Cisco Jabber and Microsoft Lync Interoperability

Infrastructure Configuration Cheatsheet

First Published: June 2016

Last Updated: August 2017

Cisco Expressway X8.9

Cisco Unified Communications Manager 10.x or later

Microsoft Lync Server 2010 or 2013

Cisco Unified Communications Manager IM & Presence 10.x or later

Contents

Preface 3
- Change History 3

Introduction 4
- Required Versions 4
- Related Documents 4

Configuration 5
- Task 1: Prepare Expressway-C for Microsoft Interoperability 7
- Task 2: Create a SIP TLS Trunk Between Cisco Unified Communications Manager and Expressway-C 8
- Task 3: Configure Microsoft Front End Server to Trust Expressway-C 9
- Task 4: Configure Microsoft Interoperability on Expressway-C 10
- Milestone 1: Test Calls From Cisco Jabber to Microsoft Client 11
- Task 5: Configure Expressway-C to Route Calls From Microsoft Hosts 12
- Task 6: Create Static SIP Route From Microsoft FE Server 13
- Milestone 2: Test Calls From Microsoft Client to Cisco Jabber 14
- Task 7: Configure Expressway-C to Filter Chat and Presence 15
- Task 8: Create Static Route, Update Incoming ACL, and Create TLS Peer Subjects 16
- Task 9: Configure the TLS Peer Context 17
- Task 10: Configure Microsoft Front End Server to Trust IM and Presence Service Publishers 18
- Milestone 3: Test Chat and Presence Between Microsoft and Jabber Clients 19

Cisco Legal Information 20

Cisco Trademark 20

Preface

Change History

Table 1 Infrastructure Configuration Cheatsheet Change History

Date	Change	Reason
August 2017	Updated	Added note that SIP broker requires TLS and therefore IM and Presence Service restricted version is required.
December 2016	Updated	Added note on need to change Default Cisco SIP Proxy TLS Listener port values on IM and Presence Service.
July 2016	Updated	Corrected configuration of application pools for IM and Presence Service. Retitled to remove reference to Skype for Business. Reinforced that this document is not for B2B deployments.
June 2016	New document	Expressway X8.8 enables chat and presence integration between MS Lync Server and Cisco IM and Presence Service.

Introduction

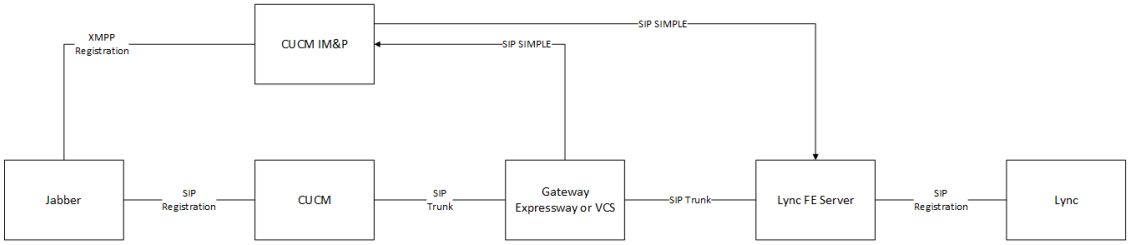
Our goal in this configuration is to get Cisco Jabber communicating with Microsoft clients. All clients are assumed to be in the network (on-premises) and registering using the same domain. **This deployment is not intended for business to business integration.**

This configuration assumes you already have Jabber clients communicating with each other, and Microsoft clients communicating with each other.

Figure 1 Before this process:

We're going to use a dedicated Expressway-C to connect the infrastructure elements. This will enable video calls, instant messaging, and presence between Jabber and Lync clients.

Figure 2 After this process:



Required Versions

- Cisco Unified Communications Manager 10.x or later
- Cisco Unified Communications Manager IM and Presence Service 10.x or later
- Expressway X8.8 or later
- Microsoft Lync Server 2010, Lync Server 2013, or Skype for Business Server 2015

Note: SIP broker requires TLS which is not available in the unrestricted version of IM and Presence Service. To use this feature, Cisco Unified Communications Manager IM and Presence Service restricted version is required.

Related Documents

- See *Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page.
- See the *Security Configuration* chapter of *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*, for your version, at the CUCM IM&P Configuration Guides page.
- See *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*, for your version, at the CUCM IM&P Configuration Guides page.
- See the Lync Server 2013 cmdlets index at TechNet.

