configure TLS, on the IM and Presence Service you need to upload the root certificate of the Certificate Authority (CA) that signs the certificate of the external enterprise. This certificate must exist in the certificate trust store on the IM and Presence Service because the Cisco Adaptive Security Appliance does not terminate the TLS connections for XMPP federation; Cisco Adaptive Security Appliance acts as a firewall for XMPP federation.

Prerequisite Configuration Tasks for this Integration

Configure the IM and Presence Service for Integration



Note These prerequisite tasks apply to both SIP and XMPP federation.

Procedure

- Step 1** Install and configure the IM and Presence Service.
- At this point, perform the following checks to ensure that your IM and Presence Service is operating properly:
- Run the IM and Presence Service System Configuration Troubleshooter.
 - Check that you can add local contacts to the IM and Presence Service.
 - Check that your clients are receiving availability states from the IM and Presence Service node.
- Step 2** Configure the IM and Presence Service node with a Cisco Unified Communications Manager node as described in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*. Ensure that the IM and Presence Service node is working and issue free.

Related Topics

[Configure the Cisco Adaptive Security Appliance for Integration](#), on page 28

Configure the Cisco Adaptive Security Appliance for Integration



-
- Note**
- For SIP federation, you require the Cisco Adaptive Security Appliance.
 - For XMPP federation, you require a firewall. You can use any firewall, including the Cisco Adaptive Security Appliance for basic firewall/NAT/PAT functionality. For XMPP federation you do not use the Cisco Adaptive Security Appliance for TLS proxy functionality.
-

Install and configure the Cisco Adaptive Security Appliance. Perform the following basic configuration checks on the Cisco Adaptive Security Appliance:

Procedure

- Step 1** Access the Cisco Adaptive Security Appliance either through a console, hyperterminal, or the web-based Adaptive Security Device Manager (ASDM).

- Step 2** Obtain the appropriate licenses for the Cisco Adaptive Security Appliance. Note that a license is required for the TLS proxy on the Cisco Adaptive Security Appliance. Contact your Cisco representative for license information.
- Step 3** Upgrade the software (if necessary).
- Step 4** Configure the hostname using the command:
- ```
(config)# hostname name
```
- Step 5** Set the timezone, date and time in ASDM by choosing **Device Setup > System Time > Clock**, or through the CLI using the `clock set` command. Note the following:
- Set the clock on the Cisco Adaptive Security Appliance 5500 before configuring the TLS proxy.
  - We recommend that the Cisco Adaptive Security Appliance use the same NTP server as the IM and Presence Service cluster. The TLS connections may fail due to certificate validation failure if the clock is out of sync between the Cisco Adaptive Security Appliance and the IM and Presence Service node.
  - To view the NTP server address, use the command `ntp server server_address`, and the command `show ntp associat | status` to view the status of the NTP server.
- Step 6** Check the Cisco Adaptive Security Appliance 5500 modes. The Cisco Adaptive Security Appliance 5500 is configured to use single mode and routed mode by default.
- Check the current mode. This value is single mode by default.
- ```
(config)# show mode
```
- Check the current firewall mode. This is routed mode by default.
- ```
(config)# show firewall
```
- Set up the external and internal interfaces.
  - Set up the basic IP routes.

---

### Related Topics

[External and Internal Interface Configuration](#), on page 59

[Configure Static IP Routes](#), on page 60

[Configure the IM and Presence Service for Integration](#), on page 28





## CHAPTER 3

# Configuration Workflows for Interdomain Federation

---

- [Microsoft Lync Workflow \(Intracompany via Expressway\)](#), on page 31
- [Microsoft Lync Workflow \(Business to Business via ASA\)](#), on page 32
- [Microsoft OCS Workflow \(Direct Federation\)](#), on page 33
- [Microsoft OCS Workflow \(Business to Business via ASA\)](#), on page 34
- [Cisco Adaptive Security Appliance for SIP Federation Workflow](#), on page 34
- [XMPP Federation Workflow](#), on page 35

## Microsoft Lync Workflow (Intracompany via Expressway)

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft Lync via Expressway in an intracompany scenario.

This configuration supports both chat-only and chat+calling deployments.

### IM and Presence Service Configuration

1. In the IM and Presence Service, add a federated domain entry for the Microsoft Lync domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry. See [Add a Microsoft Lync Domain Within Enterprise](#), on page 79.
2. In the IM and Presence Service, configure an individual TLS static route for each Microsoft Lync server domain. Each route should point to a specific Microsoft front end server. See [Configure Static Routes from IM and Presence to Lync](#), on page 79.



---

**Note** You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.

---

3. In the IM and Presence Service, upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. Also, set up TLS Peer subjects. See [Set up Certificates on IM and Presence for Federation with Lync](#), on page 86.

### Expressway Configuration

For chat+calling deployments only, add an Expressway Gateway. On the gateway, configure Microsoft interoperability and the SIP broker. For Expressway configuration, go to [Configure Expressway Gateway for Microsoft Lync Federation, on page 80](#).



**Note** For chat-only deployments, you do not need the Expressway Gateway.

For chat+calling deployments that use Expressway Gateway's SIP Broker, support is limited to intracompany scenarios only. Business to Business is not supported.

### Lync Configuration

1. On the Lync server, configure TLS static routes using one of the following procedures:
  1. If you have a chat+calling deployment, [Configure a Static Route from Lync to IM and Presence, on page 82](#)
  2. If you have a chat-only deployment, [Configure Static Route from Lync to Expressway Gateway, on page 80](#)
2. On the Lync server, add the IM and Presence Service as a trusted application and add each IM and Presence cluster node to a trusted application server pool. See [Configure Trusted Applications on Lync Server, on page 84](#).
3. On the Lync server, commit the topology. See [Publish Topology, on page 86](#).

## Microsoft Lync Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft Lync federation, see [Add a SIP Federated Domain, on page 37](#).
- Configure the DNS SRV records, see [DNS Configuration for SIP Federation, on page 38](#).
- Configure the routing on the IM and Presence Service for Microsoft Lync federation, see [Routing Configuration on IM and Presence Service, on page 38](#)
- (Optional) Configure the email address for federation feature, see [Turn On Email for Federation, on page 134](#)
- Configure the TLS security settings on the IM and Presence Service, see [Configuration of Security Settings on IM and Presence Service, on page 41](#)
- Configure the Cisco Adaptive Security Appliance for Microsoft Lync federation, see [Cisco Adaptive Security Appliance Configuration for SIP Federation, on page 59](#) and [TLS Proxy Configuration on the Cisco Adaptive Security Appliance, on page 71](#).
- Configure certificate exchange for Microsoft Lync federation, see [Security Certificate Configuration on Lync Edge Server for TLS Federation, on page 58](#).
- Configuration of Lync Server 2010 and Edge servers for interdomain federation differs from that outlined within this guide for OCS. For information on configuring the Lync enterprise for interdomain federation

with the IM and Presence Service, see Microsoft documentation <http://technet.microsoft.com/en-us/library/gg399048.aspx>.

## Microsoft OCS Workflow (Direct Federation)

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft OCS. This configuration is for SIP Federation inside an enterprise, and without an ASA firewall.

### IM and Presence Service Configuration

1. In the IM and Presence Service, add a federated domain entry for the Microsoft OCS domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry. See [Add a Microsoft OCS Domain Within Enterprise, on page 91](#).
2. In the IM and Presence Service, configure an individual static route for each Microsoft OCS server domain. Each route should point to a specific Microsoft front end server. See [Configure Static Route on IM and Presence Service for Microsoft Servers, on page 92](#).



---

**Note** For OCS, you can choose either TCP or TLS as the protocol type.

---

### Microsoft OCS Configuration

1. On the OCS server, configure TCP or TLS static routes that point to the IM and Presence Service domain. Each route must point to a specific IM and Presence Service node. See [Configure Static Routes on OCS to Point to the IM and Presence Service, on page 93](#).
2. Verify that on the IM and Presence Service the Peer Auth Listener is configured as port 5061 and the Server Auth Listener is not port 5061. See [Verify Peer Authentication Listener, on page 94](#).
3. On the OCS server, configure host authorization entries for each IM and Presence Service node. With TLS encryption, you must add two entries for each IM and Presence node: one entry with the node IP address, and one entry with the FQDN. See [Adding a Host Authorization Entry for the IM and Presence Service Node on OCS, on page 94](#).
4. If you have TLS configured between OCS to IM and Presence Service, configure certificates on OCS for interdomain federation with IM and Presence Service. If you are not using TLS, you can skip this step. See [Configure Certificates on OCS for Interdomain Federation, on page 95](#).
5. On the OCS server, confirm the listener ports for TLS (The transport can be MTLS or TLS) or TCP are configured. For TLS, use port 5061. For TCP, use port 5060. See [Enable Port 5060/5061 on the OCS Server, on page 95](#).
6. If you are using TLS, configure OCS to use FIPS. See [Configure OCS to use FIPS, on page 96](#).
7. If you are using TLS, upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service. See [Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS, on page 97](#).

## Microsoft OCS Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft OCS federation, see [Add a SIP Federated Domain](#), on page 37.
- Configure the DNS SRV records, see [DNS Configuration for SIP Federation](#), on page 38.
- Configure the routing on the IM and Presence Service for Microsoft OCS federation, see [Routing Configuration on IM and Presence Service](#), on page 38
- (Optional) Configure the email address for federation feature, see [Turn On Email for Federation](#), on page 134
- Configure the TLS security settings on the IM and Presence Service, see [Configuration of Security Settings on IM and Presence Service](#), on page 41
- Configure the Cisco Adaptive Security Appliance for Microsoft OCS federation, see [Cisco Adaptive Security Appliance Configuration for SIP Federation](#), on page 59 and [TLS Proxy Configuration on the Cisco Adaptive Security Appliance](#), on page 71.
- Configure certificate exchange for Microsoft OCS federation, see [SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance](#), on page 45
- Configure the Microsoft OCS server, see [External Server Component Configuration for SIP Federation](#), on page 99.
- (Optional) Configure a load balancer for redundancy, see [Load Balancer Configuration for Redundancy for SIP Federation](#), on page 103
- For troubleshooting information on Microsoft OCS federation, see [Troubleshooting a SIP Federation Integration](#), on page 143

## Cisco Adaptive Security Appliance for SIP Federation Workflow

- Configure certificates between the Cisco Adaptive Security Appliance and the IM and Presence Service (inside interface), see [Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance](#), on page 45.
- Configure certificates between the Cisco Adaptive Security Appliance and the federated domain (outside Interface), see [Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge \(External Interface\) with Microsoft CA](#), on page 49.
- Configure PAT rules for private to public messaging, see [Port Address Translation \(PAT\)](#), on page 61.
- Configure static PAT for public to private messaging, see [Sample Static PAT Commands](#), on page 65.
- Configure the required access lists, see [Access List Configuration Requirements](#), on page 72.
- Configure the TLS proxy instances, see [Configure TLS Proxy Instances](#), on page 73.
- Associate the access lists with the TLS proxy, see [Associate Access List with TLS Proxy Instance Using Class Maps](#), on page 74.

# XMPP Federation Workflow



---

**Note** Follow this workflow for WebEx, IM and Presence Service, and IBM Sametime.

---

- Configure the IM and Presence Service for XMPP federation, see [IM and Presence Service Configuration for XMPP Federation, on page 111](#).
- Configure security for XMPP federation, see [Security Certificate Configuration for XMPP Federation, on page 125](#).
- (Optional) Configure the email address for federation feature, see [Turn On Email for Federation, on page 134](#).
- Turn on the XMPP Federation service, see [Turn On XMPP Federation Service, on page 124](#).
- Configure the Cisco Adaptive Security Appliance for XMPP federation, see [Configure the Cisco Adaptive Security Appliance for XMPP Federation, on page 122](#).
- For troubleshooting information on XMPP federation, see [Troubleshooting an XMPP Federation Integration, on page 153](#)





## CHAPTER 4

# IM and Presence Service Configuration for SIP Federation

---

- [Add a SIP Federated Domain, on page 37](#)
- [Routing Configuration on IM and Presence Service, on page 38](#)
- [Configure Federation Routing Parameters, on page 40](#)
- [Configuration of Security Settings on IM and Presence Service, on page 41](#)
- [Turn On the SIP Federation Service, on page 42](#)

## Add a SIP Federated Domain



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

When you configure a federated domain entry, the IM and Presence Service automatically adds the incoming ACL for the federated domain entry. You can see the incoming ACL associated with a federated domain on the **Cisco Unified CM IM and Presence Administration** user interface, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) federated domain entry.

### Procedure

---

- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > SIP Federation**.
- Step 2** Click **Add New**.
- Step 3** Enter the federated domain name in the Domain Name field.
- Step 4** Enter a description that identifies the federated domain in the Description field. This text string is displayed to the user in the Cisco Jabber Release 8.x privacy preferences available from the Manage Domains tab. Therefore make sure you enter a domain name that is easily-recognizable to the user.
- Step 5** Choose **Inter-domain to OCS/Lync**
- Step 6** If you are configuring federation with Microsoft, ensure that the check box for **Direct Federation** is unchecked.

**Step 7** Click **Save**.

**Step 8** After you add, edit, or delete a SIP federated domain, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services**. When you restart Cisco XCP Router, this causes a restart of all XCP services on the IM and Presence Service.

## Routing Configuration on IM and Presence Service

### DNS Configuration for SIP Federation

In the local IM and Presence Service enterprise, IM and Presence Service must publish a DNS SRV record for each local IM and Presence Service domain so that other domains can discover the IM and Presence Service node through DNS SRV. Each of the DNS SRV records must resolve to the same public IP address.

The Microsoft enterprise deployment requires the IM and Presence Service to publish a DNS SRV record for the IM and Presence Service domain because you configure the IM and Presence Service as a Public IM Provider on the Access Edge server.

In the IM and Presence Service enterprise deployment, you need to configure a DNS SRV record that points to `_sipfederationtls._tcp.imp_domain` over port 5061 where `imp_domain` is the name of the IM and Presence Service domain. This DNS SRV should point to the public FQDN of the routing IM and Presence Service node. This FQDN must be publicly resolvable.

In order for the IM and Presence Service to discover the external domain, a DNS SRV record must exist in the DNS server of the external domain that points to the FQDN of the external interface of the external domain.



**Tip** Use this sequence of commands for performing a DNS SRV lookup:

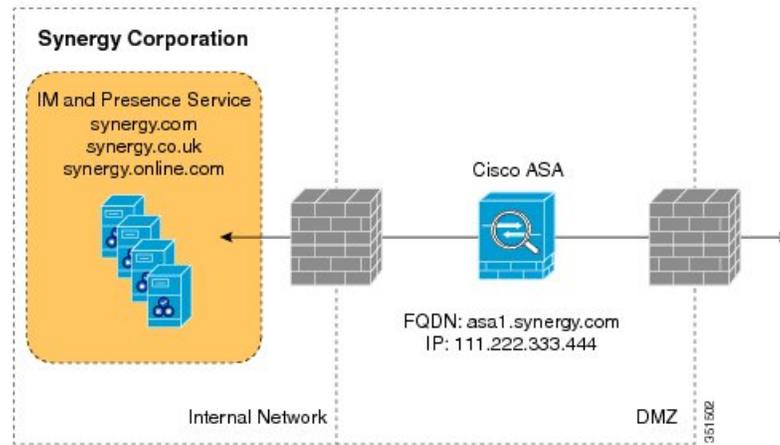
```
nslookupset type=srv _sipfederationtls._tcp.domain
```

If the IM and Presence Service cannot resolve the external enterprise through a public DNS lookup, you must configure static routes in your deployment.

#### SIP DNS SRVs in an Interdomain Federation Deployment

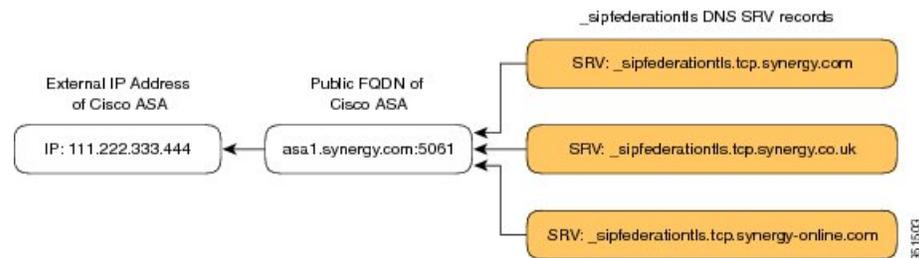
In the following example, multiple local domains must all resolve to the same Public FQDN and a DNS SRV record must be published for each domain that is hosted in the IM and Presence Service deployment. The following figure shows an example interdomain federation deployment with three local domains. You must publish a `_sipfederationtls` DNS SRV record for each domain.

Figure 14: Multiple Domains in a SIP-Based Federated Interdomain Deployment



Each DNS SRV record must resolve to the FQDN of the external (public) IP address of the Cisco Adaptive Security Appliance that is deployed in the DMZ (port 5061), as shown in the following figure.

Figure 15: SIP DNS SRV Resolving to FQDN of the Cisco Adaptive Security Appliance



### Related Topic

[Configure Static Routes Using TLS, on page 39](#)

## Configure Static Routes Using TLS



**Note** Static route configuration is only applicable to SIP federation.

If the IM and Presence Service node cannot discover the external domain using DNS SRV, you must configure a static route on IM and Presence Service that points to the external interface of the external domain.

### Procedure

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

- Step 2** Configure the static route parameters as follows:
- The destination pattern value must be configured such that the external enterprise domain is reversed. For example if the domain is "domaina.com" then the Destination Pattern value must be ".com.domaina.\*".
  - The Next Hop value is the FQDN or IP address of the external Access Edge for federation with a Microsoft server.
  - The Next Hop Port number is **5061**.
  - The Route Type value is **domain**.
  - The Protocol Type is **TLS**.
- Step 3** Click **Save**.
- 

## Configure Federation Routing Parameters

### Before you begin

Use this procedure if you need to reset the Federation routing parameter. By default, this parameter is set at installation to the FQDN of the publisher node automatically. The IM and Presence Service passes this value to each subscriber node.

### Procedure

---

- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Service Parameters**.
- Step 2** Choose the IM and Presence Service node from the Server drop-down list.
- Step 3** From the **Service** drop-down, choose **Cisco SIP Proxy**.
- Step 4** In the **Federation Routing Parameters (Clusterwide)** section, enter a public FQDN value for the **Federation Routing IM and Presence FQDN** and click **Save**.

- Note**
- This FQDN value must correspond to the `_sipfederationtls` entry in the public DNS for that IM and Presence Service domain. For example:
    - If the presence server FQDN is `imp1.cisco.com` and the DNS SRV is `_sipinternaltls._tcp.cisco.com` (pointing to FQDN `imp1-public.cisco.com`), the Federation Routing FQDN can be `imp1-public.cisco.com`.
    - If the presence server FQDN is `imp1.cisco.com` and the DNS SRV is `_sipinternaltls._tcp.extcisco.com` (`imp1-public.ciscoext.com`), the Federation Routing FQDN can be `imp1-public.ciscoext.com`.
- Note** This parameter does not apply for federation where there is a firewall (ASA) with TLS Proxy between the presence server and Lync Server and where the **Direct Federation** check box is checked under **Presence > Inter-domain federation > SIP Federation**.
- If you assign users to the routing IM and Presence Service node, this FQDN value cannot be the same as the actual FQDN of the routing IM and Presence Service node.

---

### What to do next

If you changed the Federation Routing FQDN parameter on the IM and Presence Service, restart the Cisco XCP Router. Log in to the **Cisco Unified Serviceability** user interface, choose **Tools > Control Center - Network Services in Cisco Unified Serviceability**.

When you restart Cisco XCP Router, this causes a restart of all XCP services on the IM and Presence Service.

## Configuration of Security Settings on IM and Presence Service



**Note** This procedure is only applicable if you do not have Cisco Adaptive Security Appliance in your federation deployment, for example, if you deploy federation within your enterprise and you want a secure TLS connection.

### Create a New TLS Peer Subject

When you import the Cisco Adaptive Security Appliance security certificate to the IM and Presence Service, the IM and Presence Service automatically adds the Cisco Adaptive Security Appliance as a TLS peer subject. Therefore you do not need to manually add the Cisco Adaptive Security Appliance as a TLS peer subject on the IM and Presence Service.

#### Procedure

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Security > TLS Peer Subjects**.
- Step 2** Click **Add New**.

- Step 3** Enter one of the following values:
- If you configure SIP federation with a Microsoft server, enter the external FQDN of the Access Edge Server in the Peer Subject Name field. This value must match the subject CN of the certificate that the Microsoft Access Edge server presents.
- Step 4** Enter the name of the external server in the Description field.
- Step 5** Click **Save**.
- 

**What to do next**

[Add TLS Peer to Selected TLS Peer Subjects List, on page 42](#)

**Related Topics**

[Import Self-Signed Certificate onto the IM and Presence Service, on page 47](#)

## Add TLS Peer to Selected TLS Peer Subjects List

**Before you begin**

Create a new TLS peer subject.

**Procedure**

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Security > TLS Context Configuration**.
- Step 2** Click **Find**.
- Step 3** Click **Default\_Cisco\_SIP\_Proxy\_Peer\_Auth\_TLS\_Context**.
- Step 4** Choose all ciphers from the list of available TLS ciphers.
- Step 5** Click the arrow to move these ciphers to **Selected TLS Ciphers**.
- Step 6** From the list of available TLS peer subjects, click the TLS peer subject that you configured in the previous section.
- Step 7** Click the arrow to move the TLS peer subject to **Selected TLS Peer Subjects**.
- Step 8** Check the **Disable Empty TLS Fragments** check box when you federate with Microsoft OCS.
- Step 9** Click **Save**.
- Step 10** Restart the **Cisco SIP Proxy** service.
- 

**Related Topics**

[Create a New TLS Peer Subject, on page 41](#)

## Turn On the SIP Federation Service

Turn on the Cisco XCP SIP Federation Connection Manager service. This turns on the SIP Federation feature for each user that you provision. You must complete this task on each node in the cluster.

## Procedure

---

- Step 1** Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Service Activation**.
- Step 2** Choose the server from the Server drop-down list.
- Step 3** Click **Go**.
- Step 4** Click the button next to the **Cisco XCP SIP Federation Connection Manager** service in the IM and Presence Services section.
- Step 5** Click **Save**.
- Step 6** The Cisco SIP Proxy service must be running for SIP federation to work. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Feature Services** and verify that the Cisco SIP Proxy service is running.
-





## CHAPTER 5

# SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance

---

- [Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance, on page 45](#)
- [Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge \(External Interface\) with Microsoft CA, on page 49](#)
- [Security Certificate Configuration on Lync Edge Server for TLS Federation, on page 58](#)

## Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance

### Generate Key Pair and Trustpoints on the Cisco Adaptive Security Appliance

You need to generate the key pair for this certification (for example `imp_proxy_key`), and configure a trustpoint to identify the self-signed certificate from Cisco Adaptive Security Appliance to IM and Presence Service (for example `imp_proxy`). You need to specify the enrollment type as “self” to indicate you are generating a self-signed certificate on Cisco Adaptive Security Appliance, and specify the certificate subject name as the IP address of the inside interface.

#### Before you begin

Ensure you carried out the configuration tasks described in the following chapters:

- [IM and Presence Service Configuration for SIP Federation, on page 37](#)
- [Cisco Adaptive Security Appliance Configuration for SIP Federation, on page 59](#)

#### Procedure

---

**Step 1** On the Cisco Adaptive Security Appliance enter configuration mode:

```
> Enable
> <password>
```

```
> configure terminal
```

**Step 2** Enter this command to generate the key pair for this certification:

```
crypto key generate rsa label imp_proxy_key modulus 1024
```

**Step 3** Enter the following sequence of commands to create a trustpoint for IM and Presence Service:

```
crypto ca trustpoint trustpoint_name (for example, imp_proxy)
(config-ca-trustpoint)# enrollment self
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# subject-name cn=ASA_inside_interface_ip_address
(config-ca-trustpoint)# keypair imp_proxy_key
```

Troubleshooting Tip

Enter the command `show crypto key mypubkey rsa` to check that the key pair is generated.

#### What to do next

[Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance, on page 46](#)

## Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance

#### Before you begin

- Complete the steps in [Generate Key Pair and Trustpoints on the Cisco Adaptive Security Appliance, on page 45](#).
- You need a text editor that has UNIX support to complete this procedure. We recommend Microsoft Wordpad version 5.1, or Microsoft Notepad version 5.1 service pack 2.

#### Procedure

**Step 1** Enter this command to generate the self-signed certificate:

```
(config-ca-trustpoint)# crypto ca enroll trustpoint_name (for example, imp_proxy)
```

**Step 2** Enter `no` when you are prompted to include the device serial number in the subject name.

**Step 3** Enter `yes` when you are prompted to generate the self-signed certificate.

**Step 4** Enter this command to prepare the certificate to export to the IM and Presence Service:

```
crypto ca export imp_proxy identity-certificate
```

The PEM encoded identity certificate displays on screen, for example:

```
-----BEGIN
CERTIFICATE-----MIIBnDCCAQWgAwIBAgIBMTANBgkqhkiG9w0BAQQFADAUMRIwEAYDVQQDEw1DVVAt..... -----END
CERTIFICATE-----
```

- Step 5** Copy and paste the entire contents of the Cisco Adaptive Security Appliance certificate into Wordpad or Notepad with a .pem extension.
- Step 6** Save the .pem file to your local machine.

---

**What to do next**

[Import Self-Signed Certificate onto the IM and Presence Service, on page 47](#)

## Import Self-Signed Certificate onto the IM and Presence Service

**Before you begin**

Complete the steps in [Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance, on page 46](#)

**Procedure**

- 
- Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
- Step 2** Click **Upload Certificate**.
- Step 3** For the Certificate Purpose, choose **cup-trust**.
- Note** Leave the Root Name field blank.
- Step 4** Click **Browse**, and locate the Cisco Adaptive Security Appliance .pem certificate file (that you created in the previous procedure) on your local computer.
- Step 5** Click **Upload File** to upload the certificate to the IM and Presence Service node.

**Troubleshooting Tips**

Perform a find on the certificate list, <asa ip address>.pem and an <asa ip address>.der are in the certificate list.

