



# **Administering Avaya Aura<sup>®</sup> Presence Services**

Release 6.2.4  
Issue 3  
June 2014

© 2014 Avaya Inc.

All Rights Reserved.

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed, or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

## License types

**Designated System(s) License (DS).** End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

**Concurrent User License (CU).** End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

**Database License (DL).** End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

**CPU License (CP).** End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

**Named User License (NU).** You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

**Shrinkwrap License (SR).** You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

## Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment.

Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

### **Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

### **Virtualization**

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

### **Third Party Components**

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Certain software programs or portions thereof included in the Product are open-source products. The Open Source license file, OpenSourceLicense.txt, is available in the Licenses folder on the Presence Services server: /Licenses/OpenSourceLicense.txt

### **Preventing Toll Fraud**

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### **Avaya Toll Fraud intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

### **Trademarks**

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and one-X are registered trademarks and Avaya Aura is a trademark of Avaya, Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

### **Contact Avaya Support**

See the Avaya Support website: <http://support.avaya.com> for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

<b>Chapter 1: Introduction</b> .....	9
Purpose.....	9
Intended audience.....	9
Document changes since last issue.....	9
Related resources.....	10
Documentation.....	10
Training.....	11
Viewing Avaya Mentor videos.....	11
Support.....	12
<b>Chapter 2: Presence Services overview</b> .....	13
New in this release.....	13
Key features of Presence Services.....	13
Overview.....	14
Components of the Presence Services system.....	15
External entities.....	16
Other Avaya applications.....	16
Configuration views.....	17
Areas on the Controller's main page.....	18
The System area.....	18
The Router area.....	18
Components area.....	19
Restarting the system.....	19
<b>Chapter 3: Administering System Manager for Presence Services</b> .....	21
System Manager and Presence Services.....	21
Viewing the details of the Presence server on System Manager .....	22
Viewing the status of the Presence server on System Manager.....	23
Presence configuration properties.....	23
Administering Presence configuration properties.....	23
User configuration in System Manager.....	24
Configuring System Manager to enable Presence and IM services.....	24
Creating SIP routing domains.....	25
Assigning an Avaya Presence/IM communication address to a user.....	26
Presence Profile.....	27
Assigning a Communication Profile Password to a user.....	32
Disabling cross-domain communication.....	32
Licensing.....	33
Presence Services license renewal.....	33
Renewing your Presence Services license.....	34
Presence Services Admin status check.....	35

presstatus.....	35
Using the Interactive Mode.....	35
Using the Command line mode.....	36
Example output.....	36
Status description.....	38
Exporting and importing bulk users.....	39
Bulk import and export.....	39
Bulk import and export using the Excel file.....	39
Bulk importing of users.....	40
Exporting users in bulk using CLI.....	42
<b>Chapter 4: Integrating Presence Services with Session Manager.....</b>	<b>43</b>
Overview of Session Manager with Presence Services.....	43
Adding Session Manager to Presence Services.....	43
Verifying the hostname in the Presence Session Manager .....	44
Adding Presence Services as a SIP entity in System Manager.....	45
Adding an entity link.....	46
Avaya SIP Client(s) support.....	47
Enabling required modules in Presence Session Manager.....	48
<b>Chapter 5: Configuring Presence Services components.....</b>	<b>49</b>
Managing Presence components.....	49
Presence components.....	49
Adding Presence components.....	49
Removing Presence components.....	49
Configuring Presence Components.....	50
AES Collector.....	50
Adding Microsoft OCS/Lync SIP user handles to System Manager.....	57
SIP Proxy Configuration.....	58
Microsoft Exchange Collector integration.....	60
Domino Collector integration.....	75
IM Transcript Web service.....	98
Connection Manager configuration.....	101
Connection Manager parameter reference.....	106
Connection configuration for an IM client.....	110
HTTP binding director configuration.....	112
Polling Connection configuration.....	114
S2S Command Processor Parameter Reference.....	121
Discovery protocol for querying the S2S Command Processor.....	125
Configuring Authorization ACLs on System Manager.....	127
Adding other presentities to the resource list of a user.....	128
Multiuser chat.....	129
<b>Chapter 6: Presence Services federation with third-party servers.....</b>	<b>134</b>
Overview.....	134
Overview of user configuration in System Manager.....	135