Configuration

Table 2 Configuration Overview

Task	Expressway-C	Cisco Unified Communications Manager	Microsoft FE Server	Cisco Unified Communications Manager IM and Presence Service
1	Task 1: Prepare Expressway-C for Microsoft Interoperability, page 7			
2		Task 2: Create a SIP TLS Trunk Between Cisco Unified Communications Manager and Expressway-C, page 8		
3			Task 3: Configure Microsoft Front End Server to Trust Expressway-C, page 9	
4	Task 4: Configure Microsoft Interoperability on Expressway-C, page 10			
Milestone 1: Test Calls From Cisco Jabber to Microsoft Client, page 11				
5	Task 5: Configure Expressway-C to Route Calls From Microsoft Hosts, page 12			
6			Task 6: Create Static SIP Route From Microsoft FE Server, page 13	
Milestone 2: Test Calls From Microsoft Client to Cisco Jabber, page 14				
7	Task 7: Configure Expressway-C to Filter Chat and Presence, page 15			
8				Task 8: Create Static Route, Update Incoming ACL, and Create TLS Peer Subjects, page 16

Table 2 Configuration Overview (continued)

Task	Expressway-C	Cisco Unified Communications Manager	Microsoft FE Server	Cisco Unified Communications Manager IM and Presence Service
9				Task 9: Configure the TLS Peer Context, page 17
10			Task 10: Configure Microsoft Front End Server to Trust IM and Presence Service Publishers, page 18	
Milestone 3: Test Chat and Presence Between Microsoft and Jabber Clients, page 19				

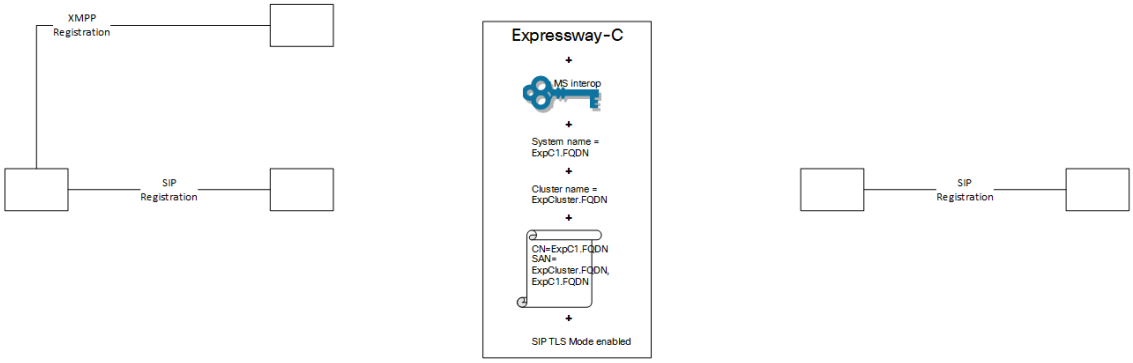
Task 1: Prepare Expressway-C for Microsoft Interoperability

1. Install the Expressway-C and configure it for networking.

   When adding IP addresses, make sure to also give it local DNS and NTP servers that are used by the other infrastructure elements in this deployment.

   - *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page.
   - *Cisco Expressway CE1100 Appliance Installation Guide* on the Expressway installation guides page.
2. Sign in to the web interface and follow the service setup wizard to get Expressway-C licensed for the Microsoft Interoperability service.
3. Give the Expressway-C a system name and a cluster name, even if it is not going to be part of a cluster.
4. Install a server certificate that has the peer FQDN as common name and has the cluster FQDN and peer FQDN as SANs. The certificate's signing authority must be trusted by the other infrastructure elements.
5. [Optional] Repeat the previous sequence on up to 5 more Expressway-Cs and then cluster them.
6. Enable SIP TLS mode.

Figure 3 Prepare the Expressway-C for Microsoft Interoperability



Task 2: Create a SIP TLS Trunk Between Cisco Unified Communications Manager and Expressway-C