---

**What to do next**

[Generate a New Certificate on the IM and Presence Service, on page 47](#)

## Generate a New Certificate on the IM and Presence Service



- Note** Cisco ASA firewall certificates must have the Server Authentication and Client Authentication attributes set for inside, outside. This can be verified by checking the certificate Enhanced Key Usage (EKU) parameter or for an Object Identifier (OID) value of:

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

**Before you begin**

Complete the steps in [Import Self-Signed Certificate onto the IM and Presence Service, on page 47](#)

**Procedure**

- 
- Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
- Step 2** Click **Generate New**.
- Step 3** From the Certificate Purpose drop-down list, choose **cup**.
- Step 4** Click **Generate**.
- 

**What to do next**

[Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance, on page 48](#)

## Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance

In order to import the IM and Presence Service certificate onto the Cisco Adaptive Security Appliance, you need to create a trustpoint to identify the imported certificate from the IM and Presence Service (for example **cert\_from\_imp**), and specify the enrollment type as “terminal” to indicate that the certificate received from the IM and Presence Service will be pasted into the terminal.

**Note**

It is essential that the IM and Presence Service and the Cisco Unified Communications Manager nodes, and the Cisco Adaptive Security Appliance are synchronized off the same NTP source.

---

**Before you begin**

- Complete the steps in [Generate a New Certificate on the IM and Presence Service, on page 47](#).
- You need a text editor that has UNIX support to complete this procedure. We recommend Microsoft Wordpad version 5.1, or Microsoft Notepad version 5.1 service pack 2.

**Procedure**

- 
- Step 1** Enter configuration mode:
- ```
> Enable
> <password>
> configure terminal
```
- Step 2** Enter this sequence of commands to create a trustpoint for the imported IM and Presence Service certificate:
- ```
crypto ca trustpoint cert_from_imp enrollment terminal
```

- Step 3** Enter this command to import the certificate from IM and Presence Service:
- ```
crypto ca authenticate cert_from_imp
```
- Step 4** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management** on the IM and Presence Service.
- Step 5** Click **Find**.
- Step 6** Locate the IM and Presence Service certificate that you created in the previous procedure.
- Step 7** Click **Download**.
- Step 8** Open the imp.pem file using one of the recommended text editors.
- Step 9** Cut and paste the contents of the imp.pem into the Cisco Adaptive Security Appliance terminal.
- Step 10** Enter `quit`.
- Step 11** Enter `yes` when you are prompted to accept the certificate.
- Step 12** Run the command `show crypto ca certificate` to view the certificate.

What to do next

[Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge \(External Interface\) with Microsoft CA, on page 49](#)

Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA

These procedures are an example, and demonstrate how to configure certificates using the Microsoft CA.



Note An example of this procedure using the VeriSign CA is provided in the appendix of this guide.

CA Trustpoints

When generating a trustpoint, you must specify an enrollment method to be used with the trustpoint. You can use Simple Certificate Enrollment Process (SCEP) as the enrollment method (assuming you are using a Microsoft CA), where you use the **enrollment url** command to define the URL to be used for SCEP enrollment with the trustpoint you declared. The URL defined should be the URL of your CA.

You can also use manual enrollment as the enrollment method, where you use the **enrollment terminal** command to paste the certificate received from the CA into the terminal. Both enrollment method procedures are described in this section. Refer to the *Cisco Security Appliance Command Line Configuration Guide* for further details about the enrollment method.

In order to use SCEP, you need to download the Microsoft SCEP add-on from the following URL:

<http://www.microsoft.com/Downloads/details.aspx?familyid=9F306763-D036-41D8-8860-1636411B2D01&displaylang=en>

The SCEP add-on must be installed on the Microsoft CA that you are configuring the certificates on.

Download the SCEP add-on as follows:

- Download and run **scepsetup.exe**.
- Select **local system account**.
- Deselect **SCEP challenge phrase to enroll**.
- Enter the details of the CA.

When you click **Finish**, retrieve the SCEP URL. You use this URL during trustpoint enrollment on the Cisco Adaptive Security Appliance.

Configure a Certificate on the Cisco Adaptive Security Appliance Using SCEP

Procedure

-
- Step 1** Enter this command to generate a key pair for the CA:
- ```
crypto key generate rsa label public_key_for_ca modulus 1024
```
- Step 2** Enter this command to generate a trustpoint to identify the CA.
- ```
crypto ca trustpoint trustpoint_name
```
- Step 3** Use the **client-types** command to specify the client connection types for the trustpoint that can be used to validate the certificates associated with a user connection. Enter this command to specify a **client-types ssl** configuration which indicates that SSL client connections can be validated using this trustpoint:
- ```
(config-ca-trustpoint)# client-types ssl
```
- Step 4** Enter this command to configure the FQDN of the public IM and Presence Service address:
- ```
fqdn fqdn_public_imp_address
```
- Note** You may be issued a warning regarding VPN authentication here.
- Step 5** Enter this command to configure a keypair for the trustpoint:
- ```
keypair public_key_for_ca
```
- Step 6** Enter this command to configure the enrollment method for the trustpoint:
- ```
enrollment url http://ca_ip_address/certsrv/mscep/mscep.dll
```
- Step 7** Enter this command to obtain the CA certificate for the trustpoint you configured:
- ```
crypto ca authenticate trustpoint_name
```
- ```
INFO: Certificate has the following attributes: Fingerprint: cc966ba6 90dfe235 6fe632fc
2e521e48
```
- Step 8** Enter **yes** when you are prompted to accept the certificate from the CA.
- ```
Do you accept this certificate? [yes/no]: yes
```

Trustpoint CA certificate accepted.

**Step 9** Run the `crypto ca enroll` command.

```
crypto ca enroll trustpoint_name
```

The following warning output displays:

```
%WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems.
```

**Step 10** Enter **yes** when you are prompted to continue with the enrollment.

```
Would you like to continue with this enrollment? [yes/no]: yes
```

```
% Start certificate enrollment..
```

**Step 11** Enter a password when you are prompted to create a challenge password.

```
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate. For security reasons your password will
not be saved in the configuration. Please make a note of it.
```

```
Password: <password>
```

```
***** Re-enter password: *****
```

**Step 12** Enter **no** when you are prompted to include the device serial number in the subject name.

**Step 13** Enter **yes** when you are prompted to request the certificate from the CA.

```
Request certificate from CA? [yes/no]: yes
```

```
% Certificate request sent to Certificate Authority
```

**Step 14** Go to the CA and issue the pending certificate (if the certificate was not issued automatically).

### What to do next

[Certificate Configuration for the External Access Edge Interface, on page 53](#)

## Configure a Certificate on the Cisco Adaptive Security Appliance Using Manual Enrollment

Enrolling a trustpoint by uploading a CA certificate:

### Procedure

**Step 1** Enter this command to generate a key pair for the CA:

```
crypto key generate rsa label public_key_for_ca modulus 1024
```

**Step 2** Enter this sequence of commands to generate a trustpoint to identify the CA:

```
crypto ca trustpoint trustpoint_name fqdn fqdn_public_imp_address client-types ssl keypair
public_key_for_ca
```

- Note**
- The FQDN value must be the FQDN of the public IM and Presence Service address.
  - The keypair value must be the keypair created for the CA.

**Step 3** Enter this command to configure the enrollment method for the trustpoint:

```
enrollment terminal
```

**Step 4** Enter this command to authenticate the certificate:

```
crypto ca authenticate trustpoint_name
```

**Step 5** Acquire the root certificate of the CA:

- Go to your CA webpage, for example, `http(s)://ca_ip_address/certsrv`.
- Click **Download a CA certificate, certificate chain, or CRL**.
- Choose **Base 64**.
- Download the CA certificate.
- Save the certificate as a `.cer` file, for example `CARoot.cer`.

**Step 6** Open the root certificate (`.cer` file) in a text editor.

**Step 7** Copy and paste the certificate contents into the Cisco Adaptive Security Appliance terminal.

**Step 8** Enter `yes` when you are prompted to accept the certificate.

Generating a CSR for Cisco Adaptive Security Appliance Public Certificate.

**Step 9** Enter this command to send an enrollment request to the CA:

```
crypto ca enroll trustpoint_name
```

**Step 10** Enter `no` when you are asked if you want to include the device serial number in the subject name.

**Step 11** Enter `yes` when you are asked to Display Certificate Request to terminal.

**Step 12** Copy and paste this base-64 certificate into a text editor (to use in a later step).

**Step 13** Enter `no` when you are asked to redisplay the enrollment request.

**Step 14** Paste the base-64 certificate (that you copied in Step 4) into the certificate request page of your CA:

- Go to your CA webpage, for example, `http(s)://ca_ip_address/certsrv`.
- Click **Request a certificate**.
- Click **Advanced Certificate request**.
- Click **Submit a certificate request by using a base-64-encoded CMC orPKCS#10 file...**
- Paste the base-64 certificate (that you copied in Step 4).
- Submit the request and issue the certificate from the CA.
- Download the certificate and save as a `*.cer` file.
- Open the certificate in a text editor, copy and paste the contents into the terminal. End with the word **quit** on a separate line.

**Step 15** Enter this command to import the certificate that you receive from the CA:

```
crypto ca import trustpoint_name certificate
```

**Step 16** Enter `yes` when you are asked if you want to continue with the enrollment.

**What to do next**

[Certificate Configuration for the External Access Edge Interface, on page 53](#)

## Certificate Configuration for the External Access Edge Interface

This procedure describes how to configure the certificate on the Access Edge server with a standalone CA.

### Download CA Certification Chain

**Procedure**

- 
- Step 1** On the Access Edge Server, choose **Start > Run**.
- Step 2** Enter `http://<name of your Issuing CA Server>/certsrv`, and click **OK**.
- Step 3** Click **Download a CA certificate, certificate chain, or CRL** from the Select a task menu.
- Step 4** Click **Download CA certificate chain** from Download a CA Certificate, Certificate Chain, or CRL menu.
- Step 5** Click **Save** in the File Download dialog box.
- Step 6** Save the file on a hard disk drive on your server. This file has an extension of .p7b. If you open this .p7b file, the chain displays the following two certificates:
- a) name of Standalone root CA certificate
  - b) name of Standalone subordinate CA certificate (if any)
- 

**What to do next**

[Install a CA Certification Chain, on page 53](#)

### Install a CA Certification Chain

**Before you begin**

Complete the steps in [Download CA Certification Chain, on page 53](#)

**Procedure**

- 
- Step 1** Choose **Start > Run**.
- Step 2** Enter `mmc`, and click **OK**.
- Step 3** From the File menu, choose **Add/Remove Snap-in**.
- Step 4** Click **Add** in the Add/Remove Snap-in dialog box.
- Step 5** In the list of Available Standalone Snap-ins, choose **Certificates**.
- Step 6** Click **Add**.
- Step 7** Choose **Computer account**.
- Step 8** Click **Next**.
- Step 9** In the Select Computer dialog box, perform the following tasks:

- a) Ensure that **<Local Computer> (the computer this console is running on)** is selected.
- b) Click **Finish**.

- Step 10** Click **Close**.
- Step 11** Click **OK**.
- Step 12** In the left pane of the Certificates console, expand **Certificates: Local Computer**.
- Step 13** Expand Trusted Root Certification Authorities.
- Step 14** Right-click **Certificates**, and point to All Tasks.
- Step 15** Click **Import**.
- Step 16** In the Import wizard, click **Next**.
- Step 17** Click **Browse** and go to where you saved the certificate chain.
- Step 18** Choose the file, and click **Open**.
- Step 19** Click **Next**.
- Step 20** Leave the default value **Place all certificates in the store** and ensure that Trusted Root Certification Authorities appears under the Certificate store.
- Step 21** Click **Next**.
- Step 22** Click **Finish**.

---

### What to do next

[Request Certificate from CA Server, on page 54](#)

## Request Certificate from CA Server

### Before you begin

Complete the steps in [Install a CA Certification Chain, on page 53](#)

### Procedure

---

- Step 1** Log in to the Access Edge server and open a web browser.
- Step 2** Open the following URL: **http://certificate\_authority\_server\_IP\_address/certsrv**
- Step 3** Click **Request a Certificate**.
- Step 4** Click **Advanced Certificate Request**.
- Step 5** Click **Create and submit a request to this CA**.
- Step 6** In the Type of Certificate Needed list, click **Other**.
- Step 7** Enter the FQDN of the Access Edge external interface for the Subject Common Name,
- Step 8** in the Object Identifier (OID) field, enter the following value:  
1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2
- Note** A comma separates the two 1s in the middle of the OID.
- Step 9** Perform one of the following procedures:

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

**Step 10** Enter a friendly name.

**Step 11** Click **Submit**.

---

#### What to do next

[Download Certificate from CA Server, on page 55](#)

## Download Certificate from CA Server

#### Before you begin

Complete the steps in [Request Certificate from CA Server, on page 54](#)

#### Procedure

---

**Step 1** Launch the CA console by choosing **Start > Administrative Tools > Certificate Authority**.

**Step 2** In the left pane, click on **Pending Requests**.

**Step 3** In the right pane, right-click on the certificate request that you submitted.

**Step 4** Choose **All Tasks > Issue**.

**Step 5** Open `http://local_server/certsrv` on the Access Edge server that CA is running on.

**Step 6** Click **View the Status of a Pending Certificate Request** then click your certificate request.

**Step 7** Click **Install this certificate**.

---

#### What to do next

[Upload a Certificate onto Access Edge, on page 55](#)

## Upload a Certificate onto Access Edge

This procedure describes how to upload the certificate on the Access Edge server using the Certificate Wizard. You can also import the certificates manually on the Access Edge server by choosing **Microsoft Office Communications Server 2007 > Properties > Edge Interfaces**.

#### Before you begin

Complete the steps in [Download Certificate from CA Server, on page 55](#)

#### Procedure

---

**Step 1** Choose **Start > Administrative Tools > Computer Management** on the Access Edge server.

- Step 2** In the left pane, right-click on **Microsoft Office Communications Server 2007**.
- Step 3** Click **Certificates**.
- Step 4** Click **Next**.
- Step 5** Click the **Assign an existing certificate** task option.
- Step 6** Click **Next**.
- Step 7** Choose the certificate that you wish to use for the External Access Edge Interface, and click **Next**.
- Step 8** Click **Next**.
- Step 9** Check the **Edge Server Public Interface** check box, and click **Next**.
- Step 10** Click **Next**.
- Step 11** Click **Finish**.

---

### What to do next

[TLS Proxy Configuration on the Cisco Adaptive Security Appliance, on page 71](#)

## Create Custom Certificate for Access Edge Using Enterprise Certificate Authority

Refer to these instructions if you are using a Microsoft Enterprise CA to issue a client/server role certificate to the external interface of Access Edge or to the public interface of the Cisco Adaptive Security Appliance.

### Before you begin

These steps require that the Certificate Authority (CA) is an Enterprise CA and is installed on the Enterprise Edition of either Windows Server 2003 or 2008.

For additional details about these steps, refer to the Microsoft instructions:

<http://technet.microsoft.com/en-us/library/bb694035.aspx>

## Create and Issue a Custom Certificate Template

### Procedure

---

- Step 1** Follow Steps 1- 6 from the Microsoft site: [Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority](http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1).
- Tip** For Step 5, use a more appropriate name for this specific template, such as Mutual Authentication Certificate.
- Step 2** Follow these steps in place of Steps 7-12 from the Microsoft site:
  - a) Choose the **Extensions** tab. Make sure that under **Application Policies** that both **Client Authentication** and **Server Authentication** are present and that no other Policies are present. If these policies are not available, then you must add them before proceeding.
    - In the **Edit Application Policies Extension** dialog box, click **Add**.

- In the **Add Application Policy** dialog box, choose **Client Authentication**, press Shift and choose **Server Authentication**, and then click **Add**.
- In the **Edit Application Policies Extension** dialog box, choose any other policy that may be present and then click **Remove**.

In the **Properties of New Template** dialog box, you should now see listed as the description of Application Policies: Client Authentication, Server Authentication.

- Choose the **Issuance Requirement** tab. If you do not want the Certificate to be automatically issued, then choose **CA certificate manager approval**. Otherwise, leave this option blank.
- Choose the **Security** tab and ensure that all required users and groups have both read and enroll permission.
- Choose the **Request Handling** tab and click the **CSP** button.
- On the **CSP Selection** dialog box choose **Requests must use one of the following CSP's**.
- From the list of CSP's choose **Microsoft Basic Cryptographic Provider v1.0** and **Microsoft Enhanced Cryptographic Provider v1.0**, and click **OK**.

**Step 3** Continue with Steps 13-15 from the Microsoft site: Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.

[http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK\\_siteserver1](http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1)

---

#### What to do next

[Request Site Server Signing Certificate, on page 57](#)

## Request Site Server Signing Certificate

### Procedure

---

**Step 1** Follow Steps 1-6 from the Microsoft site: Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server.

[http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK\\_siteserver2](http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2)

**Tip** For Step 5, select the name of the certificate template you created previously, such as Mutual Authentication Certificate and enter the external FQDN of the access edge in the **Name** field.

**Step 2** Follow these steps in place of Steps 7-8 from the Microsoft site:

- If the certificate request is automatically issued then you are presented with an option to install the signed certificate. Select **Install this Certificate**.
- If the certificate request is not automatically issued then you must wait for the administrator to issue the certificate. Once issued:
  - On the member server, load Internet Explorer and connect to the Web enrollment service with the address `http://<server>/certsrv` where `<server>` is the name or IP address of the Enterprise CA.
  - On the Welcome page, choose **View the status of a pending certificate request**.

- c) Choose the issued certificate and click **Install this Certificate**.
- 

## Security Certificate Configuration on Lync Edge Server for TLS Federation

The following guide from Microsoft's TechNet Library (<http://technet.microsoft.com/en-us/library/gg398409.aspx>) explains how to configure certificates on Access Edge for TLS federation with Microsoft Lync. The IM and Presence Service requires Mutual TLS authentication for federated connections, therefore you must configure Microsoft Lync certificates to support both Server and Client Authentication. You can use this guide to configure Lync Server to federate directly with the IM and Presence Service over TLS.

For information about how to configure static routes on Lync server for direct federation, see [Configure a Static Route from Lync to IM and Presence](#), on page 82.



## CHAPTER 6

# Cisco Adaptive Security Appliance Configuration for SIP Federation

---

- [Cisco Adaptive Security Appliance Unified Communication Wizard](#), on page 59
- [External and Internal Interface Configuration](#), on page 59
- [Configure Static IP Routes](#), on page 60
- [Port Address Translation \(PAT\)](#), on page 61
- [Sample Static PAT Commands](#), on page 65
- [Cisco Adaptive Security Appliance Upgrade Options for Existing Deployments](#), on page 68

## Cisco Adaptive Security Appliance Unified Communication Wizard

If you deploy a single IM and Presence Service in your interdomain federation deployment, you can use the Unified Communication wizard on the Cisco Adaptive Security Appliance to configure the presence federation proxy between the Cisco Adaptive Security Appliance and the IM and Presence Service.

A configuration example showing the Unified Communication wizard is provided on the IM and Presence Service documentation wiki, see the URL below.

## External and Internal Interface Configuration

On the Cisco Adaptive Security Appliance you must configure two interfaces as follows:

- Use one interface as the outside or external interface. This is the interface to the internet and to the external domain servers (for example, Microsoft Access Edge/Access Proxy).
- Use the second interface as the inside or internal interface. This is the interface to the IM and Presence Service or to the load balancer, depending on your deployment.
- When configuring an interface, you need to refer it with an interface type, for example Ethernet or Gigabit Ethernet, and an interface slot. The Cisco Adaptive Security Appliance has four embedded Ethernet or Gigabit Ethernet ports on slot 0. You may optionally add an SSM-4GE module in slot 1 to obtain an additional four Gigabit Ethernet ports on slot 1.

- For each interface to route traffic, you need to configure an interface name and an IP address. The internal and external interface IP addresses must be in different subnets, which means they must have different submasks.
- Each interface must have a security level ranging from zero to 100 (from lowest to highest). A security level value of 100 is the most secure interface (inside interface). A security level value of zero is the least secure interface. If you do not explicitly set the security level for the inside or outside interface, then the Cisco Adaptive Security Appliance sets the security level to 100 by default.
- Please refer to the *Cisco Security Appliance Command Line Configuration Guide* for details on configuring the external and internal interfaces through the CLI.



**Note** You can configure the internal and external interfaces using the ASDM startup wizard. You can also view or edit an interface in ASDM by choosing **Configuration > Device Setup > Interfaces**.

## Configure Static IP Routes

The Cisco Adaptive Security Appliance supports both static routes and dynamic routing protocols such as OSPF, RIP, and EIGRP. For this integration you need to configure static routes that define the next hop address for IP traffic routed to the inside interface and for traffic routed to the outside interface of the Cisco Adaptive Security Appliance. In the procedure below, the `dest_ip` mask is the IP address for the destination network and the `gateway_ip` value is the address of the next-hop router or gateway.

For a detailed description on setting up default and static routes on the Cisco Adaptive Security Appliance, refer to the *Cisco Security Appliance Command Line Configuration Guide*.

### Before you begin

Complete the steps in [External and Internal Interface Configuration, on page 59](#)

### Procedure

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to add a static route for the inside interface:

```
hostname(config)# route inside dest_ip mask gateway_ip
```

**Step 3** Enter this command to add a static route for the outside interface:

```
hostname(config)# route outside dest_ip mask gateway_ip
```

**Note** You can also view and configure the static routes from ASDM by choosing **Configuration > Device Setup > Routing > Static routes**.

Figure 16: Viewing Static Routes Through ASDM

| #                                        | Type    | Original Source | Destination | Service  | Translated Interface | Address      |
|------------------------------------------|---------|-----------------|-------------|----------|----------------------|--------------|
| inside (5 Static rules, 1 Dynamic rules) |         |                 |             |          |                      |              |
| 1                                        | Static  | 10.53.46.178    |             | TCP 5061 | outside              | 10.53.46.199 |
| 2                                        | Static  | 10.53.46.178    |             | UDP 5070 | outside              | 10.53.46.199 |
| 3                                        | Static  | 10.53.46.178    |             | TCP 5062 | outside              | 10.53.46.199 |
| 4                                        | Static  | 10.53.46.178    |             | TCP sip  | outside              | 10.53.46.199 |
| 5                                        | Static  | 10.53.46.178    |             | UDP sip  | outside              | 10.53.46.199 |
| 6                                        | Dynamic | any             |             |          | outside              | 10.53.46.199 |

**What to do next**

[Port Address Translation \(PAT\), on page 61](#)

## Port Address Translation (PAT)

### Port Address Translation for This Integration



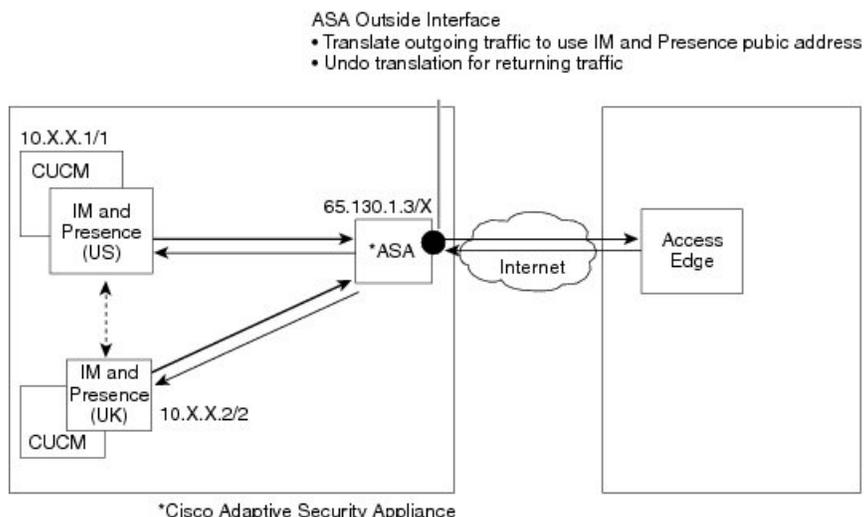
**Note** You also use Port Address Translation if you federate with another IM and Presence Service enterprise deployment in an external domain.

For this integration, Cisco Adaptive Security Appliance uses Port Address Translation (PAT) and static PAT for message address translation. Cisco Adaptive Security Appliance does not use Network Address Translation (NAT) for this integration.

This integration uses PAT to translate messages sent from the IM and Presence Service to an external domain (private to public messages). Port Address Translation (PAT) means the real address and source port in a packet is substituted with a mapped address and unique port that can be routed on the destination network. This translation method uses a two step process that translates the real IP address and port to a mapped IP address and port, and then the translation is “undone” for returning traffic.

The Cisco Adaptive Security Appliance translates messages sent from the IM and Presence Service to an external domain (private to public messages) by changing the private IP address and port on the IM and Presence Service to a public IP address and one or more public port(s). Therefore, a local IM and Presence Service domain only uses one public IP address. The Cisco Adaptive Security Appliance assigns a NAT command to the outside interface and translates the IP address and port of any message received on that interface as illustrated in the following figure.

Figure 17: Example PAT for Messages Originating from the IM and Presence Service to an External Domain

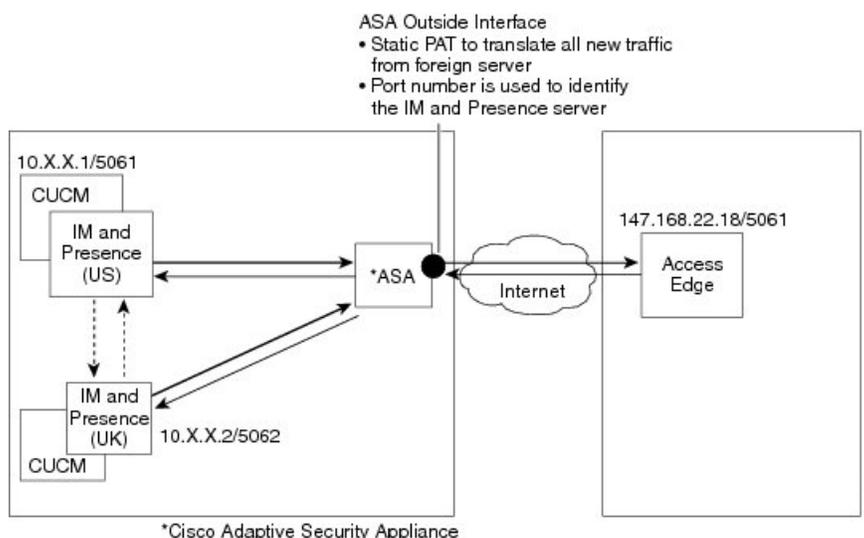


For new messages sent from an external domain to the IM and Presence Service, the Cisco Adaptive Security Appliance uses static PAT to map any message sent to the public IP address and port for the IM and Presence Service to a designated IM and Presence Service node. Using static PAT allows you to translate the real IP address to a mapped IP address, and the real port number to a mapped port number. You can translate the real port number to the same port number or to a different port number. In this case, the port number identifies the correct IM and Presence Service node to handle the message request, as shown in the following figure.