Watcher and Presentity.....	135
Aura watcher and federated presentity behaviors.....	136
user-default-policy-domain.sh ACL script.....	139
Aura or federated watcher and PC3 presentity.....	140
Federated user and Avaya Aura® presentity.....	140
XMPP federation.....	141
Overview – XMPP federation.....	141
XMPP Federation Configuration.....	143
Troubleshooting.....	157
XMPP Federation with Presence Services Cluster.....	159
Checklist for configuring XMPP federation for a Presence Services cluster.....	159
Configuring DNS.....	159
Adding Router-to-Router connection.....	161
Configuring the federation domain.....	163
Adding the S2S component.....	163
Adding the OpenPort component.....	164
OCS Gateway.....	165
Introduction.....	165
Presence Services multi-domain support with Lync federation.....	169
Integrating OCS Gateway.....	169
Trust Management and DNS Administration.....	184
Troubleshooting.....	203
Lync federation with Presence Services cluster using Session Manager as edge server.....	206
Federation between Avaya Aura® domains.....	224
Checklist for configuring federation between Avaya Aura® domains.....	224
Enabling rich Presence.....	225
<b>Chapter 7: Maintenance Operations.....</b>	<b>227</b>
Presence commands.....	227
Quick reference commands.....	227
backup.sh tool.....	229
restore.sh tool.....	230
prescert tool.....	232
swversion.sh tool.....	234
getpslogs.sh tool.....	235
changelP.sh tool.....	235
updateLogLevel.sh tool.....	236
watchers.sh tool.....	237
configureNMS.sh tool.....	238
generateTestAlarm.sh tool.....	240
Using the setProductID.sh tool.....	241
Using the getProductID.sh tool.....	241
im_manager.sh tool.....	241
Error Levels.....	245

Changing the System Manager hostname on Presence Services.....	246
Updating Presence Services entity link in Session Manager.....	246
Updating client configuration.....	247
Monit.....	247
Viewing monit using a CLI.....	249
Suspending and restarting the monitoring of a service.....	249
Checking your Presence Services license status.....	249
Network parameters.....	250
Network parameters overview.....	250
Configuring network parameters .....	250
Checking the outcome of the changed network parameters.....	259
Configuring network parameters on the non-System Platform deployments.....	259
Certificate configuration.....	265
Refreshing Presence Services certificates for System Manager .....	265
Creating new certificates in the Presence server.....	265
<b>Appendix A: Access Control Lists.....</b>	<b>266</b>
ACL scripts.....	266
presuseracls tool.....	266
User default ACL policy script.....	269
User default policy domain ACL script.....	270
Access Levels.....	271
Presence access levels.....	271
Defining rules.....	272
Filtering.....	272
Soliciting confirmation.....	272
Presence access levels in System Manager.....	273
Viewing presence access levels.....	273
Creating Presence access levels.....	273
Modifying presence access levels.....	273
Deleting Presence access levels.....	274
Presence ACL field descriptions.....	274
<b>Appendix B: Configuring users in System Manager to enable Presence and Instant Messaging.....</b>	<b>275</b>
Communications address terminology.....	275
Network login.....	276
Configuring Users.....	276
Adding contacts.....	277
Presence and Instant Messaging.....	278
<b>Appendix C: Configuring the Presence Services server for Avaya one-X<sup>®</sup> Client Enablement Services.....</b>	<b>285</b>
<b>Appendix D: CS 1000 with Presence Services.....</b>	<b>287</b>
Creating a subscriber.....	287
CS 1000 Presence publisher.....	288