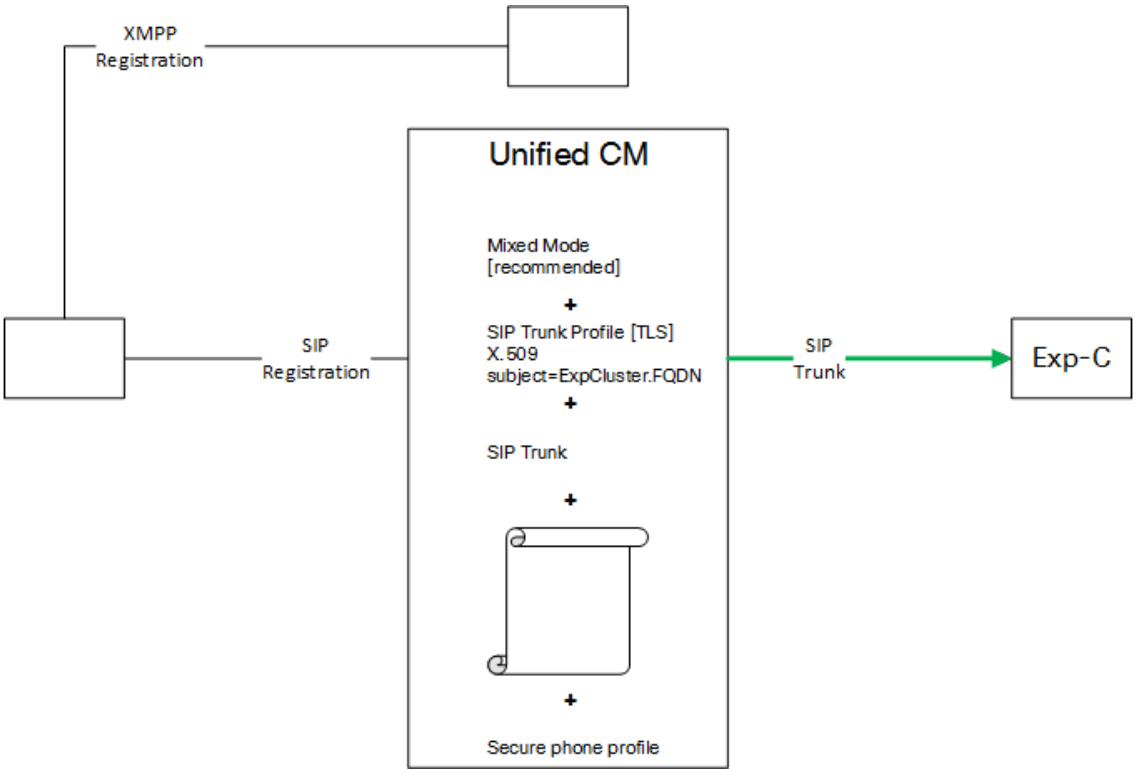
1. Put the CUCM in Mixed Mode and check its basic configuration.

   We recommend using TLS to secure all connections in this deployment. However, you can choose to leave Unified CM in Non Secure mode, and create a TCP trunk towards Expressway-C.

   In this case, you must configure the Expressway-C to encrypt/decrypt on behalf of Unified CM, because the rest of the deployment mandates TLS.
2. Install a server certificate that is signed by a CA trusted by the other infrastructure elements.
3. Configure a SIP trunk security profile with these parameters:

   Incoming and outgoing transports = TLS, inbound port = 5061, device security mode = encrypted, accept unsolicited notification checked, accept replaces header checked, X.509 subject = Expressway-C cluster FQDN.
4. Create a new SIP trunk that uses the security profile you just created and trunks to destination port 5061.
5. Make sure that Jabber is using a secure phone profile (the profile must have Device Security Mode = Encrypted).