**Note**

If a user does not exist on the IM and Presence Service node, the IM and Presence Service routing node uses intercluster routing to redirect the message. All responses are sent to the Cisco Adaptive Security Appliance from the IM and Presence Service routing node.

Figure 18: Static PAT for Messages Originating From an External Domain



## PAT for Private to Public Requests

For this integration, the address translation for private to public messages involves the following configuration:

- Define a NAT rule to identify the real IP address and port number that you wish to translate. In this case, configure a NAT rule that states that the Cisco Adaptive Security Appliance must apply a NAT action to any message received on the internal interface.
- Configure a global NAT action to specify the mapped addresses to use for messages exiting through the external (outside) interface. For this integration, specify only one address (because it uses PAT). The NAT action maps the IP address (of messages received on the internal interface) to the IM and Presence Service public address.

The following table provides sample global address translation commands for the Cisco Adaptive Security Appliance, releases 8.2 and 8.3. The first row is mandatory for both a single IM and Presence Service deployment, and a multiple IM and Presence Service deployment. The second row is for single IM and Presence Service deployment only. The third row is for a multiple IM and Presence Service deployment.

**Table 11: Sample Global Address Translation Commands**

| Sample Configuration                                                                                                                                                         | Cisco Adaptive Security Appliance Release 8.2 Global Command                                                                                        | Cisco Adaptive Security Appliance Release 8.3 Global Command                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You can use this sample NAT configuration in a deployment where there are one or more IM and Presence Service nodes on the inside interface, with no other firewall traffic. | <pre>global (outside) 1 public_imp_address nat (inside) 1 0 0</pre>                                                                                 | <pre>object network obj_any host 0.0.0.0 nat (inside,outside) dynamic public_imp_address</pre>                                                                                                                                           |
| You can use this sample NAT configuration in a deployment where there is one IM and Presence Service node on the inside interface, with other firewall traffic.              | <pre>global (outside) 1 public_imp_address nat (inside) 1 private_imp_address 255.255.255.255 global (outside) 2 interface nat (inside) 2 0 0</pre> | <pre>host private_imp_address nat (inside,outside) dynamic public_imp_address  object network my_inside subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface</pre>                                                              |
| You can use this sample NAT configuration in a deployment where there are multiple IM and Presence Service nodes on the inside interface, with other firewall traffic.       | <pre>global (outside) 1 public_imp_ip nat (inside) 1 private_imp_net private_imp_netmask  global (outside) 2 interface nat (inside) 2 0 0</pre>     | <pre>object network obj_private_subnet.0_255.255.255.0 subnet private_subnet 255.255.255.0 nat (inside,outside) dynamic public_imp_address  object network my_inside subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface</pre> |




---

**Note** The sample configuration shown in the last row of the table assumes that when there are multiple IM and Presence Service nodes located behind the Cisco Adaptive Security Appliance, and these IM and Presence Service nodes are all on the same subnet. Specifically, if all the inside IM and Presence Service nodes are on the 2.2.2.x/24 network, the NAT command is: `nat (inside) 1 2.2.2.0 255.255.255.0`

---

## Static PAT for New Requests

For this integration the address translation for private to public messages involves the following configuration:

- Configure a static PAT command on TCP for the following ports: 5060, 5061, 5062 and 5080.
- Configure a separate static PAT command on UDP for port 5080.

This integration uses the following ports:

- 5060 - the Cisco Adaptive Security Appliance uses this port for generic SIP inspection.
- 5061 - The SIP requests are sent to this port and this triggers the TLS handshake.
- 5062, 5080 - The IM and Presence Service uses these ports in the SIP VIA/CONTACT headers.




---

**Note** You can check the peer auth listener port on the IM and Presence Service by logging in to **Cisco Unified CM IM and Presence Administration** and choosing **System > Application Listeners**.

---

### Related Topics

[Sample Static PAT Commands](#), on page 65

[Sample Cisco Adaptive Security Appliance Configuration](#), on page 155

## NAT Rules in ASDM

You can view the NAT rules in ASDM by choosing **Configuration > Firewall > NAT Rules**. The first five NAT rules shown in the following figure are the static PAT entries, and the final dynamic entry is the outgoing PAT configuration that maps any outgoing traffic to the public IM and Presence Service IP address and port.

Figure 19: Viewing NAT Rules in ASDM

| #                                        | Type    | Original Source | Destination | Service  | Translated Interface | Address      |
|------------------------------------------|---------|-----------------|-------------|----------|----------------------|--------------|
| inside (5 Static rules, 1 Dynamic rules) |         |                 |             |          |                      |              |
| 1                                        | Static  | 10.53.46.178    |             | TCP 5061 | outside              | 10.53.46.199 |
| 2                                        | Static  | 10.53.46.178    |             | UDP 5070 | outside              | 10.53.46.199 |
| 3                                        | Static  | 10.53.46.178    |             | TCP 5062 | outside              | 10.53.46.199 |
| 4                                        | Static  | 10.53.46.178    |             | TCP sip  | outside              | 10.53.46.199 |
| 5                                        | Static  | 10.53.46.178    |             | UDP sip  | outside              | 10.53.46.199 |
| 6                                        | Dynamic | any             |             |          | outside              | 10.53.46.199 |

**Related Topics**

[Sample Static PAT Commands](#), on page 65

[Sample Cisco Adaptive Security Appliance Configuration](#), on page 155

## Sample Static PAT Commands



**Note** This section shows sample commands for Cisco Adaptive Security Appliance Release 8.3 and Release 8.2. You need to execute these commands when you configure a fresh configuration of Cisco Adaptive Security Appliance for federation.

## PAT Configuration for Routing the IM and Presence Service Node

The following table shows the PAT commands for the routing the IM and Presence Service node, where the peer auth listener port is 5062.



**Note** For Cisco Adaptive Security Appliance 8.3 configuration, you only need to define an object once and you can reference that object in multiple commands; you do not need to repeatedly define the same object.

Table 12: PAT Commands for Routing the IM and Presence Service Node

| Cisco Adaptive Security Appliance Release 8.2 Static Commands                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Cisco Adaptive Security Appliance Release 8.3 NAT Commands                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>static (inside,outside) tcp public_imp_ip_address 5061 routing_imp_private_address 5062 netmask 255.255.255.255</pre> <p>If the routing IM and Presence Service peer auth listening port is 5061, use the command:</p> <pre>static (inside,outside) tcp public_imp_ip_address 5061 routing_imp_private_address 5061 netmask 255.255.255.255</pre> <pre>static (inside,outside) tcp public_imp_ip_address 5080 routing_imp_private_address 5080 netmask 255.255.255.255</pre> <pre>static (inside,outside) tcp public_imp_ip_address 5060 routing_imp_private_address 5060 netmask 255.255.255.255</pre> | <pre>object network obj_host_public_imp_ip_address (for example object network obj_host_10.10.10.10) #host public_imp_ip_address</pre> <pre>object network obj_host_routing_imp_private_address host routing_imp_private_address</pre> <pre>object service obj_tcp_source_eq_5061 service tcp source eq 5061</pre> <pre>object service obj_tcp_source_eq_5062 service tcp source eq 5062</pre> <pre>nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061</pre> <p>If the routing IM and Presence Service peer auth listening port is 5061, use the command:</p> <pre>nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5061 obj_tcp_source_eq_5061</pre> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <pre>object service obj_tcp_source_eq_5080 service tcp source eq 5080 nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5080 obj_tcp_source_eq_5080</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <pre>object service obj_tcp_source_eq_5060 service tcp source eq 5060</pre> <p><b>Note</b> 5060 displays as "sip" in the service object.</p> <pre>nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5060 obj_tcp_source_eq_5060</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <pre>static (inside,outside) tcp public_imp_ip_address 5062 routing_imp_private_address 5062 netmask 255.255.255.255</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <pre>nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5062</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## PAT Configuration for Intercluster or Intracluster IM and Presence Service Nodes

In a multinode or an intercluster IM and Presence Service deployment, if the non-routing nodes in the IM and Presence Service clusters communicate directly with the Cisco Adaptive Security Appliance, you must configure a set of static PAT commands for each of these nodes. The commands listed below are an example of a set of the static PAT commands you must configure for a single node.

You must use an unused arbitrary port. We recommend that you select a corresponding number, for example, 5080 uses the unused arbitrary port X5080 where X corresponds to a number that uniquely maps to an IM and Presence Service intercluster or intracluster server. For example 45080 uniquely maps to one node and 55080 uniquely maps to another node.

The following table shows the NAT commands for the non-routing IM and Presence Service nodes. Repeat the commands for each non-routing IM and Presence Service node.



### Note

For Cisco Adaptive Security Appliance 8.3 configuration, you only need to define an object once and you can reference that object in multiple commands; you do not need to repeatedly define the same object.

**Table 13: NAT Commands for Non-Routing IM and Presence Service Nodes**

| Cisco Adaptive Security Appliance Release 8.2 Static Command                                                                                                                                                                                                                                                                                                      | Cisco Adaptive Security Appliance Release 8.3 NAT Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>static (inside,outside) tcp public_imp_address 45062 intercluster_imp_private_address 5062 netmask 255.255.255.255</pre> <p>If the intercluster IM and Presence Service peer auth listening port is 5061, use the command:</p> <pre>static (inside,outside) tcp public_imp_address 45061 intercluster_imp_private_address 5061 netmask 255.255.255.255</pre> | <pre>object network obj_host_intercluster_imp_private_address host intercluster_imp_private_address  object service obj_tcp_source_eq_45062 service tcp source eq 45062  nat (inside,outside) source static obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_45062</pre> <p>If the intercluster IM and Presence Service peer auth listening port is 5061, use the command:</p> <pre>object service obj_tcp_source_eq_45061 service tcp source eq 45061 nat (inside,outside) source static obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5061 obj_tcp_source_eq_45061</pre> |

| Cisco Adaptive Security Appliance Release 8.2 Static Command                                                                     | Cisco Adaptive Security Appliance Release 8.3 NAT Command                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>static (inside,outside) tcp public_imp_ip_address 45080 intercluster_imp_private_address 5080 netmask 255.255.255.255</pre> | <pre>object service obj_tcp_source_eq_45080 service tcp source eq 45080 nat (inside,outside) source static obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080</pre> |
| <pre>static (inside,outside) tcp public_imp_ip_address 45060 intercluster_imp_private_address 5060 netmask 255.255.255.255</pre> | <pre>object service obj_tcp_source_eq_45060 service tcp source eq 45060 nat (inside,outside) source static obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5060 obj_tcp_source_eq_45060</pre> |

**Related Topics**

[Static PAT for New Requests](#), on page 64

[PAT Configuration for Routing the IM and Presence Service Node](#), on page 65

## Cisco Adaptive Security Appliance Upgrade Options for Existing Deployments

If you upgrade from Cisco Adaptive Security Appliance Release 8.2 to Release 8.3, the Cisco Adaptive Security Appliance migrates the existing commands seamlessly during the upgrade.

**Note**

Once you upgrade to IM and Presence Service Release 9.0, you must open port 5080 on the Cisco Adaptive Security Appliance for each IM and Presence Service 9.0 node located behind the Cisco Adaptive Security Appliance. This is independent of whether you have upgraded the Cisco Adaptive Security Appliance also.

Use one of the following upgrade procedures when you upgrade both the IM and Presence Service and Cisco Adaptive Security Appliance in your existing federation deployment:

**Upgrade Procedure Option 1:**

1. Upgrade the IM and Presence Service to Release 9.0.
2. Configure NAT rules for port 5080 on the Cisco Adaptive Security Appliance.
3. Confirm that federation is working in your deployment after the IM and Presence Service upgrade.
4. Upgrade the Cisco Adaptive Security Appliance to Release 8.3.
5. Confirm that federation is working in your deployment after the Cisco Adaptive Security Appliance upgrade.

**Upgrade Procedure Option 2:**

1. Upgrade both the IM and Presence Service nodes to Release 9.0 and Cisco Adaptive Security Appliance to Release 8.3.
2. After both upgrades, configure NAT rules for port 5080 on the Cisco Adaptive Security Appliance.
3. Confirm that federation is working in your deployment.

These are the commands you require to open port 5080 for each IM and Presence Service Release 9.0 node that sits behind Cisco Adaptive Security Appliance:

**Table 14: Cisco ASA commands to open port 5080**

| <b>Cisco Adaptive Security Appliance Release 8.2 Static Command</b>                                                                                                                                                                                                                                                                                                                                | <b>Cisco Adaptive Security Appliance Release 8.3 NAT Command</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>static (inside,outside) tcp public_imp_ip_address 5080 routing_imp_private_address 5080 netmask 255.255.255.255  static (inside,outside) tcp public_imp_ip_address 45080 intercluster_imp_private_address 5080 netmask 255.255.255.255</pre> <p><b>Note</b> Configure these commands for each intercluster IM and Presence Service 9.0 node, and use a different arbitrary port for each.</p> | <pre>object service obj_tcp_source_eq_5080 # service tcp source eq 5080  nat (inside,outside) source static obj_host_routing_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5080 obj_tcp_source_eq_5080  object service obj_tcp_source_eq_45080 # service tcp source eq 45080  nat (inside,outside) source static obj_host_intercluster_imp_private_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080</pre> <p><b>Note</b> Configure these commands for each intercluster IM and Presence Service 9.0 node, and use a different arbitrary port for each.</p> |





## CHAPTER 7

# TLS Proxy Configuration on the Cisco Adaptive Security Appliance

---



**Note** For up to date release information on configuring the TLS proxy, please refer to the *Cisco Adaptive Security Appliance Configuration Guide*.

---

- [TLS Proxy, on page 71](#)
- [Access List Configuration Requirements, on page 72](#)
- [Configure TLS Proxy Instances, on page 73](#)
- [Associate Access List with TLS Proxy Instance Using Class Maps, on page 74](#)
- [Enable TLS Proxy, on page 75](#)
- [Configure Cisco Adaptive Security Appliance for an Intercluster Deployment, on page 76](#)

## TLS Proxy

The Cisco Adaptive Security Appliance acts as a TLS proxy between the IM and Presence Service and the external server. This allows the Cisco Adaptive Security Appliance to proxy TLS messages on behalf of the server (that initiates the TLS connection), and route the TLS messages from the proxy to the client. The TLS proxy decrypts, inspects and modifies the TLS messages as required on the incoming leg, and then re-encrypts traffic on the return leg.



**Note** Before configuring the TLS proxy, you must configure the Cisco Adaptive Security Appliance security certificates between the Cisco Adaptive Security Appliance and the IM and Presence Service, and between the Cisco Adaptive Security Appliance and the external server. Complete the procedures in the following sections to accomplish this:

- [Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance, on page 45](#)
  - [Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge \(External Interface\) with Microsoft CA, on page 49](#)
-

**Related Topics**

[Common Cisco Adaptive Security Appliance Problems and Recommended Actions](#), on page 143

# Access List Configuration Requirements

This section lists the access list configuration requirements for a single IM and Presence Service deployment.



**Note**

- For each access list, you must configure a corresponding class-map, and configure an entry in the policy-map global policy.
- You can check the peer auth listener port on the IM and Presence Service by logging in to **Cisco Unified Communications Manager IM and Presence Administration** and choosing **System > Application Listeners**.

**Table 15: Single IM and Presence Service Access List Configuration Requirements**

| Item                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deployment Scenario: An IM and Presence Service node federating with one or more external domains |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Configuration Requirement:                                                                        | <p>Configure the following two access lists for each external domain that IM and Presence Service is federates with:</p> <ul style="list-style-type: none"> <li>• Configure an access list to allow the IM and Presence Service to send messages to the external domain on port 5061.</li> <li>• Configure an access list to allow the IM and Presence Service to receive messages from the external domain on port 5061. If you use the Cisco Adaptive Security Appliance Release 8.3, use the actual port that IM and Presence Service listens on for SIP federation (check the peer auth listener port on IM and Presence Service).</li> </ul>                                                                                                |
| Configuration Example:                                                                            | <pre>access-list ent_imp_to_external_server extended permit tcp host routing_imp_private_address host external_public_address eq 5061</pre> <p>Cisco Adaptive Security Appliance Release 8.2:</p> <pre>access-list ent_external_server_to_imp extended permit tcp host external_public_address host imp_public_address eq 5061</pre> <p>Cisco Adaptive Security Appliance Release 8.3:</p> <pre>access-list ent_external_server_to_imp extended permit tcp host external_public_address host imp_private_address eq 5061</pre> <p><b>Note</b> In the access list above 5061 is the port that the IM and Presence Service listens on for SIP messaging. If the IM and Presence Service listens on port 5062, specify 5062 in the access list.</p> |
| Deployment Scenario: Intercluster deployment. This also applies to a multinode deployment.        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Item                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration Requirement: | <p>Configure the following two access lists for each intercluster IM and Presence Service node.</p> <ul style="list-style-type: none"> <li>• Configure an access list to allow the IM and Presence Service to send messages to the external domain on port 5061.</li> <li>• Configure an access list to allow the IM and Presence Service to receive messages from the external domain on the arbitrary port 5061. If you use Cisco Adaptive Security Appliance Release 8.3, use the actual port that the IM and Presence Service listens on for SIP federation (check the peer auth listener port on the IM and Presence Service)</li> </ul>                                                                                                                                   |
| Configuration Example:     | <pre>access-list ent_intercluster_imp_to_external_server extended permit tcp host intercluster_imp_private_address host external_public_address eq 5061</pre> <p>Cisco Adaptive Security Appliance Release 8.2:</p> <pre>access-list ent_external_server_to_intercluster_imp extended permit tcp host external_public_address host imp_public_address eq arbitrary_port</pre> <p>Cisco Adaptive Security Appliance Release 8.3:</p> <pre>ent_external_server_to_intercluster_imp extended permit tcp host external_public_address host imp_private_address eq 5061</pre> <p>In the access list above, 5061 is the port that the IM and Presence Service listens on for SIP messaging. If the IM and Presence Service listens on port 5062, specify 5062 in the access list.</p> |

**Related Topics**

- [Sample Cisco Adaptive Security Appliance Configuration](#), on page 155
- [Configure TLS Proxy Instances](#), on page 73
- [Associate Access List with TLS Proxy Instance Using Class Maps](#), on page 74
- [Enable TLS Proxy](#), on page 75

## Configure TLS Proxy Instances

For this integration, you need to create two TLS proxy instances. The first TLS proxy handles the TLS connections initiated by the IM and Presence Service, where the IM and Presence Service is the client and the external domain is the server. In this case, the Cisco Adaptive Security Appliance acts as the TLS server facing the "client" which is the IM and Presence Service. The second TLS Proxy handles the TLS connections initiated by the external domain, where the external domain is the client and where the IM and Presence Service is the server.

The TLS proxy instance defines “trustpoints” for both the server and the client. The direction from which the TLS handshake is initiated determines the trustpoint defined in the server and client commands:

- If the TLS handshake initiates from the IM and Presence Service to the external domain, the server command specifies the trustpoint that contains the Cisco Adaptive Security Appliance self-signed certificate. The client command specifies the trustpoint that contains the Cisco Adaptive Security Appliance certificate that is used in the TLS handshake between Cisco Adaptive Security Appliance and the external domain.

- If the handshake initiates from the external domain to the IM and Presence Service, the server command specifies the trustpoint that contains the Cisco Adaptive Security Appliance certificate the TLS handshake uses between the Cisco Adaptive Security Appliance and the external domain. The client command specifies the trustpoint that contains the Cisco Adaptive Security Appliance self-signed certificate.

### Before you begin

- Complete the steps in [Access List Configuration Requirements](#), on page 72.

### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Create a TLS proxy instance for TLS connections initiated by the IM and Presence Service. This example creates a TLS proxy instance called `imp_to_external`:

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

**Step 3** Create a TLS proxy instance for TLS connections initiated by a external domain. This example creates a TLS proxy instance called `external_to_imp`:

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

---

### What to do next

[Associate Access List with TLS Proxy Instance Using Class Maps](#), on page 74

## Associate Access List with TLS Proxy Instance Using Class Maps

Using the class map command, you need to associate a TLS Proxy instance to each of the external domain access lists you defined previously.

### Before you begin

Complete the steps in [Configure TLS Proxy Instances, on page 73](#)

### Procedure

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Associate each of your access lists with the TLS proxy instance that the class map uses. The TLS proxy you select depends on whether the class-map is for messages from the IM and Presence Service to an external domain, or from an external domain to the IM and Presence Service.

In the example below, the access list for messages sent from the IM and Presence Service to an external domain is associated with the TLS proxy instance for TLS connections initiated by the IM and Presence Service called "ent\_imp\_to\_external":

```
class-map ent_imp_to_external match access-list ent_imp_to_external
```

In the example below, the access list for messages sent from an external domain to the IM and Presence Service is associated with the TLS proxy instance for TLS connections initiated by the external server called "ent\_external\_to\_imp":

```
class-map ent_external_to_imp match access-list ent_external_to_imp
```

**Step 3** If you have an intercluster IM and Presence Service deployment, configure a class map for each IM and Presence Service node, and associate this with the appropriate access-list for the server that you defined previously, for example:

```
class-map ent_second_imp_to_external match access-list ent_second_imp_to_external
```

```
class-map ent_external_to_second_imp match access-list ent_external_to_second_imp
```

### What to do next

[Enable TLS Proxy, on page 75](#)

## Enable TLS Proxy

Using the policy map command, you need to enable the TLS proxy for each class map you created in the previous section.



**Note** You cannot use a High security sip-inspect policy map on Cisco Adaptive Security Appliance for a federated deployment because the configuration fails. You must use a Low/Medium security policy map.

**Before you begin**

Complete the steps in [Associate Access List with TLS Proxy Instance Using Class Maps](#), on page 74

**Procedure**


---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Define the sip-inspect policy map, for example:

```
policy-map type inspect sip sip_inspectParameters
```

**Step 3** Define the global policy map, for example:

```
policy-map global_policy class ent_cup_to_external inspect sip sip_inspect tls-proxy
ent_cup_to_external
```

---

## Configure Cisco Adaptive Security Appliance for an Intercluster Deployment

For an intercluster IM and Presence Service deployment, you must perform the following configuration on the Cisco Adaptive Security Appliance for each additional IM and Presence Service node.

**Procedure**


---

**Step 1** Create an additional access list for the IM and Presence Service node.

**Step 2** Generate and import the Cisco Adaptive Security Appliance security certificate onto the IM and Presence Service node.

**Step 3** Generate and import the IM and Presence Service security certificate onto Cisco Adaptive Security Appliance.

**Step 4** Configure a class map for each external domain.

**Step 5** Include the class maps in the global policy map.

---

**Related Topics**

[Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance](#), on page 45

[Associate Access List with TLS Proxy Instance Using Class Maps](#), on page 74

[Enable TLS Proxy](#), on page 75

[Intercluster and Multinode Deployments](#), on page 3



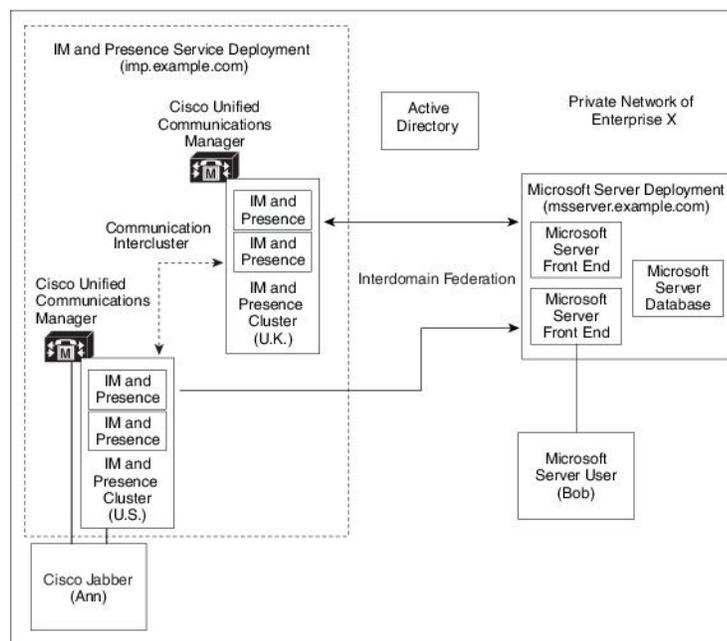
## CHAPTER 8

# Interdomain Federation to Microsoft Lync

- [Interdomain Federation to Microsoft Lync within an Enterprise, on page 77](#)
- [Configuration Task Flow for Microsoft Lync Federation, on page 78](#)

## Interdomain Federation to Microsoft Lync within an Enterprise

Figure 20: Interdomain Federation to Microsoft Server within an Enterprise



When the Microsoft server and IM and Presence Service domains are different, you can configure federation within the enterprise. You do not have to use subdomains; separate domains are equally applicable. See topics related to federation and subdomains for more information.

# Configuration Task Flow for Microsoft Lync Federation

Complete the following tasks to set up federation between IM and Presence Service and Microsoft Lync. This configuration supports both chat-only deployments and chat+calling deployments.



**Note** Interdomain federation via Expressway Gateway's SIP Broker is supported for single enterprise networks only (intracompany). For Business to Business, you must use the ASA.

## Procedure

|               | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <a href="#">Add a Microsoft Lync Domain Within Enterprise, on page 79</a>                                                                                                                                                                                                                                                  | In the IM and Presence Service, add a federated domain entry for the Microsoft Lync domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry.                                                                                                         |
| <b>Step 2</b> | <a href="#">Configure Static Routes from IM and Presence to Lync, on page 79</a>                                                                                                                                                                                                                                           | In the IM and Presence Service, configure an individual TLS static route for each Microsoft Lync server domain. Each route should point to a specific Microsoft front end server.<br><br><b>Note</b> You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync. |
| <b>Step 3</b> | <a href="#">Configure Expressway Gateway for Microsoft Lync Federation, on page 80</a>                                                                                                                                                                                                                                     | <b>Optional.</b> For chat+calling deployments only, add an Expressway Gateway. On the gateway, configure Microsoft interoperability and the SIP broker.<br><br><b>Note</b> For chat-only deployments, you do not need the Expressway Gateway.                                                       |
| <b>Step 4</b> | On the Lync server, configure TLS static routes using one of the following procedures: <ul style="list-style-type: none"> <li>• <a href="#">Configure Static Route from Lync to Expressway Gateway, on page 80</a></li> <li>• <a href="#">Configure a Static Route from Lync to IM and Presence, on page 82</a></li> </ul> | If you have a chat+calling deployment, configure the TLS static route to the Expressway Gateway.<br><br>If you have a chat-only deployment, configure the TLS static route to the IM and Presence Service routing node.                                                                             |
| <b>Step 5</b> | <a href="#">Configure Trusted Applications on Lync Server, on page 84</a>                                                                                                                                                                                                                                                  | On the Lync server, add the IM and Presence Service as a trusted application and add each IM and Presence cluster node to a trusted application server pool.                                                                                                                                        |
| <b>Step 6</b> | <a href="#">Publish Topology, on page 86</a>                                                                                                                                                                                                                                                                               | On the Lync server, commit the topology.                                                                                                                                                                                                                                                            |

|               | Command or Action                                                                           | Purpose                                                                                                                                                                    |
|---------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b> | <a href="#">Set up Certificates on IM and Presence for Federation with Lync, on page 86</a> | In the IM and Presence Service, upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. Also, set up TLS Peer subjects. |

## Add a Microsoft Lync Domain Within Enterprise

When you configure a federated domain entry for a Lync server, the IM and Presence Service automatically adds the incoming ACL for the federated domain entry. You can see the incoming ACL associated with a federated domain on IM and Presence Administration, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) federated domain entry.