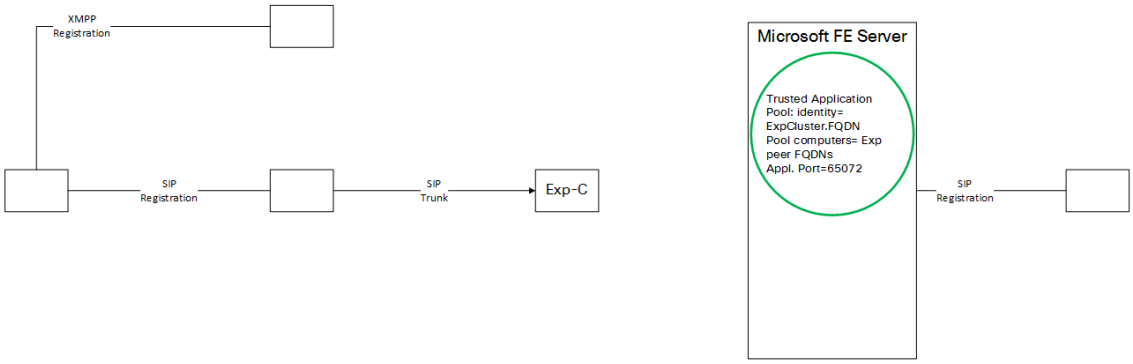
Figure 4 Create a Trunk to Expressway-C



Task 3: Configure Microsoft Front End Server to Trust Expressway-C

1. Create a trusted application pool with identity of the Expressway-C (cluster FDQN)
2. If it's a cluster of Expressway-Cs, add a new trusted application computer to the pool for each of the peer FQDNs.
3. Assign a new trusted application to the pool. Give the application the trusted application's FQDN (Expressway-C cluster FQDN) and its destination port (65072).
4. Check that the signing CA of the FE Servers' certificates is trusted by the Expressway-C and by the IM and Presence Service nodes.
5. Check that the signing CA of the Expressway-C peers' certificates is trusted by the Microsoft FE servers.
6. Enable the topology.

Figure 5 Create Application Pool For Expressway-C Trusted Application



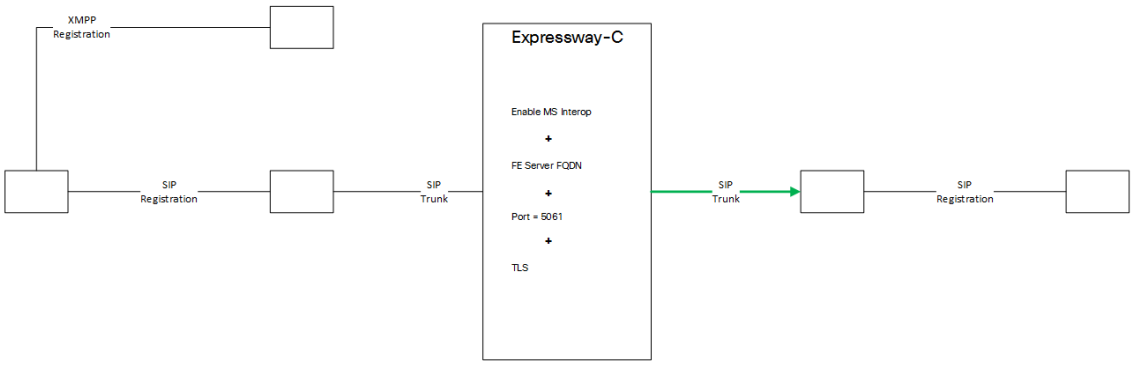
Task 4: Configure Microsoft Interoperability on Expressway-C

1. Enable Microsoft Interoperability on the Expressway-C (primary)
2. Enter the Microsoft Front End Server's address, the listening port, and set the transport to TLS.

   When you save this configuration, the Expressway-C creates a new zone towards the Microsoft Front End Server.
3. If necessary, create a transform to strip the port off the destination alias that comes from CUCM.
4. Create a search rule that matches incoming calls destined for Microsoft clients and route them to the new Microsoft Interoperability zone.

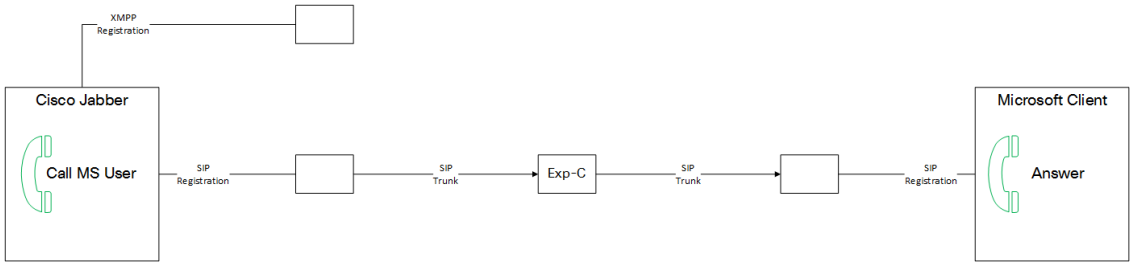
   Eg. CUCM zone > MSuser1@example.com:5063 > transform > MSuser1@example.com > search rule > MS interop zone.

Figure 6 Create Trunk From Expressway-C to Microsoft FE Server



Milestone 1: Test Calls From Cisco Jabber to Microsoft Client

Figure 7 Test SIP Call From Cisco Jabber to Microsoft Client



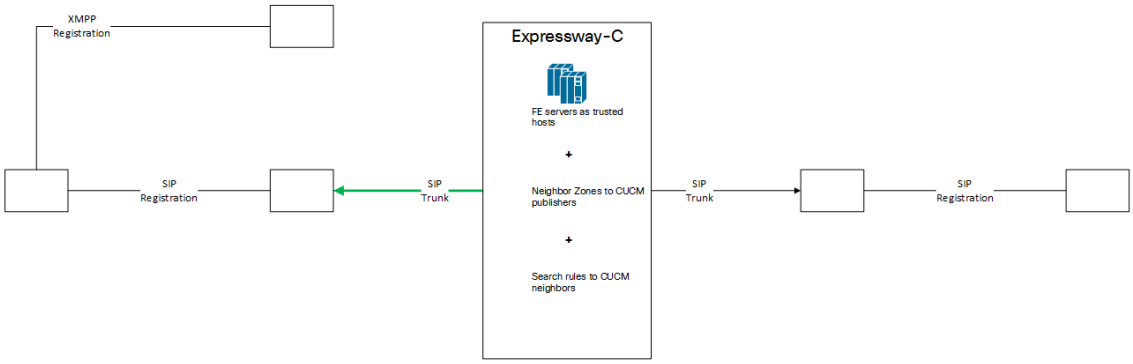
1. Cisco Jabber user makes call to known alias in the Microsoft client's domain.
2. CUCM routes the call on the trunk to Expressway-C.
3. Expressway-C receives call on CUCM neighbor zone, transforms destination string if necessary, and routes on neighbor zone to FE Server.
4. FE server receives call from trusted application and routes it to the destination alias.
5. Microsoft client answers.

Task 5: Configure Expressway-C to Route Calls From Microsoft Hosts

1. On the Expressway-C (primary), add a trusted host for each Microsoft Server that will route towards Expressway-C.
2. Create a neighbor zone to each CUCM with these parameters:

   Port = 5061, Transport = TLS enabled, TLS verify mode = On, Authentication trust mode = Off.
3. Create search rules to route calls from Microsoft Interoperability zone to CUCM zones.

Figure 8 Configure Routing From Microsoft Trusted Hosts To CUCM Neighbors



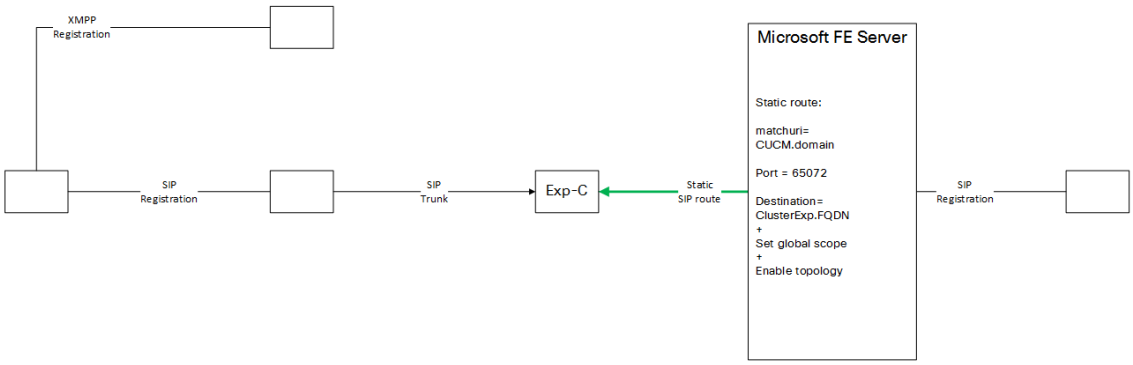
Task 6: Create Static SIP Route From Microsoft FE Server

1. Create a new static TLS route with the following parameters:

   MatchURI = CUCM domain (same as MS domain), port = 65072, destination = Expressway-C cluster FQDN, use default certificate = true.
2. Assign the route to the global routing configuration.
3. Enable the topology.