### Procedure

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > SIP Federation**.
  - Step 2** Click **Add New**.
  - Step 3** Enter the federated domain name in the Domain Name field.
  - Step 4** Enter a description that identifies the federated domain in the Description field.
  - Step 5** Choose **Inter-domain to OCS/Lync**.
  - Step 6** Check the **Direct Federation** check box.
  - Step 7** Click **Save**.
  - Step 8** After you add, edit, or delete a SIP federated domain, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Service Serviceability** user interface. Choose **Tools > Control Center - Network Services**. When you restart the Cisco XCP Router, it causes a restart of all XCP services on the IM and Presence Service.

**Note** A restart of the Cisco XCP Router is required on all IM and Presence Service nodes within the cluster.

### What to do next

[Configure Static Routes from IM and Presence to Lync, on page 79](#)

## Configure Static Routes from IM and Presence to Lync

Use this procedure to configure TLS static routes on the IM and Presence Service that point to the Microsoft Lync server domain. You must add an individual static route for each Microsoft server domain. Each static route that you set up should point to a specific Microsoft Lync Enterprise Edition front-end server or Standard Edition server.

For high availability purposes, you can configure additional backup static routes to each Microsoft server domain. The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

### Procedure

- 
- Step 1** From Cisco Unified CM IM and Presence Administration, 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 `domaina.com`, enter `.com.domaina.*`.
  - Step 4** In the **Next Hop** field, enter the Microsoft Lync server IP address or FQDN.
  - Step 5** In the **Next Hop Port** field enter **5061**.
  - Step 6** From the **Route Type** drop-down list, choose **Domain**.
  - Step 7** From the **Protocol Type** drop-down list box, select **TLS**.
  - Step 8** Click **Save**.
- 

### What to do next

For chat+calling deployments, [Configure Expressway Gateway for Microsoft Lync Federation, on page 80](#)  
 For chat-only deployments, [Configure a Static Route from Lync to IM and Presence, on page 82](#)

## Configure Expressway Gateway for Microsoft Lync Federation

Chat + calling deployments only. On the Expressway Gateway, configure Microsoft interoperability and enable the SIP broker. For Expressway Gateway configuration, see the *Cisco Expressway and Microsoft Lync Deployment Guide* at:

<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>.




---

**Note** For chat-only deployments, you do not need to deploy the Expressway Gateway.

---

### What to do next

[Configure Static Route from Lync to Expressway Gateway, on page 80](#)

## Configure Static Route from Lync to Expressway Gateway

For chat + calling deployments only. On the Lync servers, configure TLS static routes that point to the Expressway Gateway fully qualified domain name (FQDN).



**Note** Make sure that the FQDN in the static route is resolvable from the Lync front-end server and that it resolves to the correct IP address for the Expressway Gateway.

### 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**.

**Tip** Navigate to either Microsoft Lync Server 2010 or 2013, depending on your Microsoft Lync Server version.

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

```
$tlsRoute = New-CsStaticRoute -TLSSRoute -Destination expresswayGateway_fqdn -Port
expresswayGateway_TLS_listening_port -usedefaultcertificate $true -MatchUri
expresswayGateway_domain
```

where:

| Parameter    | Description                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------|
| -Destination | The fully qualified domain name (FQDN) of the Expressway Gateway. For example, expGateway.sip.com |
| -Port        | The TLS listening port on Expressway Gateway. The default listening port is 65072.                |
| -MatchUri    | The domain for the Expressway Gateway. For example, sip.com.                                      |

#### Example:

```
$tlsRoute = New-CsStaticRoute -TLSSRoute -Destination expGateway.sip.com -Port 65072
-usedefaultcertificate $true -MatchUri sip.com
```

- 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 are using IPv6 with a Microsoft Lync server 2013, the \* wildcard option is not supported in the **-MatchUri** parameter.
  - 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}
```

**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 Expressway Gateway domain) and the FQDN of the Expressway Gateway.
- b) In the new Public Provider, configure the Verification level of your users to Allow all communications with this provider.

### What to do next

[Configure Trusted Applications on Lync Server, on page 84](#)

## Configure a Static Route from Lync to IM and Presence

If you have a chat-only deployment, on the Lync server, configure a TLS static route to the IM and Presence Service routing node. 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.

However, a static route is required for each IM and Presence Service domain.

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

**Table 16: Sample Parameters for TLS Static Route on Microsoft Lync**

| Description                                                                                                                                                                                                                                                                                                                                                                                                             | Sample Parameters      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| IM and Presence Service node FQDN (routing IM and Presence Service node)<br>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             |
| IM and Presence Service node TLS port<br><br>The TLS port value must match what is configured in the user interface. To check the value, log in to the <b>Cisco Unified CM IM and Presence Administration</b> user interface and choose <b>System &gt; Application Listeners &gt; Default Cisco SIP Proxy TLS Listener - Peer Auth</b> .<br><br><b>Note</b> 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**.

**Tip** Navigate to either Microsoft Lync Server 2010 or 2013, depending on your Microsoft Lync Server version.

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

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

**Example:**

```
$tlsRoute = New-CsStaticRoute -TLSSRoute -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 are using IPv6 with a Microsoft Lync server 2013, the `*` wildcard option is not supported in the `-MatchUri` parameter.
  - 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:

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

---

### What to do next

[Configure Trusted Applications on Lync Server, on page 84](#)

## Configure Trusted Applications on Lync Server

On the Lync server, add the IM and Presence Service as a trusted application and add each IM and Presence cluster node to a trusted application server pool. This procedure applies for both Enterprise Edition and Standard Edition Lync deployments.

### 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: <code>trustedpool.sip.com</code> .<br><b>Tip</b> 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: <code>lyncserver.synergy.com</code> .<br>You can check this value using the command <b>Get-CsPool</b> .                                                                                                                  |
| -Site         | The numeric value of the site where you want to create the trusted application pool.<br><b>Tip</b> Use the <b>Get-CsSite</b> Management Shell command.                                                                                                                                              |
| -Computerfqdn | The FQDN of the IM and Presence Service routing node. For example: <code>impserverPub.sip.com</code> . <ul style="list-style-type: none"> <li>• <code>impserverPub</code> = the IM and Presence Service hostname.</li> <li>• <code>sip.com</code> = the IM and Presence Service domain.</li> </ul>  |

**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: <code>impserver2.sip.com</code> .<br><b>Note</b> Do not add the IM and Presence Service routing node as a trusted application computer using this command. |
| -Pool     | The FQDN of the trusted application pool that is used for the IM and Presence Service deployment. For example: <code>trustedpool.sip.com</code> .                                                                     |

**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: <i>imptrustedapp.sip.com</i> .                                       |
| -TrustedApplicationPoolFqdn | The FQDN of the trusted application pool server for the IM and Presence Service deployment. For example: <i>trustedpool.sip.com</i> . |
| -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 86](#)

## Publish Topology

**Procedure**

- Step 1** Log in to the Lync Server Management Shell.
- Step 2** Enter the **Enable-CsTopology** command to enable the topology.

**What to do next**

[Set up Certificates on IM and Presence for Federation with Lync, on page 86](#)

## Set up Certificates on IM and Presence for Federation with Lync

Use this procedure to set up certificates on your IM and Presence Service nodes for Federation with Microsoft Lync.

**Procedure**

- Step 1** On the IM and Presence Service, upload the root certificate for the CA that signs the Microsoft server certificate.

- Upload the certificate as a cup-trust certificate.
- Leave the **Root Certificate** field blank.
- Import the self-signed certificate onto the IM and Presence Service.

**Step 2** Generate a CSR for the IM and Presence Service so that the certificate can be signed by a CA. Upload the CSR to the CA that signs your certificate.

- Important**
- The CA must sign the certificate so that it has "Enhanced Key Usage" with both "Server Authentication" and "Client Authentication".
  - If this is Microsoft Windows Server CA, it must use a certificate template that has "Server Authentication" and "Client Authentication".

**Step 3** When you have retrieved the CA-signed certificate and the CA root certificate, upload the CA-signed certificate and the root certificate to the IM and Presence Service node.

- Upload the root certificate as a cup-trust certificate.
- Upload the CA-signed cup certificate. Specify the root certificate .pem file as the root certificate.

**Step 4** Add a TLS Peer subject on IM and Presence Service for the Microsoft server. Use the FQDN of the Microsoft server.

**Step 5** Add the TLS Peer to the Selected TLS Peer Subjects list.

- Make sure that the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher is chosen for the TLS Context Configuration.
- Make sure that you disable empty TLS fragments.

---

### What to do next

Set up certificates on the Microsoft Lync server that have "Enhanced Key Usage" with "Server Authentication" and "Client Authentication" values. For details, see:

- [Request Certificate from CA Server, on page 54](#)
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at [http://technet.microsoft.com/en-us/library/cc731256\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx).





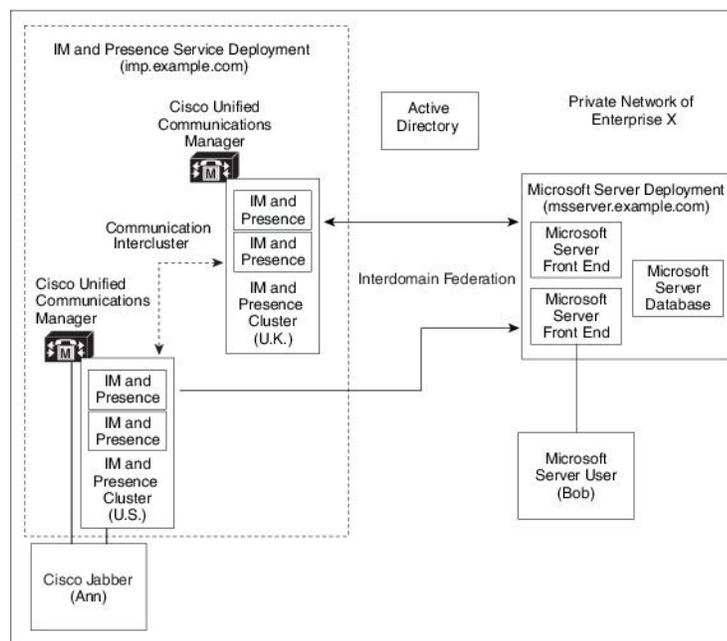
## CHAPTER 9

# Interdomain Federation to Microsoft OCS

- [Interdomain Federation to Microsoft OCS within an Enterprise, on page 89](#)
- [Configuration Task Flow for Microsoft OCS Federation, on page 89](#)

## Interdomain Federation to Microsoft OCS within an Enterprise

Figure 21: Interdomain Federation to Microsoft Server within an Enterprise



When the Microsoft server and IM and Presence Service domains are different, you can configure federation within the enterprise. You do not have to use subdomains; separate domains are equally applicable. See topics related to federation and subdomains for more information.

## Configuration Task Flow for Microsoft OCS Federation

Complete the following tasks to set up federated links between IM and Presence Service and Microsoft OCS.

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 for each domain on the OCS server. These static routes point to an IM and Presence Service node. The Cisco Adaptive Security Appliance or the Microsoft Access Edge are not required.

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

### Procedure

|               | Command or Action                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <a href="#">Add a Microsoft OCS Domain Within Enterprise, on page 91</a>                                  | In the IM and Presence Service, add a federated domain entry for the Microsoft OCS domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry.                                                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | <a href="#">Configure Static Route on IM and Presence Service for Microsoft Servers, on page 92</a>       | In the IM and Presence Service, configure an individual static route for each Microsoft OCS server domain. Each route should point to a specific Microsoft front end server.<br><br><b>Note</b> For OCS, you can choose either TCP or TLS as the protocol type.                                                                                                                                                                                                                               |
| <b>Step 3</b> | <a href="#">Configure Static Routes on OCS to Point to the IM and Presence Service, on page 93</a>        | On the OCS server, configure TCP or TLS static routes that point to the IM and Presence Service domain. Each route must point to a specific IM and Presence Service node.                                                                                                                                                                                                                                                                                                                     |
| <b>Step 4</b> | <a href="#">Verify Peer Authentication Listener, on page 94</a>                                           | Verify that on the IM and Presence Service the Peer Auth Listener is configured as port 5061 and the Server Auth Listener is not port 5061.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 5</b> | <a href="#">Adding a Host Authorization Entry for the IM and Presence Service Node on OCS, on page 94</a> | On the OCS server, configure host authorization entries for each IM and Presence Service node. With TLS encryption, you must add two entries for each IM and Presence node: <ul style="list-style-type: none"> <li>• one entry with the IM and Presence node IP address</li> <li>• one entry with the IM and Presence node FQDN</li> </ul> <p>If you are not using TLS encryption, configure one host authorization entry for each IM and Presence Service node with the node IP address.</p> |
| <b>Step 6</b> | <a href="#">Configure Certificates on OCS for Interdomain Federation, on page 95</a>                      | If you have TLS configured between OCS to IM and Presence Service, configure certificates                                                                                                                                                                                                                                                                                                                                                                                                     |

|               | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                 |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                    | on OCS for interdomain federation with IM and Presence Service.<br><b>Note</b> If you are not using TLS, you can skip this step.                                                                                                                                                                        |
| <b>Step 7</b> | <a href="#">Enable Port 5060/5061 on the OCS Server, on page 95</a>                                                                | On the OCS server, confirm the listener ports for TLS (The transport can be MTLS or TLS) or TCP are configured. .<br><br><ul style="list-style-type: none"> <li>• For TLS static routes to the OCS server, use port 5061.</li> <li>• For TCP static routes to the OCS server, use port 5060.</li> </ul> |
| <b>Step 8</b> | <a href="#">Configure OCS to use FIPS, on page 96</a>                                                                              | If you are using TLS, configure OCS to use FIPS.                                                                                                                                                                                                                                                        |
| <b>Step 9</b> | <a href="#">Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS , on page 97</a> | If you are using TLS, upload the root certificate for the CA that signs the OCS server certificates to IM and Presence Service.                                                                                                                                                                         |

## Add a Microsoft OCS Domain Within Enterprise

When you configure a federated domain entry for an OCS server, the IM and Presence Service automatically adds the incoming ACL for the federated domain entry. You can see the incoming ACL associated with a federated domain on IM and Presence Administration, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) federated domain entry.

### Procedure

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > SIP Federation**.
  - Step 2** Click **Add New**.
  - Step 3** Enter the federated domain name in the Domain Name field.
  - Step 4** Enter a description that identifies the federated domain in the Description field.
  - Step 5** Choose **Inter-domain to OCS/Lync**.
  - Step 6** Check the **Direct Federation** check box.
  - Step 7** Click **Save**.
  - Step 8** After you add, edit, or delete a SIP federated domain, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Service Serviceability** user interface. Choose **Tools > Control Center - Network Services**. When you restart the Cisco XCP Router, it causes a restart of all XCP services on the IM and Presence Service.

**Note** A restart of the Cisco XCP Router is required on all IM and Presence Service nodes within the cluster.

---

### What to do next

[Configure Static Route on IM and Presence Service for Microsoft Servers, on page 92](#)

## Configure Static Route on IM and Presence Service for Microsoft Servers

To configure the IM and Presence Service to use TLS when exchanging IM and availability with a federated Microsoft server domain, or to use TCP for an OCS domain, you must configure a static route on IM and Presence Service that points to the Microsoft server and not the external edge of Microsoft Access Edge.

You must add an individual static route for each Microsoft server domain. The Microsoft server domain static route should point to the IP address of a specific Microsoft server Enterprise Edition front-end server or Standard Edition server.

For high availability purposes, you can configure additional backup static routes to each Microsoft server domain. The backup route has a lower priority and is used only if the next hop address of the primary static route is unreachable.

### 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, or FQDN, is reversed. For example:
- If the domain is `domaina.com`, enter `.com.domaina.*` as the Destination Pattern value.
- Step 4** Enter the remaining parameters as follows:
- a) Enter the Next Hop, the value is the Microsoft server IP address or FQDN.
  - b) Choose the Next Hop Port number and Protocol Type value.
    - For TCP — from the drop-down list, choose **TCP** as the Protocol Type and **5060** as the Next Hop Port number.
    - For TLS — from the drop-down list, choose **TLS** as the Protocol Type and **5061** as the Next Hop Port number.

**Note** Microsoft OCS servers support federation over TCP or TLS.
  - c) From the Route Type drop-down list, choose Domain.
- Step 5** Click **Save**.
-

**What to do next**

[Configure Static Routes on OCS to Point to the IM and Presence Service, on page 93](#)

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

To allow OCS to route requests to IM and Presence Service for direct federation, you must configure a TLS or TCP static route on the OCS server for each IM and Presence Service domain. These static routes are to point 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**

See Verify Peer Authentication Listener in the Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager guide.

## Verify Peer Authentication Listener

Verify that the peer authentication listener is configured correctly on the IM and Presence Service.

### Procedure

- 
- Step 1** From Cisco Unified CM IM and Presence Administration, choose **System > Application Listener**.
- Step 2** Click **Find**.  
The list of configured application listener ports displays. The default peer auth listener port and server auth listener ports also display.
- Step 3** Confirm that the **Default Cisco SIP Proxy TLS Listener - Peer Auth** port is 5061.
- Step 4** Confirm that the **Default Cisco SIP Proxy TLS Listener - Server Auth** port is not 5061. If this port is configured as 5061, you must change it to another value. For example, 5063.
- 

### What to do next

[Adding a Host Authorization Entry for the IM and Presence Service Node on OCS, on page 94](#)

## Adding a Host Authorization Entry for the IM and Presence Service Node on OCS

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

If you are configuring TLS encryption between OCS 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, 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 perform this procedure on all Standard Edition servers.
  - For Enterprise Edition, you must perform this procedure on all pools.
- 

### Procedure

- 
- Step 1** Choose the **Host Authorization** tab on OCS.
- Step 2** Perform one of the following steps:

- a) Enter the IP address of the authorized host if you configured a static route on OCS that specifies the next hop computer by its IP address.
- b) Enter the FQDN of the authorized host if you configured a static route on OCS that specifies the next hop computer by its FQDN.

- Step 3** Click **Add**.
- Step 4** Choose **IP**.
- Step 5** Enter the IP address of the IM and Presence Service node.
- Step 6** Check the **Throttle as Server** check box.
- Step 7** Check the **Treat as Authenticated** check box.

**Note** Do not check the **Outbound Only** check box.

- Step 8** Click **OK**.

---

#### What to do next

[Configure Certificates on OCS for Interdomain Federation, on page 95](#)

## Configure Certificates on OCS for Interdomain Federation

If you have TLS configured between OCS to IM and Presence Service, configure certificates on OCS for interdomain federation with IM and Presence Service.



---

**Note** If you aren't using TLS, you can skip this procedure.

---

#### Procedure

---

- Step 1** Retrieve the CA root certificate and the OCS signed certificate by completing the following steps:
- a) Download and install the CA certificate chain.
  - b) Request a certificate from the CA server.
  - c) Download the certificate from the CA server.
- Step 2** From the OCS Front End Server Properties, choose the **Certificates** tab, and click **Select Certificate** to choose the OCS signed certificate.
- 

#### What to do next

[Enable Port 5060/5061 on the OCS Server, on page 95](#)

## Enable Port 5060/5061 on the OCS Server

For TCP static routes to the OCS server, use port 5060.

For TLS static routes to the OCS server, use port 5061.

### Procedure

---

- Step 1** Choose **Start > Programs > Administrative Tools > Microsoft Office Communicator Server 2007** on OCS.
- Step 2** Right-click on the FQDN of Front End server.
- Step 3** Choose **Properties > Front End Properties** and choose the **General** tab.
- Step 4** If port 5060 or 5061 is not listed under Connections, click **Add**.
- Step 5** Configure port value as follows:
- a) Choose **All** as the IP Address Value.
  - b) Choose the Port Value.
    - For TCP, choose **5060** as the Port Value.
    - For TLS, choose **5061** as the Port Value.
  - c) Choose the Transport value.
    - For TCP, choose **TCP** as the Transport Value.
    - For TLS, choose **TLS** as the Transport Value.
- Step 6** Click **OK**.
- 

### What to do next

[Configure OCS to use FIPS, on page 96](#)

## Configure OCS to use FIPS

Configure FIPS on the OCS server. Complete this procedure only if you are using TLS only (TLSv1 rather than SSLv3).

### Procedure

---

- Step 1** Open the **Local Security Settings** on OCS.
- Step 2** In 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**.

**Note** You may need to restart OCS for this to take effect.

- Step 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.
- 

#### What to do next

[Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS](#), on page 97

## Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS

This procedure applies only if you have set up TLS static routes between IM and Presence Service and Microsoft servers.

#### Procedure

---

- Step 1** On the IM and Presence Service, upload the root certificate for the CA that signs the Microsoft server certificate.
- Upload the certificate as a cup-trust certificate.
  - Leave the **Root Certificate** field blank.
  - Import the self-signed certificate onto the IM and Presence Service.
- Step 2** Generate a CSR for the IM and Presence Service so that the certificate can be signed by a CA. Upload the CSR to the CA that signs your certificate.
- Important**
- The CA must sign the certificate so that it has "Enhanced Key Usage" with both "Server Authentication" and "Client Authentication".
  - If this is Microsoft Windows Server CA, it must use a certificate template that has "Server Authentication" and "Client Authentication".
- Step 3** When you have retrieved the CA-signed certificate and the CA root certificate, upload the CA-signed certificate and the root certificate to the IM and Presence Service node.
- Upload the root certificate as a cup-trust certificate.
  - Upload the CA-signed cup certificate. Specify the root certificate .pem file as the root certificate.
- Step 4** Add a TLS Peer subject on IM and Presence Service for the Microsoft server. Use the FQDN of the Microsoft server.
- Step 5** Add the TLS Peer to the Selected TLS Peer Subjects list.
- Make sure that the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher is chosen for the TLS Context Configuration.

- Make sure that you disable empty TLS fragments.
- 

### What to do next

Set up certificates on the Microsoft Lync server that have "Enhanced Key Usage" with "Server Authentication" and "Client Authentication" values. See:

- [Request Certificate from CA Server, on page 54](#)
- Microsoft TechNet Library, Windows Server — Implementing and Administering Certificate Templates at [http://technet.microsoft.com/en-us/library/cc731256\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731256(v=ws.10).aspx)



# CHAPTER 10

## External Server Component Configuration for SIP Federation

- [Microsoft Component Configuration for SIP Federation, on page 99](#)

### Microsoft Component Configuration for SIP Federation

The following tables provide a brief checklist to configure federation on the Microsoft OCS and Access Edge servers. For detailed instructions on setting up and deploying the OCS server and the Access Edge server, refer to the Microsoft documentation.

**Table 17: Configuration Tasks for Microsoft Components - OCS Server**

| Task                                     | Procedure                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Global Federation Setting         | <ol style="list-style-type: none"> <li>1. In the global forest branch in the left pane, choose <b>Properties &gt; Global Properties &gt; Federation</b>.</li> <li>2. Check the <b>Enable Federation and Public IM Connectivity</b> check box.</li> <li>3. Enter the FQDN and the port number for the internal interface of the Access Edge server.</li> </ol> |
| Configure the Access Edge server address | <ol style="list-style-type: none"> <li>1. In the global forest branch in the left pane, choose <b>Properties &gt; Global Properties &gt; Edge Servers</b>.</li> <li>2. In the <b>Access Edge and Web Conferencing Edge Servers</b> window, click <b>Add</b>.</li> <li>3. Enter the FQDN for the internal interface of the Access Edge server.</li> </ol>      |
| Enable Each Front End Federation Setting | <p>You need to enable the federation setting for each front-end server that is federating:</p> <ol style="list-style-type: none"> <li>1. In the front-end server branch in the left pane, choose <b>Properties &gt; Front End Properties &gt; Federation</b>.</li> <li>2. Check the <b>Enable Federation and Public IM Connectivity</b> check box.</li> </ol> |

| Task                                                    | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Check your users are enabled for MOC and for Federation | <ul style="list-style-type: none"> <li>• Choose the <b>Users</b> tab and check that your users are enabled for MOC.</li> <li>• If your user is not present in this list, you need to enable the user for MOC in Microsoft Active Directory.</li> <li>• You also need to enable the user for <b>Public IM Connectivity</b> in Microsoft Active Directory.</li> </ul> <p>Refer to the Microsoft Active Directory documentation at the following URL:<br/> <a href="http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx">http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.aspx</a></p> |
| Configure the security certificates                     | <ul style="list-style-type: none"> <li>• You need to configure security certificates between the OCS server and the Access Edge server.</li> <li>• A CA server is required to perform this procedure.</li> <li>• Please refer to the Microsoft documentation for details on configuring security certificates between these servers.</li> </ul>                                                                                                                                                                                                                                                                                                     |

**Table 18: Configuration Tasks for Microsoft Components - Access Edge Server**

| Task          | Procedure                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure DNS | In the Microsoft enterprise deployment, you need to configure an external SRV record for all Access Edge Servers that points to <code>_sipfederationtls._tcp.domain</code> , over port 5061, where <i>domain</i> is the name of the SIP domain of your organization. This SRV should point to the external FQDN of the Access Edge server. |

| Task                                                | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure IM and Presence Service as an IM Provider | <ol style="list-style-type: none"> <li>1. On the external Access Edge server, choose <b>Start &gt; Administrative Tools &gt; Computer Management</b>.</li> <li>2. In the left pane, right-click <b>Microsoft Office Communications Server 2007</b>.</li> <li>3. Choose the <b>IM Provider</b> tab.</li> <li>4. Click <b>Add</b>.</li> <li>5. Check the <b>Allow the IM service provider</b> check box.</li> <li>6. Define the IM service provider name, for example, the IM and Presence node.</li> <li>7. Define the network address of the IM service provider, in this case the public FQDN of the IM and Presence Service node.</li> <li>8. Ensure that the IM service provider is not marked as “public”.</li> <li>9. Click the filtering option <b>Allow all communications from this provider</b> option.</li> <li>10. Click <b>OK</b>.</li> </ol> <p>In the IM and Presence Service enterprise deployment, you need to configure a DNS SRV record for each IM and Presence Service domain. The DNS SRV record should point to <code>_sipfederationtls._tcp.IM and Presence_domain</code> over port 5061, where <i>IM and Presence_domain</i> is the name of the IM and Presence Service domain. This DNS SRV should point to the public FQDN of the IM and Presence Service node.</p> |
| Check the Access Method Settings                    | <ol style="list-style-type: none"> <li>1. In the console tree, right-click on Microsoft Office Communications Server 2007.</li> <li>2. Choose <b>Properties &gt; Access Methods</b>.</li> <li>3. Check the <b>Federation</b> check box.</li> <li>4. Check the <b>Allow discovery</b> check box if you are using DNS SRV.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Task                                | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure Access Edge to use TLSv1  | <ol style="list-style-type: none"> <li>1. To open the Local Security Policy, choose <b>Start &gt; Administrative Tools &gt; Local Security Policy</b>.           <p><b>Note</b> If you are configuring this on a domain controller, the path is <b>Start &gt; Administrative Tools &gt; Domain Controller Security Policy</b>.</p> </li> <li>2. In the console tree, choose <b>Security Settings &gt; Local Policies &gt; Security Options</b>.</li> <li>3. Double-click the FIPS security setting in the details pane.</li> <li>4. Enable the FIPS security setting.</li> <li>5. Click <b>OK</b>.           <p><b>Note</b> There is a known issue with remote desktop to the Access Edge server with FIPS enabled on Windows XP. Refer to <a href="#">Unable to Remote Desktop to Access Edge, on page 151</a> for a resolution to this issue.</p> </li> </ol> |
| Configure the security certificates | <ul style="list-style-type: none"> <li>• You need to configure security certificates between the OCS server and the Access Edge server.</li> <li>• A CA server is required to perform this procedure.</li> <li>• Please refer to the Microsoft documentation for details on configuring security certificates between these servers.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Related Topics**

[Interdomain Federation to Microsoft OCS/Lync Configuration within Enterprise](#)



## CHAPTER 11

# Load Balancer Configuration for Redundancy for SIP Federation

---

- [About the Load Balancer, on page 103](#)
- [IM and Presence Service Node Updates, on page 103](#)
- [Cisco Adaptive Security Appliance Updates, on page 104](#)
- [CA-Signed Security Certificate Updates, on page 109](#)
- [Microsoft Component Updates, on page 110](#)

## About the Load Balancer

For redundancy and high availability purposes, you can incorporate a load balancer into the federated network. The load balancer is placed between the IM and Presence Service node and the Cisco Adaptive Security Appliance (see [High Availability for SIP Federation, on page 4](#)).