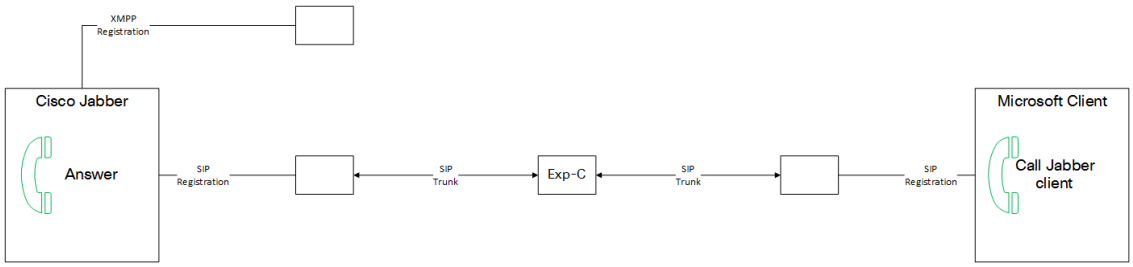
Note: When the domain is the same, the Microsoft FE Servers will only use the global static route if they can't find a Microsoft-registered client with a matching alias.

Figure 9 Create Global Static Route From FE Server to Expressway-C Cluster



Milestone 2: Test Calls From Microsoft Client to Cisco Jabber

Figure 10 Test SIP Call From Microsoft Client to Cisco Jabber



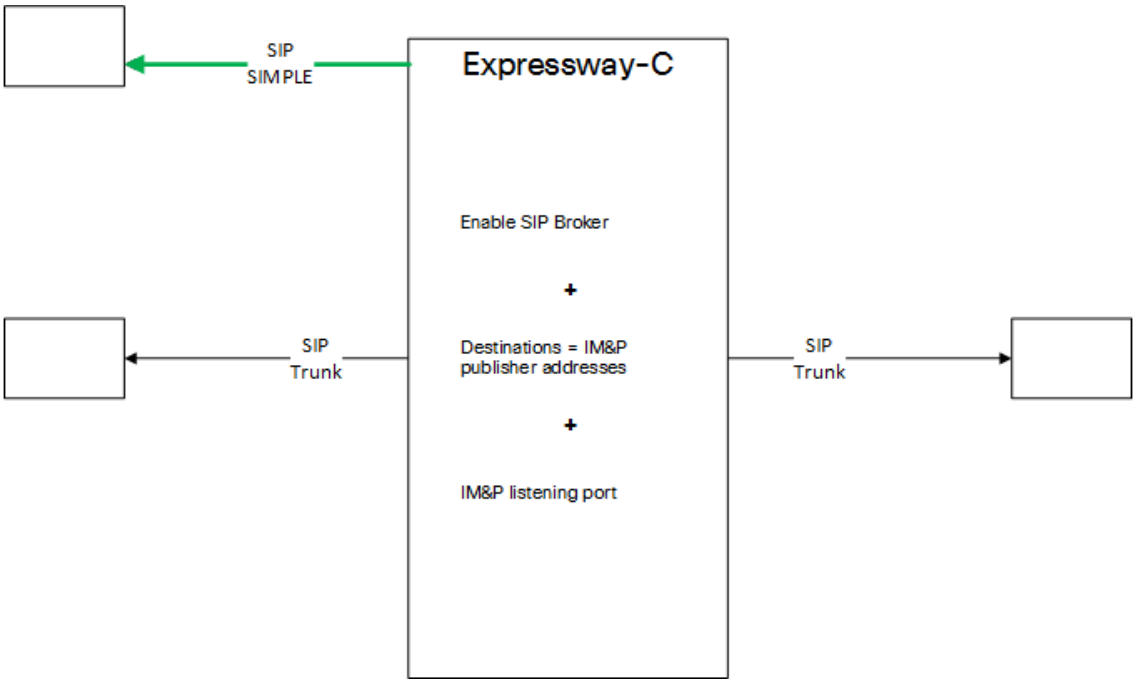
1. Microsoft user makes call to known alias in the Jabber client's domain.
2. FE server does not find the alias locally and routes the call on the static route to Expressway-C.
3. Expressway-C receives call on Microsoft interoperability zone, transforms destination string if necessary, and routes on neighbor zone to CUCM.
4. CUCM receives call on trunk from Expressway-C and routes it to the destination alias.
5. Jabber client answers.

Task 7: Configure Expressway-C to Filter Chat and Presence

1. Enable the SIP broker.
2. Enter the FQDNs of the IM&P nodes and the listening port.

Note: You must change the Default Cisco SIP Proxy TLS Listener port values for both server authentication and peer authentication on IM and Presence Service. It performs peer (mutual) TLS authentication on port 5062 by default. You must modify this default setting so that peer TLS authentication takes place on port 5061 and configure the server TLS authentication port value to 5062. See the Node Configuration for Partitioned Intradomain Federation chapter of *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*, for your version, at the CUCM IM&P Configuration Guides page.

Figure 11 Enable SIP Broker to Send SIP SIMPLE to IM and Presence Service



Task 8: Create Static Route, Update Incoming ACL, and Create TLS Peer Subjects

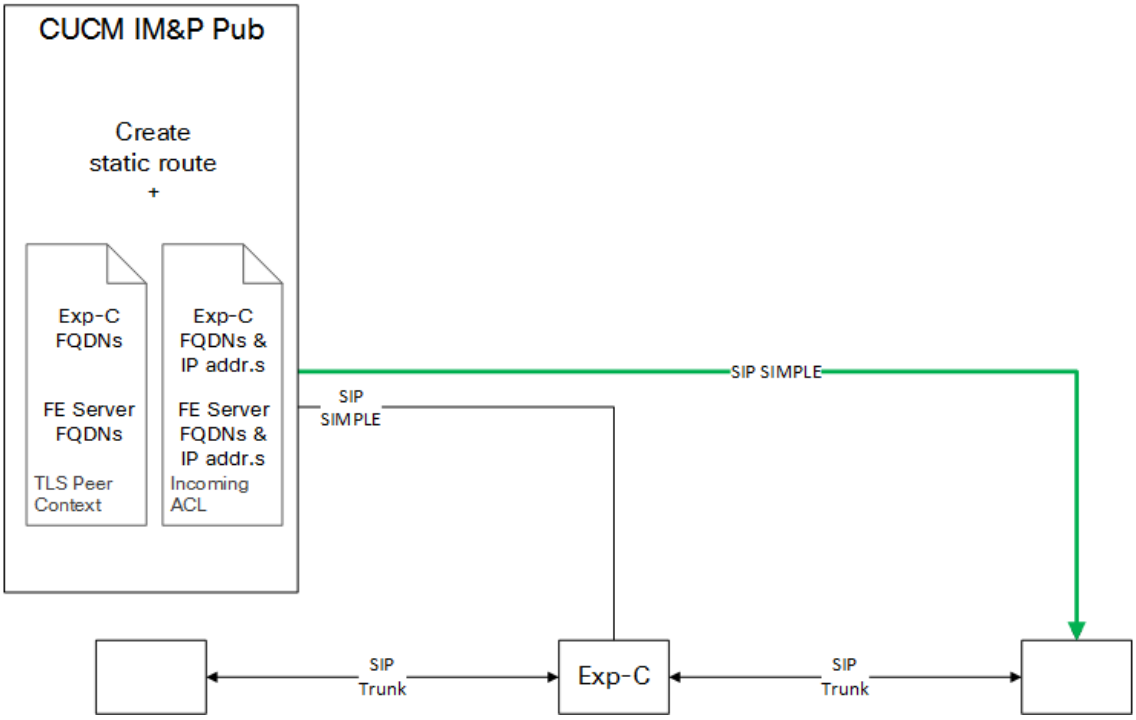
On each publisher node:

1. Configure a cluster-wide static route to carry IM&P traffic to Microsoft FE Server.
2. Add all Expressway-C peers' FQDNs as new TLS Peer Subjects.
3. Add all Expressway-C peers' IP addresses and FQDNs to the Incoming ACL.
4. Add all Front End servers' FQDNs as new TLS Peer Subjects.
5. Add all Front End servers' IP addresses and FQDNs to the Incoming ACL.

Task 9: Configure the TLS Peer Context

1. In Cisco Unified CM IM and Presence Administration, go to **System > Security > TLS Context Configuration**.
2. Click **Find**.
3. Choose *Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context*.
4. From the list of available TLS peer subjects, choose the TLS peer subjects that you configured for the Expressways and Microsoft FE Servers.
5. Move the chosen entries over to the **Selected TLS Peer Subjects**.
6. [For IM and Presence Service 11.x] In the **TLS Cipher Mapping** pane, remove the ECDHE_ECDSA ciphers from the Selected TLS Ciphers list.
7. Click **Save**.
8. Restart the SIP Proxy service.