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

## IM and Presence Service Node Updates

When using a load balancer for redundancy, you must update settings on the IM and Presence Service publisher and subscriber nodes.

### Procedure

| Task                                           | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Update the federation routing parameter        | <p>Log in to <b>Cisco Unified IM and Presence Administration</b>, choose <b>System &gt; Service Parameters &gt; Cisco SIP Proxy</b> from the Service menu and enter these values:</p> <ul style="list-style-type: none"> <li>• <b>Virtual IP Address</b> - enter the virtual IP address set on the load balancer</li> </ul> <ol style="list-style-type: none"> <li>1. <b>Server Name</b> - set to the FQDN of the load balancer</li> <li>2. <b>Federation Routing IM and Presence FQDN</b> - set to the FQDN of the load balancer.</li> </ol> |
| Create a new TLS peer subject                  | <ol style="list-style-type: none"> <li>1. Log in to <b>Cisco Unified IM and Presence Administration</b>, choose <b>System &gt; Security &gt; TLS Peer Subjects</b>.</li> <li>2. Click <b>Add New</b> and enter these values: <ul style="list-style-type: none"> <li>• <b>Peer Subject Name</b> - enter the external FQDN of the load balancer</li> <li>• <b>Description</b> - enter the name of the load balancer</li> </ul> </li> </ol>                                                                                                      |
| Add the TLS peer to the TLS peer subjects list | <ol style="list-style-type: none"> <li>1. Log in to <b>Cisco Unified IM and Presence Administration</b>, choose <b>System &gt; Security &gt; TLS Context Configuration</b>.</li> <li>2. Click <b>Find</b>.</li> <li>3. Click <b>Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context</b></li> <li>4. Move the load balancer federation-TLS peer subject for the load balancer to the TLS peer subjects list.</li> </ol>                                                                                                                          |

**Related Topics**

[Configure Federation Routing Parameters](#), on page 40

[Create a New TLS Peer Subject](#), on page 41

[Add TLS Peer to Selected TLS Peer Subjects List](#), on page 42

## Cisco Adaptive Security Appliance Updates

When using a load balancer, the external domain still sends messages to the public IM and Presence Service address, but the Cisco Adaptive Security Appliance maps that address to a virtual IP address on the load balancer. Thus, when the Cisco Adaptive Security Appliance receives messages from the external domain, it

forwards it to the load balancer. The load balancer then passes it on to the appropriate IM and Presence Service nodes.

To support this configuration, you must make some changes to the Cisco Adaptive Security Appliance:

## Static PAT Message Updates

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

Procedure

| Task                                                                                                   | Cisco Adaptive Security Appliance Release 8.2 Command                                                                                                                                                                                                                                             | Cisco Adaptive Security Appliance Release 8.3 Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Changes Required for the IM and Presence Service Publisher                                             |                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Change the static PAT to use an arbitrary, unused port for the public IM and Presence Service address. | <p>Change:</p> <pre>static (inside,outside) tcp public_imp_ip_address 5061 routing_imp_private_ip_address 5062 netmask 255.255.255.255</pre> <p>to:</p> <pre>static (inside,outside) tcp public_imp_ip_address 55061 routing_imp_publisher_ private_ip_address 5062 netmask 255.255.255.255</pre> | <p>Change:</p> <pre>object service obj_tcp_source_eq_5061 # service tcp source eq 5061</pre> <pre>nat (inside,outside) source static obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061</pre> <p>to</p> <pre>object service obj_tcp_source_eq_55061 # service tcp source eq 55061</pre> <pre>nat (inside,outside) source static obj_host_routing_imp_private_ip_address obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_55061</pre> |

| Task                                                                                                                                                                                                                                                                                      | Cisco Adaptive Security Appliance Release 8.2 Command                                                                                                                                                                                                                                 | Cisco Adaptive Security Appliance Release 8.3 Command                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add a new static PAT to allow messages sent to the public IM and Presence Service address to be forwarded to the virtual port address (on whichever port the load balancer is listening for TLS messages).                                                                                | <pre>static (inside,outside) tcp public_imp_address 5061 load_balancer_vip 5062 netmask 255.255.255.255</pre>                                                                                                                                                                         | <pre>object network obj_host_load_balancer_vip # host routing_imp_private_address  object service obj_tcp_source_eq_5061 # service tcp source eq 5061  nat (inside,outside) source static obj_host_load_balancer_vip obj_host_public_imp_ip_address service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061</pre> |
| Changes Required for IM and Presence Service Subscriber                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                 |
| Add a new access list for the load balancer virtual IP address. You must add an access list for each external domain that IM and Presence Service needs to access.                                                                                                                        | <pre>access-list ent_lber_to_external_ocs extended permit tcp host subscriber_private_ip_address host external_domain_public_ip_address 5061  access-list ent_lcs_to_lber_routg_imp extended permit tcp host external_domain_public_ip_address host imp_public_ip_address 65061</pre> |                                                                                                                                                                                                                                                                                                                 |
| Add a new access list for a <b>extended permit tcp</b> external domain to initiate messages to a IM and Presence Service server when the load balancer virtual IP address is in place. You must add an access list for each external domain that needs to access IM and Presence Service. |                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                 |

**Related Topics**

[Configure Static IP Routes](#), on page 60

[Port Address Translation \(PAT\)](#), on page 61

## Access List Updates

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

**Note**

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

## Procedures

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

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

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

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

#### Related Topics

[Access List Configuration Requirements](#), on page 72

## TLS Proxy Instance Updates

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

#### Procedure

Change:

```
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point imp_proxy

client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1

tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point msoft_public_fqdn

client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1

to:
```

```
tls-proxy ent_external_to_imp server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn

client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1

tls-proxy ent_imp_to_external
server trust-point msoft_public_fqdn
client trust-point msoft_public_fqdn
```

```
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

### Related Topics

[Configure TLS Proxy Instances](#), on page 73

## CA-Signed Security Certificate Updates

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

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

This topic provides an overview of the required steps for configuring the security certificate between the load balancer and the Cisco Adaptive Security Appliance.

| Task                                                                                              | Procedure                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generate CA-signed certificate for the load balancer on the Cisco Adaptive Security Appliance.    | Use the <code>crypto ca enroll</code> command and specify the FQDN of the load balancer.                                                                    |
| Import the CA-signed certificate from the Cisco Adaptive Security Appliance to the load balancer. | Refer to your load balancer documentation.                                                                                                                  |
| Generate a CA-signed certificate for the Cisco Adaptive Security Appliance on the load balancer.  | Refer to your load balancer documentation.                                                                                                                  |
| Import the CA-signed certificate from the load balancer to the Cisco Adaptive Security Appliance  | Use the <code>crypto ca trustpoint</code> command.<br>To verify that the certificate was imported, use the <code>show crypto ca certificate</code> command. |

### Related Topics

[Configure a Certificate on the Cisco Adaptive Security Appliance Using SCEP](#), on page 50

[Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance](#), on page 48

[Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge \(External Interface\) with Microsoft CA](#), on page 49

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

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

| Task                                                                         | Procedure                                                                      |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Generate a CA-signed certificate on both the publisher and subscriber nodes. | Follow the instructions to exchange certificates using CA-signed certificates. |

| Task                                                                                             | Procedure                                  |
|--------------------------------------------------------------------------------------------------|--------------------------------------------|
| Import the CA-signed certificates (from the publisher and subscriber nodes) to the load balancer | Refer to your load balancer documentation. |

## Microsoft Component Updates

You must update some Microsoft components with the load balancer details.

### Procedure

| Task                                                                      | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Update all instances of the FQDN to correspond to the load balancer FQDN. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Update the domain name in the IM Provider list with the load balancer.    | <ol style="list-style-type: none"> <li>1. On the external Access Edge server, choose <b>Start &gt; Administrative Tools &gt; Computer Management</b>.</li> <li>2. In the left pane, right-click <b>Microsoft Office Communications Server 2007</b>.</li> <li>3. Click the <b>IM Provider</b> tab.</li> <li>4. Click <b>Add</b>.</li> <li>5. Check the check box for <b>Allow the IM service provider</b>.</li> </ol> <p>Define the network address of the IM service provider as the public FQDN of the load balancer</p> |

### Related Topics

[External Server Component Configuration for SIP Federation](#), on page 99



## CHAPTER 12

# IM and Presence Service Configuration for XMPP Federation

---

- [External XMPP Federation through Cisco Expressway, on page 111](#)
- [Configure General Settings for XMPP Federation, on page 113](#)
- [DNS Configuration for XMPP Federation, on page 115](#)
- [Policy Settings Configuration for XMPP Federation, on page 121](#)
- [Configure the Cisco Adaptive Security Appliance for XMPP Federation, on page 122](#)
- [Turn On XMPP Federation Service, on page 124](#)

## External XMPP Federation through Cisco Expressway

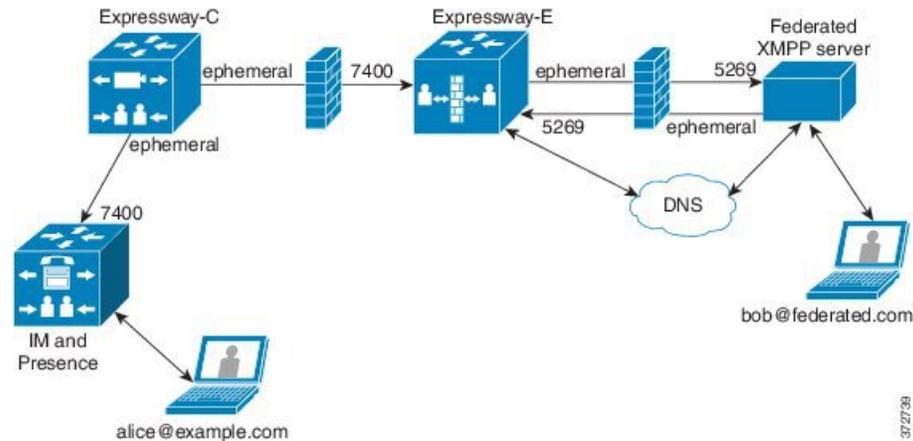
The preferred method for deploying external XMPP federation is through Cisco Expressway. Cisco Expressway enables users registered to IM and Presence Service to communicate via the Expressway-E with users from a different XMPP deployment. The following diagram shows how XMPP messages are routed from an on-premises IM and Presence Service server via the Expressway-C and Expressway-E Collaboration Edge solution to the federated XMPP server. It also shows the ports and connections that are used as the messages traverse DMZ firewalls.



**Note** The Expressway-C and Expressway-E combination is shown here, however the same external XMPP federation functionality is also available when using a VCS Control and VCS Expressway combination. Refer to [Cisco Expressway Administrator Guide \(X8.2\)](#) for more information about the Expressway series option or [Cisco TelePresence Video Communication Server Administrator Guide \(X8.2\)](#) for more information about the VCS option.

---

Figure 22: External XMPP Federation through Cisco Expressway



**Note** SIP and XMPP federations are separate and do not impact each other. For example, it is possible to deploy SIP federation on IM and Presence Service and external XMPP federation on Cisco Expressway.

### Supported Federations

Expressway-E supports XMPP federation with the following enterprises:

- Cisco Unified Communications Manager IM and Presence Service Release 9.1 or later
- Cisco WebEx Connect Release 6.x
- XMPP standards-compliant servers

### Supported Deployment Configurations

The following XMPP federation deployment options are available:

- external XMPP federation only (terminated on Cisco Expressway)
- internal XMPP federation only (terminated on IM and Presence Service)
- internal and external XMPP federation (terminated on IM and Presence Service) but requires you to configure your firewall to allow inbound connections.

For more information about external XMPP federation through Cisco Expressway, see [Cisco Expressway Administrator Guide \(X8.2\)](#)

### Restrictions

- Simultaneous internal XMPP federation terminated on IM and Presence Service and external XMPP federation terminated on Cisco Expressway is not supported.



---

**Important** If you deploy external XMPP federation through Cisco Expressway, do not activate the Cisco XCP XMPP Federation Connection Manager feature service on IM and Presence Service.

---

- Expressway-E does not support XMPP address translation (of email addresses, for example). If you are using Expressway-E for XMPP federation, you must use native presence Jabber IDs from IM and Presence Service.

## Configure General Settings for XMPP Federation

### XMPP Federation Overview

The IM and Presence Service supports XMPP federation with the following enterprises:

- Cisco WebEx Messenger Release 7.x
- IBM Sametime Release 8.2 and 8.5
- IM and Presence Release 9.x or greater

When IM and Presence Service is federating with WebEx Enterprise, it is not possible for WebEx Connect client users to invite IM and Presence Service users to temporary or persistent chat rooms. This is due to a design constraint on the WebEx Connect client.

To allow the IM and Presence Service to federate over XMPP, you must enable and configure XMPP federation on the IM and Presence Service, following the procedures we describe in this chapter.

If you have multiple IM and Presence Service clusters, you must enable and configure XMPP federation on at least one node per cluster. The XMPP federation configuration must be identical across clusters. The **Diagnostics Troubleshooter** compares the XMPP federation configuration across clusters, and reports if the XMPP federation configuration is not identical across cluster.

If you deploy Cisco Adaptive Security Appliance for firewall purposes, note the following:

- See topics related to integration preparation for considerations on routing, scale, public IP addresses and the CA authority.
- See the task to configure the Cisco Adaptive Security Appliance for information on configuring the prerequisite information such as the hostname, timezone, clock, and so on.

### Important Notes about Restarting Services for XMPP Federation

If you make a change to any of the XMPP Federation settings, you must restart the Cisco XCP Router and the Cisco XCP XMPP Federation Connection Manager. To restart the services, log in to the **IM and Presence Serviceability** user interface:

- Cisco XCP Router, choose **Tools > Control Center - Network Services**.
- Cisco XCP XMPP Federation Connection Manager, choose **Tools > Control Center - Feature Services**.

When you restart the Cisco XCP Router service, the IM and Presence Service restarts all the XCP services.

If you enable or disable XMPP federation on a node, you must restart the Cisco XCP Router on all nodes within a cluster, not just on the node where XMPP federation has been enabled or disabled. For all other XMPP federation settings, a Cisco XCP Router restart is only required on the node to which the setting is being changed.

## Turn On XMPP Federation on a Node

This setting is turned off by default.

### Procedure

---

**Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Settings**.

In the XMPP Federation Node Status drop-down list, choose **On**.

**Step 2** Click **Save**.

Troubleshooting Topics

You cannot start the XCP XMPP Federation Connection Manager service on the IM and Presence Service node, unless you turn on XMPP Federation on the node.

---

### What to do next

[Configure Security Settings for XMPP Federation, on page 114](#)

## Configure Security Settings for XMPP Federation

### Before you begin

- Determine whether the external domain that you are federating with supports TLS connections.
- The TLS and SASL specific settings are only configurable if you select the SSL mode “TLS Optional” or “TLS Required”.
- If you are configuring federation between the IM and Presence Service and IBM using TLS, you must configure the SSL mode “TLS Required”, and you must enable SASL.

### Procedure

---

**Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Settings**.

**Step 2** Choose a security mode from the drop-down list:

- a) No TLS - IM and Presence Service does not establish a TLS connection with the external domain. The system uses a non-encrypted connection to federate with the external domain, and uses the server dialback mechanism to verify the identity of the other server.

- b) TLS Optional - IM and Presence Service attempts to establish a TLS connection with the external domain. If the IM and Presence Service fails to establish a TLS connection, it reverts to server dialback to verify the identity of the other server.
- c) TLS Required - The system guarantees a secure (encrypted) connection with the external domain.

**Step 3** Check the **Require client-side security certificates** check box if you want to enforce strict validation of certificates from external domain servers against an installed root CA certificate. This setting turns on, by default, if you select either TLS Optional or TLS Required security settings.

**Note** If you are configuring XMPP federation with WebEx, do not check the **Require client-side security certificates** check box.

**Step 4** Check the **Enable SASL EXTERNAL on all incoming connections** check box to ensure that the IM and Presence Service advertises support for SASL EXTERNAL on incoming connection attempts and implements SASL EXTERNAL validation.

**Step 5** Check the **Enabling SASL on outbound connections** check box to ensure that the IM and Presence Service sends a SASL auth id to the external domain if the external server requests SASL EXTERNAL.

**Step 6** Enter the dialback secret if you want to use DNS to verify the identity of an external server that is attempting to connect to the IM and Presence Service. The IM and Presence Service does not accept any packets from the external server until DNS validates the identity of the external server.

**Step 7** Click **Save**.

- Tip**
- For further information on the security settings, see the Online Help.
  - If the node is part of an intercluster deployment, then you must configure each cluster with the same security settings. Run the System Troubleshooter to ensure that your configuration is consistent on all nodes.

---

#### Related Topics

[Turn On XMPP Federation on a Node](#), on page 114

## DNS Configuration for XMPP Federation

### DNS SRV Records for XMPP Federation

To allow the IM and Presence Service to discover a particular XMPP federated domain, the federated enterprise must publish the `_xmpp-server` DNS SRV record in its public DNS server. Similarly, the IM and Presence Service must publish the same DNS SRV record in the DNS for its domain. Both enterprises must publish the port 5269. The published FQDN must also be resolvable to an IP address in DNS.

A DNS SRV record should be published for each domain in the IM and Presence Service deployment. You can use the **Cisco Unified Communications Manager IM and Presence Administration** user interface to view a list of all the domains. Go to the **Presence Domains** window to view a list of all domains in the system. Log in to **Cisco Unified IM and Presence Administration** and choose **Presence > Domains**.

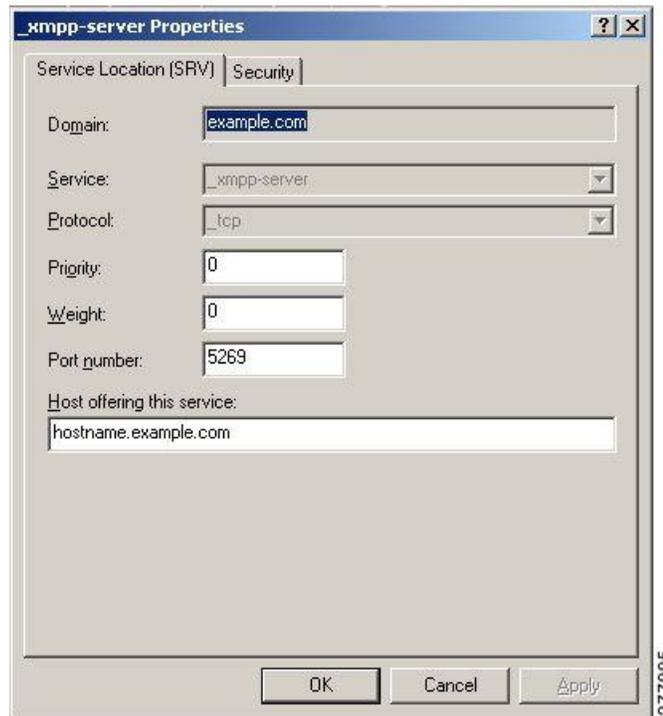
You can also use the **Email Domains for Federation** window to view the list of all email domains in the system if the email address for federation feature is enabled. Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**.

The required DNS record is:

`_xmpp-server._tcp.domain`

The following figure shows a sample DNS configuration for the `_xmpp-server` DNS SRV record for the domain **example.com**.

**Figure 23: DNS SRV for `_xmpp-server`**



Two DNS records are needed for each server in the cluster: one DNS record for IPv4 and the second DNS record for IPv6. Indicate if the record is the IPv4 or IPv6 version using the `hostname` value in the **Host offering this service** field. For example:

- **hostname-v4.example.com** indicates that the DNS record is the IPv4 version.
- **hostname-v6.example.com** indicates that the DNS record is the IPv6 version.

If you have remote root access to the IM and Presence Service, you can run `nslookup` to determine if the federated domain is discoverable.



**Tip** Use this sequence of commands for performing a DNS SRV lookup:

```
nslookup

set type=srv

_xmpp-server._tcp.domain
```

(*domain* is the domain of the federated enterprise.)

This command returns an output similar to this example, where "example.com" is the domain of the federated server:

```
_xmpp-server._tcp.example.com service = 0 0 5269 hostname.example.com.
```

For a single cluster, you only need to enable XMPP federation on one node in the cluster. You publish one DNS SRV record for the enterprise in the public DNS. The IM and Presence Service routes all incoming requests from external domains to the node running federation. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service also routes all outgoing requests to the node running XMPP federation.

You can also publish multiple DNS SRV records (for example, for scale purposes), or if you have multiple IM and Presence Service clusters and you must enable XMPP federation at least once per cluster. Unlike SIP federation, XMPP federation does not require a single point of entry for the IM and Presence Service enterprise domain. As a result, the IM and Presence Service can route incoming requests to any one of the published nodes in the cluster that you enable for XMPP federation.

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external XMPP federated domain initiates a new session, it performs a DNS SRV lookup to determine where to route the request. If you publish multiple DNS SRV records for each domain, the DNS lookup returns multiple results; the IM and Presence Service can route the request to any of the servers that DNS publishes. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation.

If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, the IM and Presence Service routes all incoming requests to that single node, rather than load-balancing the incoming requests across the nodes running XMPP federation. The IM and Presence Service load-balances outgoing requests and sends outgoing requests from any of the nodes running XMPP federation.

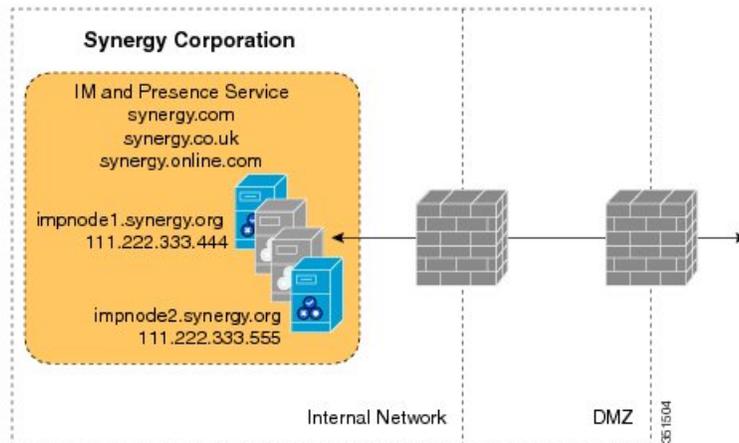


**Note** Along with the DNS SRV records that you publish, you must also add the corresponding DNS A and AAAA records.

### XMPP DNS SRVs in an Interdomain Federation Deployment

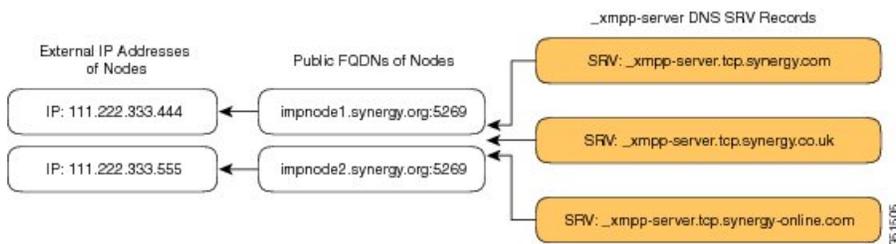
In the following example interdomain federation deployment, two IM and Presence Service nodes are enabled for XMPP federation. A DNS SRV record must be published for each domain that is hosted in the IM and Presence Service deployment. The following figure shows an example interdomain federation deployment with three local domains. You must publish an `_xmpp-server` DNS SRV record for each domain.

Figure 24: Multiple Domains in an XMPP-Based Federated Interdomain Deployment



Each DNS SRV record must resolve to the public FQDN of both IM and Presence Service nodes that are designated for XMPP federated traffic, and the FQDNs must resolve to the external IP addresses of the IM and Presence Service nodes.

Figure 25: XMPP DNS SRV Resolving to Public FQDNs of IM and Presence Service Nodes



**Note** The firewalls that are deployed within the DMZ can translate the IP addresses (NAT) to the internal IP address of the node. The FQDN of the nodes must be publically resolvable to a public IP address.

### Related Topics

[DNS SRV Records for Chat Feature for XMPP Federation](#), on page 118

## DNS SRV Records for Chat Feature for XMPP Federation

If you configure the Chat feature on an IM and Presence Service node in an XMPP federation deployment, you must publish the chat node alias in DNS.

The hostname, to which the DNS SRV record for the chat node resolves, resolves to a public IP address. Depending on your deployment, you may have a single public IP address or a public IP address for each chat node within your network:

Table 19: Chat Request Routing

| Deployment                                              | Chat Request Routing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Single public IP address, multiple nodes internally     | <p>To route all chat requests to the XMPP federation node, and then on to the chat node:</p> <ol style="list-style-type: none"> <li>1. Configure the DNS SRV for the chat node alias to point to port 5269.</li> <li>2. Configure a NAT command configured on Cisco Adaptive Security Appliance or firewall\NAT server that maps publicIPAddress:5269 to XMPPFederationNodePrivateIPAddress:5269.</li> </ol>                                                                                                                                                                                                                                               |
| Multiple public IP addresses, multiple nodes internally | <p>If you have multiple public IP addresses, you can choose to route chat requests directly to the appropriate chat node.</p> <ol style="list-style-type: none"> <li>1. Configure the DNS SRV for the chat node to use some arbitrary port other than 5269, for example, 25269.</li> <li>2. Configure a NAT command on Cisco Adaptive Security Appliance or firewall\NAT server that maps textChatServerPublicIPAddress:25269 to textChatServerPrivateIPAddress:5269.</li> </ol> <p><b>Note</b> To allow the chat node to handle incoming federated text requests, you must turn on the Cisco XCP XMPP Federation Connection Manager on the chat node.</p> |

For information on configuring the Chat feature on the IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

#### Related Topics

[Configure DNS SRV Record for Chat Node for XMPP Federation](#), on page 119

## Configure DNS SRV Record for Chat Node for XMPP Federation

### Procedure

- 
- Step 1** To retrieve the chat node alias:
- a) Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Messaging > Group Chat Server Alias Mapping**.
  - b) Click **Find** to display a list of chat node aliases.
  - c) Choose the chat node alias that you want to publish in DNS, for example:  
conference-2.StandAloneCluster.example.com
- Step 2** In the public DNS server for the example.com domain, create the StandAloneCluster domain.
- Step 3** In the StandAloneClusterdomain, create the conference-2domain.
- Step 4** In the conference-2 domain, create the \_tcp domain.
- Step 5** In the \_tcp domain, create two new DNS SRV records for \_xmpp-server: one for IPv4 and another one for IPv6. See the following figures for a sample DNS configuration records.

**Note** If the text conference server alias is `conference-2-StandAloneCluster.example.com` then the domain in Step 2 is `conference-2-StandAloneCluster`, and you skip Step 3. In Step 4, create the `_tcp` domain under `conference-2-StandAloneCluster`.

Figure 26: IPv4 DNS SRV Record for `_xmpp-server` for Chat Feature

The screenshot shows the `_xmpp-server Properties` dialog box with the `Service Location (SRV)` tab selected. The fields are filled with the following values:

- Domain: `conference-2-StandAloneClusterab004.example.com`
- Service: `_xmpp-server`
- Protocol: `_tcp`
- Priority: `2`
- Weight: `0`
- Port number: `5269`
- Host offering this service: `cup-dod67-v4.example.com`

Buttons at the bottom include `OK`, `Cancel`, `Apply`, and `Help`. A vertical label `371266` is on the right side.

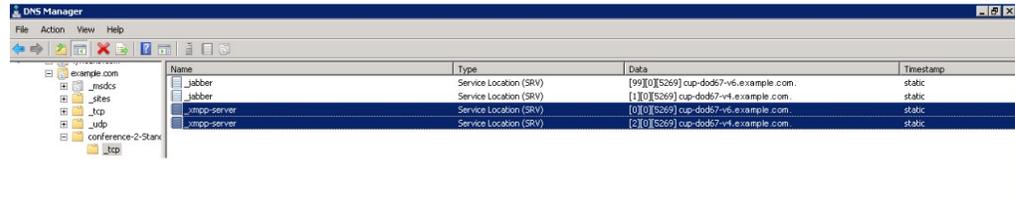
Figure 27: IPv6 DNS SRV Record for `_xmpp-server` for Chat Feature

The screenshot shows the `_xmpp-server Properties` dialog box with the `Service Location (SRV)` tab selected. The fields are filled with the following values:

- Domain: `conference-2-StandAloneClusterab004.example.com`
- Service: `_xmpp-server`
- Protocol: `_tcp`
- Priority: `0`
- Weight: `0`
- Port number: `5269`
- Host offering this service: `cup-dod67-v6.example.com`

Buttons at the bottom include `OK`, `Cancel`, `Apply`, and `Help`. A vertical label `371267` is on the right side.

Figure 28: DNS Configuration for Chat Feature



| Name         | Type                   | Data                                   | Timestamp |
|--------------|------------------------|----------------------------------------|-----------|
| _jabber      | Service Location (SRV) | [99][0][5269]cup-dod67-v6.example.com. | static    |
| _sips        | Service Location (SRV) | [1][0][5269]cup-dod67-v4.example.com.  | static    |
| _sip         | Service Location (SRV) | [0][0][5269]cup-dod67-v6.example.com.  | static    |
| _xmpp-server | Service Location (SRV) | [2][0][5269]cup-dod67-v4.example.com.  | static    |

371255

## Related Topics

[DNS SRV Records for XMPP Federation](#), on page 115

# Policy Settings Configuration for XMPP Federation

## Policy Exception Configuration

You can configure exceptions to the default policy for XMPP federation. In the exception, you must specify the external domain to which you want to apply the exception, and a direction rule for the exception. When you configure the domain name for a policy exception, note the following:

- If the URI or JID of the user is `user@example.com`, configure the external domain name in the exception as `example.com`.
- If the external enterprise uses `hostname.domain` in the URI or JID of the user, for example `user@hostname.example.com`, configure the external domain name in the exception as `hostname.example.com`.
- You can use a wildcard (\*) for the external domain name in the exception. For example, the value `*.example.com` applies the policy on `example.com` and any subdomain of `example.com`, for example, `somewhere.example.com`.

You must also specify the direction that IM and Presence Service applies the policy exception. These direction options are available:

- **all federated packets from/to the above domain/host** - The IM and Presence Service allows or denies all traffic going to and coming from the specified domain.
- **only incoming federated packets from the above domain/host** - Allow the IM and Presence Service to receive inbound broadcasts from the specified domain, but the IM and Presence Service does not send responses.
- **only outgoing federated packets to the above domain/host** - Allow the IM and Presence Service to send outbound broadcasts to the specified domain, but the IM and Presence Service does not receive responses.

## Configure Policy for XMPP Federation



**Caution** If you make a change to any of the XMPP Federation settings, you must restart these services in the **Cisco Unified IM and Presence Serviceability** user interface: Cisco XCP Router (choose **Tools > Control Center - Network Services**), Cisco XCP XMPP Federation Connection Manager (choose **Tools > Control Center - Feature Services**). When you restart the Cisco XCP Router service, the IM and Presence Service restarts all the XCP services.

### Procedure

**Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Policy**.

**Step 2** Choose the policy settings from the drop-down list:

- Allow - IM and Presence Service permits all federated traffic from XMPP federated domains, except those domains that you explicitly deny on the policy exception list.
- Deny - IM and Presence Service denies all federated traffic from XMPP federated domains, except those domains that you explicitly permit on the policy exceptions list.

**Step 3** To configure a domain on the policy exception list:

- a) Click **Add New**.
- b) Specify the domain name or the hostname of the external server.
- c) Specify the direction to apply the policy exception.
- d) Click **Save** on the policy exception window.

**Step 4** Click **Save** on the policy window.

#### Tip:

See the Online Help for federation policy recommendations.

### Related Topics

[Policy Exception Configuration](#), on page 121

## Configure the Cisco Adaptive Security Appliance for XMPP Federation

For XMPP Federation, the Cisco Adaptive Security Appliance acts as a firewall only. You must open port 5269 for both incoming and outgoing XMPP federated traffic on the Cisco Adaptive Security Appliance.

These are sample access lists to open port 5269 on the Cisco Adaptive Security Appliance, Release 8.3.

Allow traffic from any address to any address on port 5269:

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

Allow traffic from any address to any single node on port 5269:

```
access-list ALLOW-ALL extended permit tcp any host private_imp_ip_address eq 5269
```

If you do not configure the access list above, and you publish additional XMPP federation nodes in DNS, you must configure access to each of these nodes, for example:

```
object network obj_host_private_imp_ip_address
#host private_imp_ip_address

object network obj_host_private_imp2_ip_address
#host private_imp2_ip_address

object network obj_host_public_imp_ip_address
#host public_imp_ip_address
```

Configure the following NAT commands:

```
nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

If you publish a single public IP address in DNS, and use arbitrary ports, configure the following:

(This example is for two additional XMPP federation nodes)

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_35269

nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```

If you publish multiple public IP addresses in DNS all using port 5269, configure the following:

(This example is for two additional XMPP federation nodes)

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp3_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

**Related Topics**

[Cisco Adaptive Security Appliance Configuration for SIP Federation](#), on page 59

## Turn On XMPP Federation Service

You need to turn on the Cisco XCP XMPP Federation Connection Manager service on each IM and Presence Service node that runs XMPP federation. Once you turn on the Federation Connection Manager service from the **Service Activation** window, IM and Presence Service automatically starts the service; you do not need to manually start the service from the **Control Center - Feature Services** window.

**Before you begin**

Turn on XMPP Federation for the node from Cisco Unified CM IM and Presence Administration, see [Turn On XMPP Federation on a Node, on page 114](#).

**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, select the server.
  - Step 3** Click **Go**.
  - Step 4** In the IM and Presence Services area, click the button next to the **Cisco XCP XMPP Federation Connection Manager** service.
  - Step 5** Click **Save**.
- 

**Related Topics**

[Serviceability Configuration for Federation](#), on page 137



## CHAPTER 13

# Security Certificate Configuration for XMPP Federation

---

- [Security Certificate Configuration for XMPP Federation, on page 125](#)
- [Local Domain Validation for XMPP Federation, on page 125](#)
- [Multi-Server Certificate Overview, on page 126](#)
- [Use a Self-Signed Certificate for XMPP Federation, on page 126](#)
- [Use of a CA Signed Certificate for XMPP Federation, on page 127](#)
- [Import a Root CA Certificate for XMPP Federation, on page 130](#)

## Security Certificate Configuration for XMPP Federation

To configure security for XMPP federation, you must complete the following procedures:

1. Verify that all local domains are created and configured on the system and, if necessary, manually create any missing local domains before you generate the cup-xmpp-s2s certificate.
2. Create the certificate once using one of the following types of certificates:
  - Self-signed single server certificate for XMPP federation
  - CA-signed single-server or multiple server certificate for XMPP federation
3. Import the root CA certificate.

You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the root CA certificate.

## Local Domain Validation for XMPP Federation

All local domains must be included in the generated cup-xmpp-s2s certificate. Before you generate the cup-xmpp-s2s certificate, validate that all local domains are configured and appear in the Domains window. Manually add any domains that are planned for, but that don't yet appear in the list of local domains. For example, a domain that does not currently have any users assigned normally does not appear in the list of domains.

Log in to the **Cisco Unified CM IM and Presence Administration** user interface, choose **Presence > Domains**.

After you have validated that all domains are created in the system, you can proceed to create the cup-xmpp-s2s certificate once using either a self-signed certificate or a CA-signed certificate for XMPP federation. If email address for federation is enabled, all email domains must also be included in the certificate.

If you add, update, or delete any local domains and regenerate the cup-xmpp-s2s certificate, you must restart the Cisco XCP XMPP Federation Connection Manager service. To restart this service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools > Control Center - Feature Services**.

#### Related Topics

[Add or Update Email Domain](#), on page 135

[Use a Self-Signed Certificate for XMPP Federation](#), on page 126

[Use of a CA Signed Certificate for XMPP Federation](#), on page 127

[View Email Domains](#), on page 134

## Multi-Server Certificate Overview

IM and Presence Service supports multi-server SAN based certificates for the certificate purposes of tomcat, cup-xmpp and cup-xmpp-s2s. You can select between a single-server or multi-server distribution to generate the appropriate Certificate Signing Request (CSR). The resulting signed multi-server certificate and its associated chain of signing certificates is automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.

## Use a Self-Signed Certificate for XMPP Federation

This section describes how to use a self-signed certificate for XMPP federation. For information about using a CA-signed certificate, see [Use of a CA Signed Certificate for XMPP Federation, on page 127](#).

#### Procedure

- 
- Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
  - Step 2** Click **Generate Self-signed**.
  - Step 3** From the Certificate Purpose drop-down list, choose **cup-xmpp-s2s** and click **Generate**.
  - Step 4** Restart the Cisco XCP XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services** to restart this service.
  - Step 5** Download and send the certificate to another enterprise so that it can be added as a trusted certificate on their XMPP server. This can be a IM and Presence Service node or another XMPP server.
-

**What to do next**

[Use of a CA Signed Certificate for XMPP Federation, on page 127](#)

## Use of a CA Signed Certificate for XMPP Federation

This section describes how to use a CA signed certificate. For information about using a self-signed certificate, see [Use a Self-Signed Certificate for XMPP Federation, on page 126](#).

### Generate a Certificate Signing Request for XMPP Federation

This procedure describes how to generate a Certificate Signing Request (CSR) for a Microsoft Certificate Services CA.



**Note** While this procedure is to generate a CSR for signing a Microsoft Certificate Services CA, the steps to generate the CSR (steps 1 to 3) apply when requesting a certificate from any Certificate Authority.

**Procedure**

- Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
- Step 2** To generate the CSR, perform these steps:
- Click **Generate CSR**.
  - From the Certificate Purpose drop-down list, choose **cup-xmpp-s2s** for the certificate name.
  - For the distribution select the FQDN of the local server to generate a single-signed certificate or **Multi-server(SAN)** to generate a multi-server certificate.  
**Note** For both distribution options all presence domains, email domains, and Group Chat Server aliases configured on the Cisco Unified IM and Presence Administration user interface will be automatically included in the CSR that is generated. If you choose the **Multi-server(SAN)** option, the hostname or FQDN of each IM and Presence Service node(s) is also added to the CSR that is generated. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.
  - Click **Generate**.
- Note** If you have selected **Multi-server(SAN)** the CSR will be copied to the file-system on all other IM and Presence Service nodes in the cluster.
- Click **Close**, and return to the main certificate window.
- Step 3** To download the `.csr` file to your local machine:
- Click **Download CSR**.
  - Choose **cup-xmpp-s2s** from the Certificate Purpose drop-down menu.
  - Click **Download CSR** to download this file to your local machine.

- Step 4** Using a text editor, open the `cup-xmpp-s2s.csr` file.
- Step 5** Copy the contents of the CSR file.  
You must copy all information from and including  
- BEGIN CERTIFICATE REQUEST  
to and including  
END CERTIFICATE REQUEST -
- Step 6** On your internet browser, browse to your CA server, for example: `http://<name of your Issuing CA Server>/certsrv`.
- Step 7** Click **Request a certificate**.
- Step 8** Click **Advanced certificate request**.
- Step 9** Click **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 10** Paste the contents of the CSR file (that you copied in step 5) into the Saved Request field.
- Step 11** Click **Submit**.
- Step 12** On your internet browser, return to the URL: `http://<name of your Issuing CA Server>/certsrv`.
- Step 13** Click **View the status of a pending certificate request**.
- Step 14** Click on the certificate request that you issued in the previous section.
- Step 15** Click **Base 64 encoded**.
- Step 16** Click **Download certificate**.
- Step 17** Save the certificate to your local machine:
- Specify a certificate file name `cup-xmpp-s2s.pem`.
  - Save the certificate as type **Security Certificate**.

---

### What to do next

[Upload a CA-Signed Certificate for XMPP Federation, on page 128](#)

#### Troubleshooting Tips

- If the list of supported domains on IM and Presence Service changes, then the `cup-xmpp-s2s` certificate must be regenerated to reflect the new domain list.

## Upload a CA-Signed Certificate for XMPP Federation

### Before you begin

Complete the steps in [Generate a Certificate Signing Request for XMPP Federation, on page 127](#).

## Procedure

---

- Step 1** Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
- Step 2** Click **Upload Certificate/Certificate chain..**
- Step 3** Choose **cup-xmpp-s2s** for Certificate Name.
- Step 4** Browse to the location of the CA-signed certificate that you saved to your local machine.
- Step 5** Click **Upload File**.
- Note** If you have generated a multi-server SAN based certificate, you can upload this to any IM and Presence Service node in the cluster. When this is done the resulting signed multi-server certificate and its associated chain of signing certificates are automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. If a self-signed certificate already exists on any of the nodes, it will be overwritten by the new multiple server certificate. For more information on multi-server certificates, see the New and Changed Features chapter of the *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*.
- Step 6** Restart the Cisco XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services** to restart this service.
- Note** If you upload a multi-server certificate you must restart the XCP Router service on **all** IM and Presence Service nodes in the cluster.
- 

## What to do next

To support cross navigation for serviceability between nodes in the same cluster, the Cisco Tomcat service trust stores between IM and Presence Service and Cisco Unified Communications Manager are automatically synchronized.

When CA signed certificates are generated to replace the original self-signed trust certificates on either IM and Presence Service or Cisco Unified Communications Manager, the original certificates persist in the node's service trust store. Leaving the original self-signed certificates in the service trust store is not an issue because no service presents them. However, you can delete these certificates, but if you do, you must delete them on the IM and Presence Service and Cisco Unified Communications Manager,

See the section Delete Self-Signed Trust Certificates in Part II, Chapter 9 — Security Configuration on IM and Presence Service, in the appropriate release of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* at <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>.

# Import a Root CA Certificate for XMPP Federation



**Note** This section describes how to manually upload the cup-xmpp-s2s trust certificates to IM and Presence Service. You can also use the Certificate Import Tool to automatically upload cup-xmpp-s2s trust certificates. To access the Certificate Import Tool, log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Security > Certificate Import Tool**, and see the Online Help for instructions on how to use this tool.

If IM and Presence Service federates with an enterprise, and a commonly trusted Certificate Authority (CA) signs the certificate of that enterprise, you must upload the root certificate from the CA to an IM and Presence Service node.

If IM and Presence Service federates with an enterprise that uses a self-signed certificate rather than a certificate signed by a commonly trusted CA, you can upload the self-signed certificate using this procedure.

## Before you begin

Download the root CA certificate and save it to your local machine.

## Procedure

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

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

**Step 3** Choose **cup-xmpp-trust** for Certificate Name.

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

**Step 4** Click **Browse**, and browse to the location of the root CA certificate that you previously downloaded and saved to your local machine.

**Step 5** Click **Upload File** to upload the certificate to the IM and Presence Service node.

**Note** You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the Root CA certificate.

## Troubleshooting Tip

If your trust certificate is self-signed, you cannot turn on the **Require client side certificates** parameter in the XMPP federation security settings window.



## CHAPTER 14

# Email Address for Federation Configuration

This chapter provides information about the Email Address for Federation feature and multiple domain configuration.

- [Email for Federation Enablement, on page 131](#)
- [Email Address for Federation Considerations, on page 131](#)
- [Email Address for Federation Configuration and Email Domain Management, on page 134](#)

## Email for Federation Enablement

When you turn on the email address for federation feature, the IM and Presence Service changes the JID of the local user to the email address of the contact.

If you have an intercluster deployment, you must turn on the email address for federation on all intercluster nodes in your deployment. You must then restart the Cisco XCP Router service after the email for federation feature is turned on.

In an XMPP federation deployment, the email address for federation feature does not currently support temporary or persistent chat rooms in a multicluster IM and Presence Service deployment. In the deployment scenario where there are multiple IM and Presence Service clusters in the local domain, the local users actual JID may be sent to the federated user. The only impact to the chat room is that the name that displays to the federated user is the userid of the local user, instead of the email address of the local user; all other chat room functionality operates as normal. This only occurs in temporary or persistent chat rooms with federated users.

For more information about the email address for federation feature for SIP and XMPP federation, and for instructions to turn on the feature, see topics related to email address for federation configuration.

## Email Address for Federation Considerations

When you configure the IM and Presence Service to use the email address for SIP or XMPP federation, the IM and Presence Service swaps the IM address of the local user for the user's email address in all communications with a federated contact.

Before you turn on email address for interdomain federation, note the following:

- If you have not yet attempted to federate with the external domain, and you wish to turn on email for federation, we recommend that you turn on this setting before users begin to add any federated contacts.

- If you turn on email address for federation, and a user does not have an email address configured in Active Directory, the IM and Presence Service uses the JID of the user for federation.
- A prerequisite for this feature is that the Cisco Unified Communications Manager Mail ID for each user must match the full email address for the user.

If the Mail ID field for the user is empty or does not contain a full email address, the IM and Presence Service defaults to using the IM and Presence Service JID of the user for federation

- If you turn on email address for federation, and a federated contact uses the JID of an IM and Presence Service user rather than using the email address, the IM and Presence Service drops these requests (even if a valid email address is configured for the user).
- The IM and Presence Service does not support email aliases for the email address for federation feature.

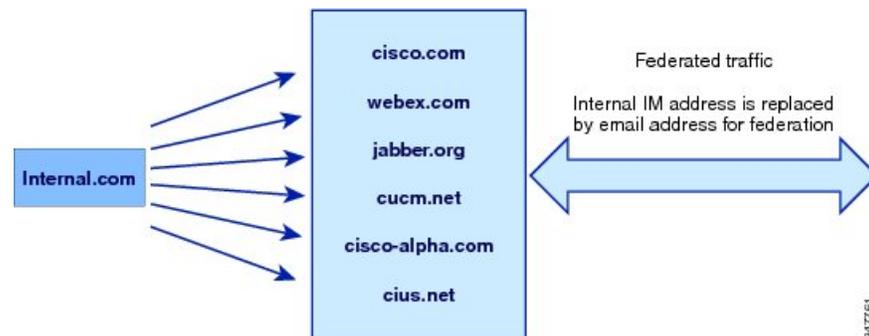


**Note** This feature applies to both SIP and XMPP federation.

## Email Address for Federation Support of Multiple Domains

The Email Address for Federation feature supports multiple domains. The following figure shows an example of multiple email domains that are being used for federated traffic.

*Figure 29: Email Address for Federation Support for Multiple Domains*



If the local IM and Presence Service deployment is managing multiple email domains, you must publish the required DNS SRV records for each local email domain.

For XMPP federation, the cup-xmpp-s2s security certificate must have all local IM and email domains included as Subject Alt Names.

## Email Domain Configuration Overview

Manually adding and editing email domains for use with the Email Address for Federation feature is optional since the IM and Presence Service automatically reads all unique domains for each of the user's email addresses and uses that information for the Email Address for Federation feature.

If you have domains that have users who are not yet configured for the IM and Presence Service but plan to configure those users, then you can manually add those domains to the IM and Presence Service using the

**Cisco Unified CM IM and Presence Administration** user interface. A domain that does not currently have any users assigned is not automatically listed as a local email domain in the user interface.

User domains that are used for Email Address for Federation are listed as system-managed domains on the **Email Domain** window in the **Cisco Unified CM IM and Presence Administration** user interface. These are not configurable with the user interface.

## Information to Provide to the Administrator of an External Domain

Before you turn on email address for federation, you must alert the system administrator of the external domain to the following:

- You are using email address for federation, and that the users in the external domain must specify an email address when adding a federated contact to their contact list.
- If you are already federating with the external domain, and you wish to turn on email for federation, users in the external domain must remove the existing federated contacts in their contact list, and add these federated contacts again specifying an email address.

## Information to Provide IM and Presence Service Users

When you turn on email address for federation, you must notify all IM and Presence Service users of the following:

- Federated contacts now use email addresses rather than the `user_id@domain` addresses.
- When adding new contacts to their contact list, federated contacts must now use the email address for IM and Presence Service users, rather than the `user_id@domain`.
- Existing IM and Presence Service contacts (on the federated watcher's contact list) that were added with `user_id@domain` must be removed, and added again using the email address for the IM and Presence Service user.
- Any messages that the IM and Presence Service receives from federated contacts to the `user_id@domain` address are dropped (unless it happens to be the same as the email address configured in Active Directory, and the address configured in the users table on the IM and Presence Service).
- If IM and Presence Service users already have federated contacts on their contact list, when these users sign in to the client again, the federated contact may get a pop-up containing the email address.

**Note**

When you turn on email address for federation, the IM and Presence Service user does NOT need to change anything on the client when they connect to the IM and Presence Service, nor do they interact any differently with the IM and Presence Service node.

## Email Domain Management Interactions and Restrictions

- You can add or delete only administrator-managed domains that are associated with the local cluster.
- You cannot edit system managed domains.

- You cannot edit system-managed or administrator managed domains that are associated with other clusters.
- It is possible to have a domain configured on two clusters, but in use on only the peer cluster. This appears as a system-managed domain on the local cluster, but is identified as being in use on only the peer cluster.
- For XMPP Federation over TLS, you must regenerate the TLS certificate `cup-xmpp-s2s` if adding or removing an IM address domain.

# Email Address for Federation Configuration and Email Domain Management

## Turn On Email for Federation



---

**Note** If you have an intercluster deployment, you must turn on the email address for federation on any intercluster nodes in your deployment.

---

### Procedure

---

- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Settings**.
  - Step 2** Check the **Enable use of Email Address for Inter-domain Federation** check box.
  - Step 3** Read the warning message, and click **OK**.
  - Step 4** Click **Save**.
  - Step 5** After you turn on email for federation, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services**.
- 



---

**Note** If you want to edit routing parameters for Federation, go to [Configure Federation Routing Parameters](#), on [page 40](#).

---

## View Email Domains

System-managed domains and local domains that are administrator-managed are displayed on the Find and List Email Domains window using the **Cisco Unified CM IM and Presence Administration** user interface. This window also specifies whether each administrator-managed domain was configured on the local cluster, peer cluster, or both.

## Procedure

---

Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**. The **Find and List Email Domains** window appears.

---

## Add or Update Email Domain

You can manually add IM address domains to your local cluster and update existing IM address domains that are on your local cluster using **Cisco Unified CM IM and Presence Administration** user interface.