Figure 12 Static Route and Trust Configuration on IM and Presence Service

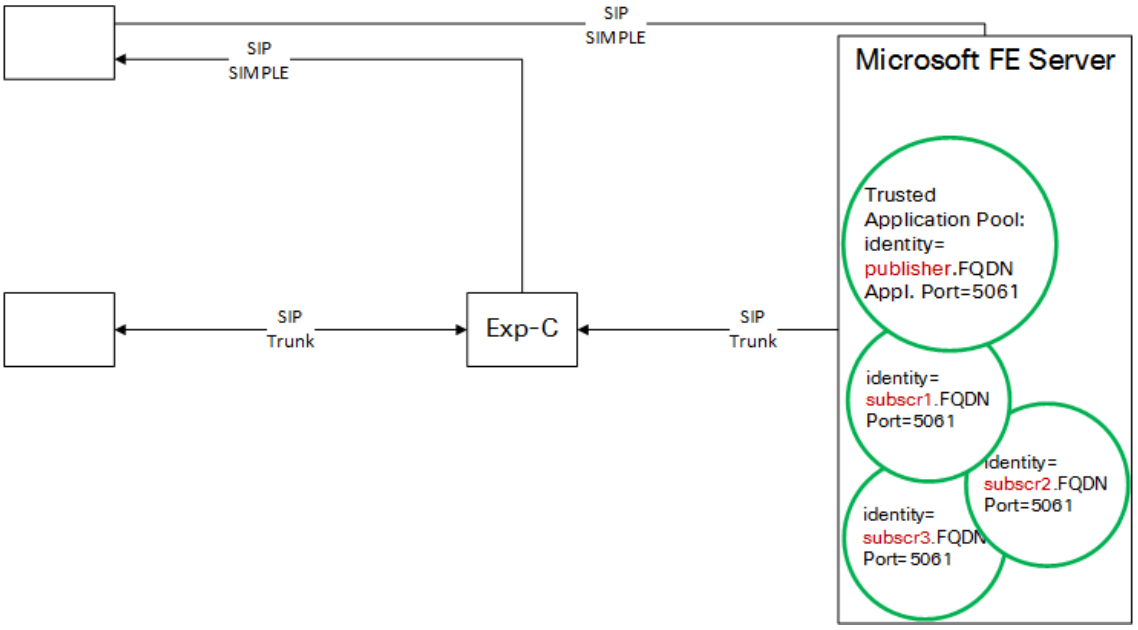


Task 10: Configure Microsoft Front End Server to Trust IM and Presence Service Publishers

You need to create a trusted application on FE server for each IM and Presence Service node.

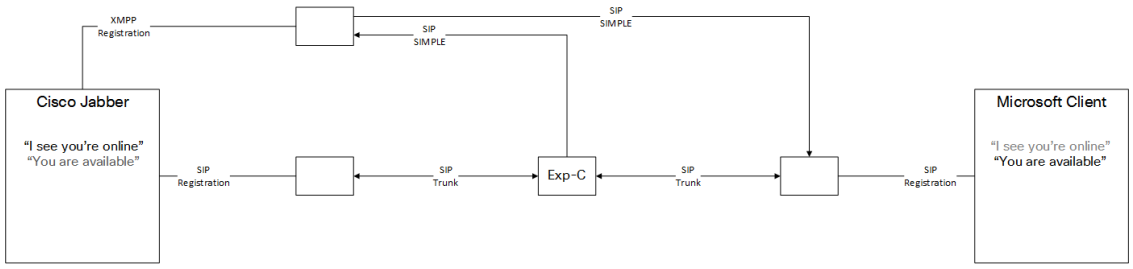
1. Create a trusted application pool with identity parameter equal to the IM and Presence Service node's FQDN.
2. Assign a new trusted application to the pool. Give the application the trusted pool's identity (=the node's FQDN) and its destination port (typically 5061).
3. Check that the signing CA of the IM and Presence Service node's certificate is trusted by the Microsoft FE servers.
4. Repeat this task for every IM and Presence Service node (publishers and subscribers).
5. Enable the topology.

Figure 13 Create Application Pool For IM and Presence Service Trusted Application



Milestone 3: Test Chat and Presence Between Microsoft and Jabber Clients

Figure 14 Test Chat and Presence Between Jabber and Microsoft Client



1. Jabber user opens chat to known Microsoft alias.
2. IM and Presence Service node interworks XMPP to SIP SIMPLE and routes it on static route to FE server
3. Microsoft user answers chat.
4. All Microsoft traffic goes to the Expressway-C
5. The SIP broker routes the SIP SIMPLE to the IM and Presence Service node.
6. IM and Presence Service routes the chat to the requested Jabber alias.
7. Presence status updates follow the same paths.

Cisco Legal Information

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

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

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

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

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)