You can enter a domain name of up to a maximum of 255 characters and each domain must be unique across the cluster. Allowable values are any upper or lower case letter (a-z, A-Z), any number (0-9), the hyphen (-), or the dot (.). The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.lom is an example of an invalid domain.

System-managed domains and local domains that are administrator-managed are displayed on the Find and List Domains window. This window also specifies whether each administrator-managed domain was configured on the local cluster, peer cluster, or both.

System-managed domains cannot be edited because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that IM address domain (for example, due to user deletion). You can edit or delete administrator-managed domains.

## Procedure

---

- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**.
- The **Find and List Email Domains** window appears displaying all administrator-managed and system-managed email domains.
- Step 2** Perform one of the following actions:
- Click **Add New** to add a new domain. The **Email Domain** window appears.
  - Choose the domain to edit from the list of domains. The **Email Domain** window appears.
- Step 3** Enter the new domain name in the **Domain Name** field, and then click **Save**.
- Enter a unique domain name up to a maximum of 255 characters. Allowable values are any upper or lower case letter (a-z, A-Z), any number (0-9), the hyphen (-), or the dot (.). Domain labels must not start with a hyphen, and the last label (for example, .com) must not start with a number.
- Tip** A warning message appears. If you are using TLS XMPP federation, you should proceed to generate a new TLS certificate.
-

## Delete an Email Domain

You can delete administrator-managed email address domains that are in the local cluster using **Cisco Unified CM IM and Presence Administration** user interface.

System-managed domains cannot be deleted because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that email domain (for example, due to user deletion). You can edit or delete administrator-managed domains.

**Note**

If you delete an administrator-managed domain that is configured on both local and peer clusters, the domain remains in the administrator-managed domains list; however, that domain is marked as configured on the peer cluster only. To completely remove the entry, you must delete the domain from all clusters on which it is configured.

**Procedure**

**Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**.

The **Find and List Email Domains** window appears displaying all administrator-managed and system-managed email address domains.

**Step 2** Choose the administrator-managed domains to delete using one of the following methods, and then click **Delete Selected**.

- Check the check boxes beside the domains to delete.
- Click **Select All** to select all domains in the list of administrator-managed domains.

**Tip** Click **Clear All** to clear all selections.

**Step 3** Click **OK** to confirm the deletion or click **Cancel**.



## CHAPTER 15

# Serviceability Configuration for Federation

---

- [Use of Logging for Federation, on page 137](#)
- [How to Restart the Cisco XCP Router, on page 138](#)

## Use of Logging for Federation

### Location of Log Files for SIP Federation

The following log files are applicable for SIP federation:

- `sip-cm-3_0000000X.log` located in `/var/log/active/epas/trace/xcp/log`
- `esp0000000X.log` located in `/var/log/active/epas/trace/esp/sdi`

You can also capture these logs from RTMT.

### Location of Log File for XMPP Federation

The following log file applies to XMPP federation:

- `xmpp-cm-4_0000000X.log` located in `/var/log/active/epas/trace/xcp/log`

You can also capture logs from RTMT.

## Turn On Logging for Federation

### Procedure

---

- Step 1** Log on to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace > Configuration**.
- Step 2** From the Server drop-down list, choose the IM and Presence Service server, and click **Go**.
- Step 3** From the Service Group list box, choose **IM and Presence Services**, and click **Go**.
- Step 4** Perform one of the following steps:

- a) For SIP federation, choose the Cisco XCP SIP Federation Connection Manager service from the Service drop-down list, and click **Go**.
- b) For XMPP federation, choose the Cisco XCP XMPP Federation Connection Manager service from the Service drop-down list, and click **Go**.

**Step 5** Click **Trace On**.

Choose the Debug Trace Level in the Trace Filter Settings. If you want to enable Debug level on the traces choose Debug for Debug Trace Level.

---

## How to Restart the Cisco XCP Router

### Cisco XCP Router

If you make any configuration changes for SIP or XMPP federation configuration, you must restart the Cisco XCP Router on the IM and Presence Service. If you restart the Cisco XCP Router, the IM and Presence Service automatically restarts all active XCP services.

Note that you must restart the Cisco XCP Router, not turn off and turn on the Cisco XCP Router. If you turn off the Cisco XCP Router, rather than restart this service, the IM and Presence Service stops all other XCP services. Subsequently when you then turn on the XCP router, the IM and Presence Service does not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

### Restart Cisco XCP Router

#### Procedure

---

- Step 1** Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services**.
  - Step 2** From the Server drop-down list, choose the server.
  - Step 3** Click **Go**.
  - Step 4** In the IM and Presence Services area, click the radio button next to the Cisco XCP Router service.
  - Step 5** Click **Restart**.
  - Step 6** Click **OK** when a message indicates that restarting may take a while.
-



# CHAPTER 16

## Federation Integration Verification

---

- [Verify SIP Federation Configuration, on page 139](#)
- [Verify XMPP Federation Configuration, on page 140](#)

### Verify SIP Federation Configuration

This procedure describes how to verify the configuration for a federated network between a IM and Presence Service enterprise deployment, and a Microsoft OCS enterprise deployment. Use this procedure as a guide for verifying the other types of integrations if necessary.



---

**Note** If there are multiple local IM and Presence Service domains, re-run this procedure for a user in each local domain.

---

#### Procedure

---

- Step 1** Log on to the Cisco Jabber client or the third-party XMPP client.
- Step 2** Log on to two federated Microsoft Office Communicator clients.
- Step 3** Perform the following steps on the first Microsoft Office Communicator client:
- Add the IM and Presence Service user as a contact.
  - A pop-up message displays on IM and Presence Service requesting that you accept or block or ignore the presence subscription of Microsoft Office Communicator user.
  - Check that the IM and Presence Service user and the Microsoft Office Communicator user are able to see each other's availability.
- Step 4** Perform the following steps on the client of the IM and Presence Service client:
- Add the second Microsoft Office Communicator user as a contact.
  - Check that you can see the availability of the Microsoft Office Communicator user.
  - A pop-up message should appear on the user client for the Microsoft Office Communicator user informing you that the Cisco Jabber user has been added as a contact.
- Step 5** Toggle between the availability states on both the clients of the IM and Presence Service user and the Microsoft Office Communicator clients. Check that the availability state changes for the contacts on each client.
- Step 6** Initiate an IM from the client of a IM and Presence Service user to a Microsoft Office Communicator user.

- Step 7** Check that the IM window appears on Microsoft Office Communicator with the message from the IM and Presence Service user.
- Step 8** Close both the IM window on the client of the IM and Presence Service user and IM window on the Microsoft Office Communicator client.
- Step 9** Initiate an IM from Microsoft Office Communicator user to the IM and Presence Service user.
- Step 10** Check that an IM window appears on the client of the IM and Presence Service user with the message from the Microsoft Office Communicator user.
- Step 11** On the Cisco Jabber client, perform the following steps:
- a) Block one of the Microsoft Office Communicator users.
 

**Note** Any third-party clients that do not support XEP-0016 - Privacy Lists, if you block from a third-party XMPP client, you only block IM; users can still exchange availability status. To block server-side IM and availability, the user configures their privacy settings from the IM and Presence Users Options interface, or from the Privacy configuration on Cisco Jabber.
  - b) Check that this Microsoft Office Communicator user now sees that the availability of the IM and Presence Service user as offline. The second Microsoft Office Communicator user should still be able to see availability status for the IM and Presence Service user.
  - c) On the client of the IM and Presence Service user, the blocked Microsoft Office Communicator user should still appear online, and you should be able to initiate an IM to the blocked Microsoft Office Communicator user.
- Step 12** Block the IM and Presence Service user from the Microsoft Office Communicator client.
- Step 13** Verify that the presence of the Microsoft Office Communicator user is no longer available on the client of the IM and Presence Service user.

## Verify XMPP Federation Configuration

This procedure describes how to verify the configuration for a federated network between an IM and Presence Service Release 9.0 enterprise deployment, and either a WebEx, an IBM Sametime, or another IM and Presence Service Release 9.0 enterprise deployment. The procedure below describes the procedure for an IM and Presence Service Release 9.0 and a WebEx deployment. Use this procedure as a guide to verify the other types of XMPP federations.



**Note** If there are multiple local IM and Presence Service domains, re-run this procedure for a user in each local domain.

### Procedure

- Step 1** Log on to the Cisco Jabber client or the third-party XMPP client connected to the IM and Presence Service Release 9.0 server.
- Step 2** Log on to two federated WebEx Connect clients.
- Step 3** Perform the following steps on the first WebEx Connect client:

- a) Add the IM and Presence Service user as a contact.
- b) A pop-up message displays on client of the IM and Presence Service user requesting that you accept or block or ignore the presence subscription from the WebEx Connect user. Accept the subscription.
- c) Check that the IM and Presence Service user and the WebEx Connect user are able to see each other's availability.

**Step 4** Perform the following steps on the client of the IM and Presence Service user:

- a) Add the second WebEx Connect user as a contact.
- b) A pop-up should appear on the WebEx Connect client. Accept the subscription.
- c) Check that you can see the availability of the WebEx Connect user.

**Step 5** Toggle between the availability states on both the client of the IM and Presence Service user and the WebEx Connect client. Check that the availability state changes for the contacts on each client.

**Step 6** Initiate an IM from the client of the IM and Presence Service user to a WebEx Connect contact.

**Step 7** Check that the IM window displays on WebEx Connect client with the IM from the IM and Presence Service user.

**Step 8** Close the IM window on both clients.

**Step 9** Initiate an IM from the WebEx Connect user to the IM and Presence Service user.

**Step 10** Check that an IM window displays on the client of the IM and Presence Service user with the IM from the WebEx Connect user.

**Step 11** On the client of the IM and Presence Service user, perform the following steps:

- a) Block one of WebEx Connect users.

**Note** If you block from a third-party XMPP client, you only block IM; users can still exchange availability status. To block server-side IM and availability, the user configures their privacy settings from the IM and Presence Users Options interface, or from the Privacy configuration on Cisco Jabber.

- b) Check that this WebEx Connect user now sees that the availability of the IM and Presence Service user as offline. The second WebEx Connect user should still be able to see availability status for the IM and Presence Service user.
- c) On the client of the IM and Presence Service user, the blocked WebEx Connect user should still appear as online, however you cannot send an IM to the blocked WebEx Connect user.

**Step 12** Block the IM and Presence Service user from the WebEx Connect client.

**Step 13** Verify that the availability of the WebEx Connect user is no longer available on the client of the IM and Presence Service user.

---





## CHAPTER 17

# Troubleshooting a SIP Federation Integration

- [Common Cisco Adaptive Security Appliance Problems and Recommended Actions, on page 143](#)
- [Common Integration Problems and Recommended Actions, on page 146](#)

## Common Cisco Adaptive Security Appliance Problems and Recommended Actions

### Certificate Configuration Problems

#### Certificate Failure Between the IM and Presence Service and Cisco Adaptive Security Appliance

The certificate configuration between the IM and Presence Service and Cisco Adaptive Security Appliance is failing.

The time and time zones on the Cisco Adaptive Security Appliance may not be configured correctly.

- Set the time and time zones on the Cisco Adaptive Security Appliance.
- Check that the time and time zones are configured correctly on the IM and Presence Service and Cisco Unified Communications Manager.

[Prerequisite Configuration Tasks for this Integration, on page 28](#)

#### Certificate Failure Between the Cisco Adaptive Security Appliance and Microsoft Access Edge

The certificate configuration between the Cisco Adaptive Security Appliance and Microsoft Access Edge is failing at certificate enrollment on the Cisco Adaptive Security Appliance.

If you are using SCEP enrollment on the Cisco Adaptive Security Appliance, the SCEP add-on may not be installed and configured correctly. Install and configure the SCEP add-on.

##### Related Topics

[CA Trustpoints, on page 49](#)

### Certificate Error in SSL Handshake

A certificate error displays in the SSL handshake.

There is no FQDN in the certificate. You need to configure the domain on the IM and Presence Service CLI, and regenerate the certificate on IM and Presence Service to have a FQDN. You need to restart the SIP proxy on the IM and Presence Service when you regenerate a certificate.

#### Related Topics

[Configure an IM and Presence Service Domain from the CLI](#)

## Error When Submitting a Certificate Signing Request to VeriSign

I am using VeriSign for certificate enrollment. When I paste the Certificate Signing Request into the VeriSign website, I get an error (usually a 9406 or 9442 error).

The subject-name in the Certificate Signing Request is missing information. If you are submitting a renewal certificate signing request (CSR) file to VeriSign, the subject-name in the Certificate Signing Request must contain the following information:

- Country (two letter country code only)
- State (no abbreviations)
- Locality (no abbreviations)
- Organization Name
- Organizational Unit
- Common Name (FQDN)

The format of the subject-name line entry should be:

```
(config-ca-trustpoint)# subject-name
cn=fqdn,U=organisational_unit_name,C=country,St=state,L=locality,O=organisation
```

#### Related Topics

[Generate New Trustpoint for VeriSign](#), on page 162

## SSL Errors when an IM and Presence Service Domain or Hostname is Changed

I changed the IM and Presence Service domain from the CLI, and I am getting SSL certificate errors between the IM and Presence Service and the Cisco Adaptive Security Appliance.

If you change the IM and Presence Service domain name from the CLI, the IM and Presence Service self-signed cert, sipproxy.pem, regenerates. As a result you must reimport the sipproxy.pem certificate into Cisco Adaptive Security Appliance. Specifically you must delete the current sipproxy.pem certificate on Cisco Adaptive Security Appliance, and reimport the (regenerated) sipproxy.pem certificate.

#### Related Topics

[Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance](#), on page 45

## Errors When Creating TLS Proxy Class Maps

The following errors are displayed when configuring the TLS Proxy class maps:

```
ciscoasa(config)# class-map ent_imp_to_external
ciscoasa(config-cmap)# match access-list ent_imp_to_external
```

```
ERROR: Specified ACL (ent_imp_to_external) either does not exist or its type is not supported
by the match command.
```

```
ciscoasa(config-cmap)# exit
```

```
ciscoasa(config)# class-map ent_external_to_imp
```

```
ciscoasa(config-cmap)# match access-list ent_external_to_imp
```

```
ERROR: Specified ACL (ent_external_to_imp) either does not exist or its type is not supported
by the match command.
```

```
ciscoasa(config-cmap)#
```

The access list for the external domain does not exist. In the example above the access list called `ent_external_to_imp` does not exist. Create an extended access list for the external domain using the `access list` command.

### Related Topics

[Access List Configuration Requirements](#), on page 72

[TLS Proxy Debugging Commands](#), on page 174

## Subscriptions Do Not Reach Access Edge

Subscriptions from Microsoft Office Communicator do not reach the Access Edge. OCS reports network function error with Access Edge as the peer. The Access Edge service does not start.

On Access Edge, the IM and Presence Service domain may be configured in both the Allow tab and the IM provider tab. The IM and Presence Service domain should only be configured in the IM Provider tab. On Access Edge, remove the IM and Presence Service domain entry from the Allow tab. Make sure there is an entry for the IM and Presence Service domain on the IM Provider tab.



---

**Note** The IM and Presence Service supports multiple domains. Make sure that you check each IM and Presence domain to determine if there are erroneous entries in the Allow tab that should be removed.

---

## Problems with Cisco Adaptive Security Appliance after Upgrade

The Cisco Adaptive Security Appliance does not boot after a software upgrade.

You can download a new software image to the Cisco Adaptive Security Appliance using a TFTP server and using the ROM Monitor (ROMMON) on the Cisco Adaptive Security Appliance. ROMMON is command line interface used for image loading and retrieval over TFTP and related diagnostic utilities.

### Procedure

---

- Step 1** Attach a console cable (the blue cable that is distributed with the Cisco Adaptive Security Appliance) from the console port to a port on a nearby TFTP server.
- Step 2** Open hyperterminal or equivalent.
- Step 3** Accept all default values as you are prompted.
- Step 4** Reboot the Cisco Adaptive Security Appliance.

**Step 5** Hit ESC during bootup to access ROMMON.

**Step 6** Enter this sequence of commands to enable Cisco Adaptive Security Appliance to download the image from your TFTP server

```
ip asa_inside_interface server tftp_server interface ethernet 0/1 file name_of_new_image
```

**Note** The Ethernet interface you specify must equate to the Cisco Adaptive Security Appliance inside interface.

**Step 7** Place the software image on the TFTP server in a recommended location (depending on your TFTP software).

**Step 8** Enter this command to start the download:

```
tftp dnld
```

**Note** You need to define a gateway if the TFTP server is in a different subnet.

---

## Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008

Cannot install a server-client authentication certificate that is signed by a Microsoft CA into the local computer store of a Microsoft Office Communications Server (OCS) running Windows 2008. Attempting to copy the certificate from the current user store to the local computer store fails with the error message that the private key is missing.

You can perform the following procedure:

1. Log in to the OCS as a local user.
2. Create the certificate.
3. Approve the certificate from the CA server.
4. While logged on to the OCS, export the certificate to a file and ensure that the private key is exported.
5. Log off the OCS (Local Computer).
6. Log in to the OCS again, but this time log in as an OCS domain user.
7. Use the Certificate Wizard to import the certificate file. The certificate is installed in the local computer store. You can now select the certificate in the OCS certificate tab.

## Common Integration Problems and Recommended Actions

### Unable to Get Availability Exchange

**Problem** Unable to exchange availability information between Cisco Jabber and Microsoft Office Communicator.

**Solution** Perform the troubleshooting steps that are listed for the OCS/Access Edge, IM and Presence Service, and Cisco Jabber.

OCS/Access Edge:

1. The certificate may have been configured incorrectly on the public interface of Access Edge. If you are using a Microsoft CA, ensure that you are using an OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2. The incorrect value displays on the general tab of the certificate (if it is correct it is not visible). You can also see the incorrect value on an ethereal trace of the TLS handshake between IM and Presence Service and Access Edge.

Regenerate the certificate for the public interface of the Access Edge with a certificate type of "Other" and OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

2. The front end server may not be running on OCS.

Ensure that the "Office Communications Server Front-End" service is running. You can check this service by choosing **Start > Programs > Administrative Tools > Computer Management**. In **Services and Applications**, choose **Services** and locate the "Office Communications Server Front-End" service. If running, this service should have a status of "Started".

IM and Presence Service:

1. The certificate may have been configured incorrectly on IM and Presence Service.

Generate the correct sipproxys-trust certificate for IM and Presence Service.

2. If you are using static routes, configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set. For example, if the federated domain is abc.com then the destination address pattern should be set to ".com.abc.\*". Static routes are configured using Cisco Unified CM IM and Presence Administration by choosing **Presence > Routing > Static Routes**.
3. Perform a check of the DNS SRV and ensure that both sides can resolve the domain of the affected users.

Cisco Jabber client:

Cisco Jabber might retrieve incorrect DNS configuration from the client computer. You should do the following:

1. Verify the DNS configuration on the client computer.
2. If you modify the DNS configuration, restart Cisco Jabber.

#### Related Topics

[Certificate Configuration for the External Access Edge Interface](#), on page 53

[Generate a New Certificate on the IM and Presence Service](#), on page 47

[DNS Configuration for SIP Federation](#), on page 38

## Problems Sending and Receiving IMs

Problems sending and receiving IM's between a Microsoft Office Communicator user and a Cisco Jabber 8.0 user.

Perform the troubleshooting steps that are listed for the DNS settings, Access Edge, Microsoft Office Communicator client, and the IM and Presence Service.

DNS Settings:

DNS SRV records may not have been created, or configured incorrectly. Check if the DNS SRV records have been configured correctly for all domains. Perform an nslookup for type=srv from both the IM and Presence and Access Edge.

**On Access Edge:**

1. From a command prompt on Access Edge, enter `nslookup`.
2. Enter `set type=srv`.
3. Enter the SRV record for the IM and Presence domain, for example `_sipfederationtls._tcp.abc.com` where `abc.com` is the domain name. If the SRV record exists, the FQDN for IM and Presence Service/Cisco Adaptive Security Appliance is returned.

On the IM and Presence Service:

4. Using a remote access account, ssh into the IM and Presence Service node.
5. Perform the same steps as per the Access Edge above, except in this case use the OCS domain name.

**Microsoft Office Communicator client:**

The Microsoft Office Communicator 2007 user may have their presence set to "Do Not Disturb" (DND). If Microsoft Office Communicator 2007 is set to DND then does not receive IM's from other users. Set the presence of the Microsoft Office Communicator user to another state.

**IM and Presence Service:**

1. If you are using static routes instead of DNS SRV, a static route may have been configured incorrectly. Configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set. For example, if the federated domain is "abc.com" then the destination address pattern should be set to ".com.abc.\*". Static routes are configured in **Cisco Unified CM IM and Presence Administration** by choosing **Presence > Routing > Static Routes**.
2. The Federation IM Controller Module Status may be disabled. In **Cisco Unified CM IM and Presence Administration**, choose **System > Service Parameters**, and choose the SIP Proxy service. At the bottom of the window, check that the **IM Gateway Status** parameter is set to On.
3. The Federated Domain may have not have been added, or configured incorrectly. In **Cisco Unified CM IM and Presence Administration**, choose **Presence > Inter-Domain Federation** and check that the correct federated domain has been added.

**Related Topics**

[DNS Configuration for SIP Federation](#), on page 38

[Add a SIP Federated Domain](#), on page 37

[Add a Microsoft OCS Domain Within Enterprise](#), on page 91

## Losing Availability and IM Exchange after a Short Period

The user can share availability and IMs between Cisco Jabber and Microsoft Office Communicator but after a short period, they start to lose each others availability, and then can no longer exchange IM's.

**OCS/Access Edge:**

1. On Access Edge, both the internal and external edges may have the same FQDN. Also in DNS there may be two "A" record entries for that FQDN, one resolving to the IP address of the external edge and the other to the IP address of the internal edge.

On Access Edge, change the FQDN of the internal edge, and add an updated record entry in DNS. Remove the DNS entry that was originally resolving to the internal IP of the Access Edge. Also reconfigure the certificate for the internal edge on Access Edge.

2. On OCS, under global settings and front end properties, the FQDN for the access edge may have been entered incorrectly. On OCS, reconfigure the server to reflect the new FQDN of the internal edge.

**DNS Settings:**

DNS SRV records may not have created, or configured incorrectly. Add the necessary "A" records and SRV records.

**Related Topics**

[External Server Component Configuration for SIP Federation](#), on page 99

## Delay in Availability State Changes and IM Delivery Time

There is a delay in the delivery time of IM and Presence Service state changes between Cisco Jabber and Microsoft Office Communicator.

On the IM and Presence Service node, the **Disable Empty TLS Fragments** option may not be selected for the `Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context`.

**Procedure**

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Security > TLS Context Configuration**.
  - Step 2** Click the link for the `Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context`.
  - Step 3** In the TLS Context Information area, check the **Disable Empty TLS Fragments** check box.
  - Step 4** Click **Save**.
- 

## 403 FORBIDDEN Returned Following an Availability Subscription Attempt

IM and Presence Service attempts to subscribe to the availability of a Microsoft Office Communicator user and receives a 403 FORBIDDEN message from the OCS server.

On the Access Edge server, the IM and Presence Service node may not have been added to the IM service provider list. On the Access Edge server, add an entry for the IM and Presence Service node to the IM service provider list. On the DNS server for Access Edge, ensure that there is a `_sipfederationtls` record for the IM and Presence Service domain that points to the public address of the IM and Presence Service node.

Or

On the Access Edge server, the IM and Presence Service node may have been added to the Allow list. On the Access Edge server, remove any entry from the Allow list that points to the IM and Presence Service node.

**Related Topics**

[External Server Component Configuration for SIP Federation](#), on page 99

## Time Out on NOTIFY Message

The IM and Presence Service times out when sending a NOTIFY message, when federating directly between IM and Presence Service and Microsoft OCS using TCP.

On the IM and Presence Service node, the **Use Transport in Record-Route Header** may need to be enabled.

### Procedure

- 
- Step 1** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **System > Service Parameters**.
  - Step 2** From the Server drop-down list, choose the node.
  - Step 3** From the Service drop-down list, choose the **Cisco SIP Proxy** service.
  - Step 4** In the SIP Parameters (Clusterwide) section, choose **On** for the Use Transport in Record-Route Header parameter.
  - Step 5** Click **Save**.
- 

## IM and Presence Service Certificate not Accepted

Access Edge is not accepting the certificate from the IM and Presence Service.

The TLS handshake between the IM and Presence Service/Cisco Adaptive Security Appliance and the Access Edge may be failing.

OCS/Access Edge:

1. Ensure that the IM Provider list on the Access Edge contains the public FQDN of the the IM and Presence Service node, and it matches the subject CN of the IM and Presence Service certificate. If you have opted not to populate the Allow List with the FQDN of the IM and Presence Service, then you must ensure that the subject CN of the IM and Presence Service certificate resolves to the FQDN of the SRV record for the IM and Presence Service domain.
2. Ensure that FIPS is enabled on Access Edge (use TLSv1).
3. Ensure that Federation is enabled globally on OCS, and enabled on the front end server.
4. If failing to resolve DNS SRV, ensure that DNS is set up correctly and perform an nslookup for type=srv from Access Edge:
5. From a command prompt on Access Edge, enter **nslookup**.
6. Enter **set type=srv**.
7. Enter the SRV record for the IM and Presence Service domain, for example, **\_sipfederationtls.\_tcp.abc.com** where **abc.com** is the domain name. If the SRV record exists, the FQDN for the IM and Presence Service/Cisco Adaptive Security Appliance is returned.

IM and Presence Service/Cisco Adaptive Security Appliance:

Check the ciphers on the IM and Presence Service and Cisco Adaptive Security Appliance. Log in to **IM and Presence Service Administration**, choose **System > Security > TLS Context Configuration > Default Cisco SIP Proxy Peer Auth TLS Context**, and ensure that the "TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA" cipher is chosen.

### Related Topics

- [External Server Component Configuration for SIP Federation](#), on page 99
- [Add TLS Peer to Selected TLS Peer Subjects List](#), on page 42

## Problems Starting Front-End Server on OCS

The front-end server on OCS does not start.

On OCS, the FQDN of the private interface of the Access Edge may have been defined in the list of Authorized Hosts. Remove the private interface of the Access Edge from the list of Authorized Hosts on OCS.

During OCS install, two Active Directory user accounts are created called RTCSservice and RTCComponentService. These accounts are given an administrator-defined password, however, on both of these accounts the "Password never expires" option is not selected by default so the password expires periodically. To reset the password of the RTCSservice or RTCComponentService on the OCS server, follow the procedure below.

### Procedure

---

- Step 1** Right-click on the user account.
  - Step 2** Choose **Reset Password**.
  - Step 3** Right-click on the user account.
  - Step 4** Choose **Properties**.
  - Step 5** Choose the **Account** tab.
  - Step 6** Check the **Password never expires** check box.
  - Step 7** Click **OK**.
- 

## Unable to Remote Desktop to Access Edge

Unable to successfully remote desktop to the Access Edge Server with FIPS enabled on Windows XP.

This is a known Microsoft issue. The workaround to resolve the issue involves installing a Remote Desktop Connection application on the Windows XP computer. To install Remote Desktop Connection 6.0, follow the instructions at the following Microsoft URL:

<http://support.microsoft.com/kb/811770>





## CHAPTER 18

# Troubleshooting an XMPP Federation Integration

- [Check System Troubleshooter, on page 153](#)

## Check System Troubleshooter

If you deploy multiple IM and Presence Service clusters and you configure XMPP federation, you must turn on XMPP federation on at least one node per cluster. You must configure the same XMPP federation settings and policy on each cluster; the IM and Presence Service does not replicate the XMPP federation configuration across cluster. The System Troubleshooter reports if XMPP federation settings across clusters are not synchronized. The System Troubleshooter performs the following checks:

### Procedure

- 
- Step 1**
- XMPP federation is enabled consistently across intercluster peers.
  - The SSL Mode is configured consistently across intercluster peers.
  - The "Required Valid client-side certificates" is configured consistently across intercluster peers.
  - The SASL settings are configured consistently across intercluster peers.
  - The dialback secret is configured consistently across intercluster peers.
  - The default Admin Policy for XMPP Federation is configured consistently across inter-cluster peers.
  - The Policy hosts are configured consistently across inter-cluster peers.
- Step 2** Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Diagnostics > System Troubleshooter**.
- Step 3** Ensure there are green check marks beside the following:
- Verify the XMPP Federation settings match on all interclustered peers.
  - Verify that SASL settings have been correctly configured for all intercluster peers.
  - Verify that XMPP has been uniformly disabled or enabled on at least one node in each all clusters.
  - Verify that the default Admin Policy is consistent across all intercluster peers.
  - Verify that the Host Policy is consistent across all intercluster peers.

The System Troubleshooter provides recommended actions if it reports a problem with any of these checks.

---



**Note** If all tests in System Troubleshooter are passed and problems with exchanging IM and availability still persist, check if the **Enable use of Email Address for Inter-domain Federation** setting, on the **Presence Settings** page is configured consistently across intercluster peers.

---

#### Related Topics

[Location of Log File for XMPP Federation](#), on page 137



## CHAPTER 19

# Sample Cisco Adaptive Security Appliance Configuration

---

- [Sample PAT Commands and Access List Configuration for SIP Federation, on page 155](#)
- [Sample Access List Configuration for XMPP Federation, on page 158](#)
- [Sample NAT Configuration for XMPP Federation, on page 159](#)

## Sample PAT Commands and Access List Configuration for SIP Federation

This section provides a sample configuration for a IM and Presence Service node that is federating with an external OCS enterprise deployment. There are two additional intercluster IM and Presence Service nodes in the local enterprise deployment.

The following values are used in this sample configuration:

- Public IM and Presence Service IP Address = 10.10.10.10
- Private Routing IM and Presence Service IP Address = 1.1.1.1
- Private Second IM and Presence Service IP Address = 2.2.2.2
- Private Third IM and Presence Service IP Address = 3.3.3.3
- Peer Auth Listener Port on IM and Presence Service = 5062
- Netmask = 255.255.255.255
- External Domain = abc.com
- Microsoft OCS External Interface = 20.20.20.20

These PAT commands are defined for the (routing) IM and Presence Service node:

**(Cisco Adaptive Security Appliance Release 8.2:)**

```
static (inside,outside) tcp 10.10.10.10 5061 1.1.1.1 5062 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 5080 1.1.1.1 5080 netmask 255.255.255.255
static (inside,outside) tcp 10.10.10.10 5060 1.1.1.1 5060 netmask 255.255.255.255
```

**(Cisco Adaptive Security Appliance Release 8.3:)**

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5061 obj_tcp_source_eq_5062
```

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_5080
```

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5060 obj_tcp_source_eq_5060
```

These PAT commands are defined for the two additional intercluster IM and Presence Service nodes in the enterprise deployment:

**(Cisco Adaptive Security Appliance Release 8.2:)**

```
static (inside,outside) tcp 10.10.10.10 45080 2.2.2.2 5080 netmask 255.255.255.255
```

```
static (inside,outside) udp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255
```

```
static (inside,outside) tcp 10.10.10.10 55070 3.3.3.3 5070 netmask 255.255.255.255
```

```
static (inside,outside) udp 10.10.10.10 45062 2.2.2.2 5062 netmask 255.255.255.255
```

```
static (inside,outside) tcp 10.10.10.10 55062 3.3.3.3 5062 netmask 255.255.255.255
```

**(Cisco Adaptive Security Appliance Release 8.3:)**

```
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5080 obj_tcp_source_eq_45080
```

```
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5070 obj_tcp_source_eq_55070
```

```
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5070 obj_udp_source_eq_55070
```

```
nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_45062
```

```
nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5062 obj_tcp_source_eq_55062
```

The corresponding access lists for this configuration are provided below. Note that for each external domain that you federate with, you must add access lists similar to these access lists for the domain abc.com.

**(Cisco Adaptive Security Appliance Release 8.2:)**

```
access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061
```

```
access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq 5061
```

```
access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq 5061
```

```
access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq 5061
```

```
access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq
45061
```

```
access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 10.10.10.10 eq
55061
```

**(Cisco Adaptive Security Appliance Release 8.3:)**

```

access-list ent_imp_to_abc extended permit tcp host 1.1.1.1 host 20.20.20.20 eq 5061
access-list ent_abc_to_imp extended permit tcp host 20.20.20.20 host 1.1.1.1 eq 5062
access-list ent_second_imp_to_abc extended permit tcp host 2.2.2.2 host 20.20.20.20 eq 5061
access-list ent_third_imp_to_abc extended permit tcp host 3.3.3.3 host 20.20.20.20 eq 5061
access-list ent_abc_to_second_imp extended permit tcp host 20.20.20.20 host 2.2.2.2 eq 5062
access-list ent_abc_to_third_imp extended permit tcp host 20.20.20.20 host 3.3.3.3 eq 5062

```

Associate each of your access lists with the a class map:

```

class-map ent_imp_to_abc
match access-list ent_imp_to_abc

class-map ent_abc_to_imp
match access-list ent_abc_to_imp

class-map ent_second_imp_to_abc
match access-list ent_second_imp_to_abc

class-map ent_third_imp_to_abc
match access-list ent_third_imp_to_abc

class-map ent_abc_to_second_imp
match access-list ent_abc_to_second_imp

class-map ent_abc_to_third_imp
match access-list ent_abc_to_third_imp

```

Update the global policy map for each class map you created. In this example, the TLS proxy instance for TLS connections initiated by the IM and Presence Service is called "imp\_to\_external", and the TLS proxy instance for TLS connections initiated by an external domain is called "external\_to\_imp".

```

policy-map global_policy
class ent_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external

policy-map global_policy
class ent_abc_to_imp
inspect sip sip_inspect tls-proxy ent_external_to_imp

policy-map global_policy
class ent_second_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external

policy-map global_policy
class ent_third_imp_to_abc
inspect sip sip_inspect tls-proxy ent_imp_to_external

policy-map global_policy

```

```

class ent_abc_to_second_imp

inspect sip sip_inspect tls-proxy ent_external_to_imp

policy-map global_policy

class ent_abc_to_third_imp

inspect sip sip_inspect tls-proxy ent_external_to_imp

```

## Sample Access List Configuration for XMPP Federation




---

**Note** The examples in this section apply to the Cisco Adaptive Security Appliance Release 8.3.

---

### Any Address Access to any Address on Port 5269

This example access list configuration allows from any address to any address on port 5269:

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

### Any Address Access to any Single XMPP Federation Node on Port 5269

This example access list configuration allows from any address to any single XMPP federation node on port 5269. The following values are used in this example:

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
```

### Any Address Access to Specific XMPP Federation Nodes Published in DNS

This example access list configuration allows from any address to specific XMPP federation nodes published in DNS.




---

**Note** The public addresses are published in DNS, but the private addresses are configured in the access-list command.

---

The following values are used in this sample configuration:

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address= 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269

```
access-list ALLOW-ALL extended permit tcp any host 1.1.1.1 eq 5269
access-list ALLOW-ALL extended permit tcp any host 2.2.2.2 eq 5269
access-list ALLOW-ALL extended permit tcp any host 3.3.3.3 eq 5269
```

### Specific Federated Domain Only Access to Specific XMPP Federation Nodes Published in DNS

This example access list configuration allows only from a specific federated domain interface to specific XMPP federation nodes published in DNS.



**Note** The public addresses are published in DNS, but the private addresses are configured in the access-list command.

The following values are used in this sample configuration:

- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269
- External interface of the external XMPP enterprise = 100.100.100.100

```
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 1.1.1.1 eq 5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 2.2.2.2 eq 5269
access-list ALLOW-ALL extended permit tcp host 100.100.100.100 host 3.3.3.3 eq 5269
```

## Sample NAT Configuration for XMPP Federation

**Example 1:** Single node with XMPP federation enabled

The following values are used in this sample configuration:

- Public IM and Presence Service IP address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- XMPP federation listening port = 5269

```
nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

**Example 2:** Multiple nodes with XMPP federation, each with a public IP address in DNS

The following values are used in this sample configuration:

- Public IM and Presence Service IP addresses = 10.10.10.10, 20.20.20.20, 30.30.30.30
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3
- XMPP federation listening port = 5269

```

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_20.20.20.20 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_30.30.30.30 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

```

**Example 3:** Multiple nodes with XMPP federation, but a single public IP address in DNS with arbitrary ports published in DNS (PAT).

The following values are used in this sample configuration:

- Public IM and Presence Service IP Address = 10.10.10.10
- Private XMPP federation IM and Presence Service Release 9.x IP address = 1.1.1.1, port 5269
- Private second IM and Presence Service Release 9.x IP address = 2.2.2.2, arbitrary port 25269
- Private third IM and Presence Service Release 9.x IP address = 3.3.3.3, arbitrary port 35269

```

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static obj_host_1.1.1.1 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static obj_host_2.2.2.2 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_udp_source_eq_5269 obj_udp_source_eq_35269

nat (inside,outside) source static obj_host_3.3.3.3 obj_host_10.10.10.10 service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269

```



## CHAPTER 20

# Security Certificate Exchange Between the Cisco Adaptive Security Appliance and Microsoft Access Edge Using VeriSign

---

- [Security Certificate Configuration on Cisco Adaptive Security Appliance, on page 161](#)
- [Import VeriSign Certificates onto Microsoft Access Edge, on page 169](#)

## Security Certificate Configuration on Cisco Adaptive Security Appliance

### Delete Old Certificates and Trustpoints

This procedure describes how to delete the old intermediate and signed certificate, and the trustpoint for the root certificate on Cisco Adaptive Security Appliance.

#### Before you begin

Ensure you carried out the configuration tasks described in the following chapters:

- [IM and Presence Service Configuration for SIP Federation, on page 37](#)
- [Cisco Adaptive Security Appliance Configuration for SIP Federation, on page 59](#)

#### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to display the trustpoints:

```
show crypto ca trustpoints
```

**Step 3** Enter this command to delete the trustpoint and associated certificates:

```
no crypto ca trustpoint trustpoint_name
```

The following warning output displays:

```
WARNING: Removing an enrolled trustpoint will destroy allcertificates received from the
related Certificate Authority.
```

**Step 4** Enter **yes** when you are prompted to delete the trustpoint.

---

### What to do next

[Generate New Trustpoint for VeriSign, on page 162](#)

## Generate New Trustpoint for VeriSign

### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to generate the key pair for this certification:

```
crypto key generate rsa label keys_for_verisign
```

**Step 3** Enter the following sequence of commands to create a trustpoint for IM and Presence Service:

```
(config)# crypto ca trustpoint trustpoint_name
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# subject-name
cn=fqdn,OU=organisational_unit,O=organisation_name,C=country,St=state,L=locality
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# exit
```

**Note** If you are submitting a renewal certificate signing request (CSR) file to VeriSign, the subject-name value must contain the following information:

- Country (two letter country code only)
- State (no abbreviations)
- Locality (no abbreviations)
- Organization Name
- Organizational Unit
- Common Name (FQDN) - This value must be the FQDN of the public IM and Presence.

Troubleshooting Tips

Enter the command `show crypto key mypubkey rsa` to check that the key pair is generated.

---

### What to do next

[Import Intermediate Certificate, on page 166](#)

## Import Root Certificate

### Before you begin

Complete the steps in [Generate New Trustpoint for VeriSign, on page 162](#).

### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to import the certificate onto Cisco Adaptive Security Appliance:

```
crypto ca authenticate trustpoint_name
```

**Step 3** Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----MIIDAzCCAmwCEQC5L2DMiJ+heKYYuFtwbIqvMA0GCSqGSIb3DQEBBQUAMIH...
-----END CERTIFICATE-----
```

```
quit
```

**Note** Finish with the word "quit" on a separate line.

**Step 4** Enter **yes** when you are prompted to accept the certificate.

---

#### What to do next

[Generate Certificate Signing Request, on page 164](#)

## Generate Certificate Signing Request

#### Before you begin

Complete the steps in [Import Root Certificate, on page 163](#).

#### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to send an enrollment request to the CA:

```
(config)# crypto ca enroll trustpoint_name
```

The following warning output displays:

```
%WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems.
```

**Step 3** Enter **yes** when you are prompted to continue with the enrollment.

```
% Start certificate enrollment..% The subject name in the certificate will be: <fqdn>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

**Step 4** Enter **no** when you are prompted to include the device serial number in the subject name.

**Step 5** Enter **yes** when you are prompted to display the certificate request in the terminal.

The certificate request displays.

---

#### What to do next

[Submit Certificate Signing Request to VeriSign, on page 164](#)

## Submit Certificate Signing Request to VeriSign

When you submit the Certificate Signing Request, VeriSign provides you with the following certificate files:

- `verisign-signed-cert.cer` (signed certificate)

- `trial-inter-root.cer` (subordinate intermediate root certificate)
- `verisign-root-ca.cer` (root CA certificate)

Save the certificate files in separate notepad files once you have downloaded them.

### Before you begin

- Complete the steps in [Generate Certificate Signing Request, on page 164](#).
- You must have the challenge password that you defined when generating the Certificate Signing Request.

### Procedure

---

- Step 1** Go to the VeriSign website.
- Step 2** Follow the procedure to enter a Certificate Signing Request.
- Step 3** When prompted, submit the challenge password for the Certificate Signing Request.
- Step 4** Paste the Certificate Signing Request into the window provided.
- Note** You must paste from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` inclusive.
- 

### What to do next

[Delete Certificate Used for Certificate Signing Request, on page 165](#)

## Delete Certificate Used for Certificate Signing Request

You must delete the temporary root certificate used to generate the Certificate Signing Request.

### Before you begin

Complete the steps in [Submit Certificate Signing Request to VeriSign, on page 164](#).

### Procedure

---

- Step 1** Enter configuration mode:
- ```
> Enable
> <password>
> configure terminal
```
- Step 2** Enter this command to display the certificates:
- ```
(config)# show running-config crypto calook for crypto ca certificate chain trustpoint_name
```
- Step 3** Enter this command to delete the certificate:
- ```
(config)# crypto ca certificate chain trustpoint_name
(config-cert-chain)# no certificate ca 00b92f60cc889fa17a4609b85b70$
```

The following warning output displays:

```
WARNING: The CA certificate will be disassociated from this trustpoint and will be removed
if it is not associated with any other trustpoint. Any other certificates issued by this
CA and associated with this trustpoint will also be removed.
```

Step 4 Enter **yes** when you are prompted to delete the trustpoint.

What to do next

[Import Intermediate Certificate, on page 166](#)

Import Intermediate Certificate

Before you begin

Complete the steps in [Delete Certificate Used for Certificate Signing Request, on page 165](#).

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Enter this command to import the certificate onto the Cisco Adaptive Security Appliance:

```
crypto ca authenticate trustpoint_name
```

Step 3 Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----MIIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQU...
-----END CERTIFICATE-----
```

```
quit
```

Note Finish with the word "quit" on a separate line.

Step 4 Enter **yes** when you are prompted to accept the certificate.

What to do next

[Create a Trustpoint for Root Certificate, on page 167](#)

Create a Trustpoint for Root Certificate

Before you begin

Complete the steps in [Import Intermediate Certificate](#), on page 166.

Procedure

- Step 1** Enter configuration mode:
- ```
> Enable
> <password>
> configure terminal
```
- Step 2** Enter this command to generate the trustpoint:
- ```
(config)# crypto ca trustpoint verisign_root
(config-ca-trustpoint)#
```
- Step 3** Enter the following sequence of commands:
- ```
(config-ca-trustpoint)# revocation-check none
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# exit
```
- 

## Import a Root Certificate

### Before you begin

Complete the steps in [Create a Trustpoint for Root Certificate](#), on page 167.

### Procedure

---

- Step 1** Enter configuration mode:
- ```
> Enable
> <password>
> configure terminal
```
- Step 2** Enter this command to import the certificate onto the Cisco Adaptive Security Appliance:
- ```
crypto ca authenticate verisign_root
```
- Step 3** Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----MIIcMCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAw....
-----END CERTIFICATE-----
```

```
quit
```

**Note** Finish with the word “quit” on a separate line.

**Step 4** Enter **yes** when you are prompted to accept the certificate.

---

### What to do next

[Import Signed Certificate, on page 168](#)

## Import Signed Certificate

### Before you begin

Complete the steps in [Import a Root Certificate, on page 167](#).

### Procedure

---

**Step 1** Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

**Step 2** Enter this command to import the certificate onto the Cisco Adaptive Security Appliance:

```
crypto ca import verisignca certificate
```

The following warning output displays:

```
WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems.
```

**Step 3** Enter **yes** when you are prompted to continue with the certificate enrollment.

**Step 4** Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----MIIIFYTCCBEmgAwIBAgIQXtEPGWzZ0b9gejHejq+HazANBgkqhkiG9w0B....
-----END CERTIFICATE-----
```

```
quit
```

**Note** Finish with the word “quit” on a separate line.

**Step 5** Enter **yes** when you are prompted to accept the certificate.

---

**What to do next**

[Import VeriSign Certificates onto Microsoft Access Edge, on page 169](#)

# Import VeriSign Certificates onto Microsoft Access Edge

This procedure describes how to import the VeriSign root and intermediate certificates onto the Microsoft Access Edge server.

**Before you begin**

Save the certificates that were provided by VeriSign to the Access Edge server, for example, in C : \.

**Procedure**

- 
- Step 1** On the Access Edge server, enter `mmc` from the run command.
  - Step 2** Choose **File > Add/Remove Snap-in**.
  - Step 3** Click **Add**.
  - Step 4** Click **Certificates**.
  - Step 5** Click **Add**.
  - Step 6** Choose **Computer account**.
  - Step 7** Click **Next**.
  - Step 8** Choose **Local computer**.
  - Step 9** Click **Finish**.
  - Step 10** To close the **Add/Remove Snap-In** window., click **OK**.
  - Step 11** In the main console, expand the Certificates tree.
  - Step 12** Open the **Trusted Root Certificates** branch.
  - Step 13** Right-click on **Certificates**.
  - Step 14** Choose **All Tasks > Import**.
  - Step 15** Click **Next** on the certificate wizard.
  - Step 16** Browse for a VeriSign certificate in the C : \ directory.
  - Step 17** Click **Place all certificates in the following store**.
  - Step 18** As the certificate store, choose **Trusted Root Certification Authorities**.
  - Step 19** Repeat steps 13 to 18 to import the additional VeriSign certificates.
-





# CHAPTER 21

## Integration Debugging Information

- [Debugging Information for the Cisco Adaptive Security Appliance, on page 171](#)
- [Access Edge and OCS Server Debugging, on page 175](#)

### Debugging Information for the Cisco Adaptive Security Appliance

#### Cisco Adaptive Security Appliance Debugging Commands

The following table lists the debugging commands for the Cisco Adaptive Security Appliance.

*Table 20: Cisco Security Appliance Debugging Commands*

| To                                                                                                                                                                          | Use the Command                           | Notes                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show ICMP packet information for pings to the Cisco Adaptive Security Appliance interfaces                                                                                  | <code>debug icmp trace</code>             | We strongly recommend that you disable debug messages once you have completed your troubleshooting. To disable ICMP debug messages, use the <code>no debug icmp trace</code> command. |
| Show messages relating to the certificate validation between IM and Presence Service/Cisco Adaptive Security Appliance or Cisco Adaptive Security Appliance/external domain | <code>debug crypto ca</code>              | You can increase log level on the Cisco Adaptive Security Appliance by adding the log level parameter to this command, for example:<br><br><code>debug crypto ca 3</code>             |
|                                                                                                                                                                             | <code>debug crypto ca messages</code>     | Displays only debug messages for input and output messages                                                                                                                            |
|                                                                                                                                                                             | <code>debug crypto ca transactions</code> | Displays only debug messages for transactions                                                                                                                                         |

| To                                                                   | Use the Command                                     | Notes                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show the SIP messages sent through Cisco Adaptive Security Appliance | <code>debug sip</code>                              |                                                                                                                                                                                                                                                                                                   |
| Send log messages to a buffer (for later viewing)                    | <code>terminal monitor</code>                       |                                                                                                                                                                                                                                                                                                   |
| Enable system log messages                                           | <code>logging on</code>                             | We strongly recommend that you disable system log messages once you have completed your troubleshooting. To disable system log messages, use the <code>no logging on</code> command.                                                                                                              |
| Send system log messages to a buffer                                 | <code>logging buffer debug</code>                   |                                                                                                                                                                                                                                                                                                   |
| Set system log messages to be sent to Telnet or SSH sessions         | <code>logging monitor debug</code>                  |                                                                                                                                                                                                                                                                                                   |
| Designate a (syslog) server to receive the system log messages       | <code>logging host interface_name ip_address</code> | <ul style="list-style-type: none"> <li>• The <code>interface_name</code> argument specifies the Cisco Adaptive Security Appliance interface through which you access the syslog server.</li> <li>• The <code>ip_address</code> argument specifies the IP address of the syslog server.</li> </ul> |

| To                                                                            | Use the Command            | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ping the Interfaces                                                           | <code>ping</code>          | Refer to the Troubleshooting section of the <i>Cisco Security Appliance Command Line Configuration Guide</i> for details on pinging the Cisco Adaptive Security Appliance interfaces, and also pinging between hosts on different interfaces to ensure that the traffic can pass successfully through the Cisco Adaptive Security Appliance.<br><br>You can also ping an interface in ASDM by choosing <b>Tools &gt; Ping</b> .<br><br><b>Note</b> You cannot ping the public IM and Presence Service IP address. However the MAC address of the Cisco Adaptive Security Appliance outside interface should appear in the ARP table ( <code>arp -a</code> ). |
| Trace the route of a packet                                                   | <code>tracert</code>       | You can also trace the route of a packet in ASDM, choose <b>Tools &gt; Traceroute</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Trace the life span of a packet through the Cisco Adaptive Security Appliance | <code>packet-tracer</code> | You can also trace the life span of a packet in ASDM, choose <b>Tools &gt; Packet Tracer</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Related Topics**

[TLS Proxy Debugging Commands](#), on page 174

## Capture Output on Internal and External Interfaces

**Procedure**

- 
- Step 1** Enter configuration mode:
- > `Enable`
  - > `<password>`
  - > `configure terminal`

- Step 2** Define an access-list to specify the traffic to be captured, for example:
- ```
access-list cap extended permit ip 10.53.0.0 255.255.0.0 10.53.0.0 255.255.0.0
```
- Step 3** It is recommended that you clear the capture content before starting the tests. Use the command “clear capture in” to clear the internal interface capture, and the command “clear capture out” to clear the external interface capture.
- Step 4** Enter this command to capture the packets on the internal interface:
- ```
cap in interface inside access-list cap
```
- Step 5** Enter this command to capture the packets on the external interface:
- ```
cap out interface outside access-list cap
```
- Step 6** Enter this command to capture TLS specific packets:
- ```
capture capture_name type tls-proxy interface interface_name
```
- Step 7** Enter this command to retrieve the packet capture:
- ```
copy /pcap capture:in tftp://xx.xx.xx.xx copy /pcap capture:out tftp://xx.xx.xx.xx
```
- Enter this command to copy the output to disk and retrieve using ASDM (choose **Actions > File Management > File Transfer**):
- ```
copy /pcap capture:in disk0:in_1
```

## TLS Proxy Debugging Commands

The following table lists the debugging commands for the TLS Proxy.

*Table 21: TLS Proxy Debugging Commands*

| To                                                                                                                                                                                                  | Use the Command(s)                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Enable TLS proxy-related debug and syslog output                                                                                                                                                    | <pre>debug inspect tls-proxy events debug inspect tls-proxy errors debug inspect tls-proxy all</pre> |
| Show a TLS proxy session output                                                                                                                                                                     | <pre>show log</pre>                                                                                  |
| Check the active TLS proxy sessions                                                                                                                                                                 | <pre>show tls-proxy</pre>                                                                            |
| View the detail of the current TLS proxy sessions<br>(Use when the Cisco Adaptive Security Appliance successfully establishes connections with the IM and Presence Service and the external domain) | <pre>show tls-proxy session detail</pre>                                                             |

# Access Edge and OCS Server Debugging

## Initiate Debug Session on OCS/Access Edge

### Procedure

---

- Step 1** On the external Access Edge server, choose **Start > Administrative Tools > Computer Management**.
  - Step 2** In the left pane, right-click **Microsoft Office Communications Server 2007**.
  - Step 3** Choose **Logging Tool > New Debug Session**.
  - Step 4** In the Logging Options, choose **SIP Stack**.
  - Step 5** For the Level value, choose **All**.
  - Step 6** Click **Start Logging**.
  - Step 7** When complete, click **Stop Logging**.
  - Step 8** Click **Analyze Log Files**.
- 

## Verify DNS Configuration on Access Edge

### Procedure

---

- Step 1** On the external Access Edge server, choose **Start > Administrative Tools > Computer Management**.
  - Step 2** Right-click on **Microsoft Office Communications Server 2007** in the left pane.
  - Step 3** Choose the **Block** tab.
  - Step 4** Check that none of the IM and Presence Service managed domains are blocked.
  - Step 5** Ensure that the following options are selected in the **Access Methods** pane:
    - a) Federate with other domains
    - b) Allow discovery of federation partners
  - Step 6** Check the Access Edge is publishing DNS SRV records.
-