Configuring Presence publisher.....	289
<b>Appendix E: Presence Services field descriptions.....</b>	<b>291</b>
<b>Appendix F: Sample deployment configurations.....</b>	<b>300</b>
OCS Gateway configuration worksheet.....	300
<b>Appendix G: Process flow of a SIP Subscribe.....</b>	<b>301</b>
The SIP OCS Gateway component.....	301
Inbound requests.....	301
Outbound requests.....	301
Initiating a SIP SUBSCRIBE from the OCS server to Presence Services .....	303
Initiating an IM conversation from Presence Services to the OCS server .....	306
Initiating an IM conversation from the OCS server to Presence Services.....	307
<b>Appendix H: Configuration parameters and references .....</b>	<b>308</b>
SIP Proxy parameter reference.....	308
SIP Proxy basic parameters.....	308
<b>Appendix I: Presence Services cluster solution overview.....</b>	<b>315</b>
Presence Services cluster configuration.....	315
Configuring the Router-to-Router component.....	315
Sample R2R configuration.....	316
Verifying the jsMLD and SIP entity of Presence Services.....	318
User provisioning.....	318
<b>Appendix J: Known Issue – Configuring Presence Server as the Exchange Server URL in the XCP configuration.....</b>	<b>319</b>
<b>Glossary.....</b>	<b>320</b>

# Chapter 1: Introduction

---

## Purpose

This document provides procedures for configuring Avaya Aura® Presence Services Release 6.2.

---

## Intended audience

The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining, and verifying Presence Services at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

---

## Document changes since last issue

The following changes have been made to this document since the last issue:

- Updated the topic [New in this release](#) on page 13 to include the updates of Presence Services Release 6.2.
- Updated the topic [Other Avaya applications](#) on page 16 to include the latest version of the products.
- Added the topic [User configuration in System Manager](#) on page 24.
- Added the topic [Configuring System Manager to enable Presence and IM services](#) on page 24.
- Added the section [Domino Collector integration](#) on page 75.
- Added the chapter [Presence Services federation with third-party servers](#) on page 134.
- Added the topic [Overview of user configuration in System Manager](#) on page 135.
- Added the topic [Watcher and Presentity](#) on page 135.
- Added the topic [Aura watcher and federated presentity behaviors](#) on page 136.
- Added the topic [user-default-policy-domain.sh ACL script](#) on page 139.
- Added the topic [Running the user-default-policy-domain.sh ACL script](#) on page 139.

- Added the topic [Aura or federated watcher and PC3 presentity](#) on page 140.
- Added the topic [Federated user and Avaya Aura presentity](#) on page 140.
- Added the topic [Presence Services multi-domain support with Lync federation](#) on page 169.
- Added the section [Lync federation with Presence Services cluster using Session Manager as edge server](#) on page 206.
- Added the section [Federation between Avaya Aura domains](#) on page 224.
- Added the topic [User default policy domain ACL script](#) on page 270.

---

## Related resources

---

## Documentation

Document number	Title	Use this document to:	Audience
Implementing			
-	<i>Deploying Avaya Aura® Presence Services</i>	Install Presence Services and for information about High Availability.	The audience is expected to have some experience installing Avaya products and performing administration procedures.
Supporting			
-	Avaya Aura® Core Solution Description	Know about the Avaya Aura® components.	This document is intended for people who want to understand how the solution and related verified reference configurations meet customer requirements.
Administering			
-	<i>Administering Avaya Aura® System Manager</i>	Configure System Manager.	The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining, and verifying System Manager.

Document number	Title	Use this document to:	Audience
-	<i>Administering Avaya Aura® Session Manager</i>	Understand the end-to-end TLS connection for Session Manager.	The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining, and verifying Session Manager.
-	<i>Administering Avaya Session Border Controller for Enterprise</i>	Understand the end-to-end TLS connection for Session Border Controller.	The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining, and verifying Session Border Controller.

---

## Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. To search for the course, log in to the Avaya Learning Center, enter the course code in the **Search** field and click **Go**.

Course code	Course title
3U00125O	Designing Avaya Aura® Presence Services – Tech Sales L1
8U00170E	Avaya Aura® Presence Services Implementation and Maintenance

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

### Procedure

- To find videos on the Avaya Support website, go to [support.avaya.com](http://support.avaya.com) and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

---

## Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Chapter 2: Presence Services overview

---

## New in this release

Presence Services 6.2 supports:

- 16,000 H.323 and SIP users for each node and up to 125,000 H.323 and SIP users in an eight-node cluster.
- High Availability. For more information about High Availability, see *Deploying Avaya Aura® Presence Services*.
- Multiple Presence Services domains on a single Presence Services system.
- Inter domain Presence Services to Presence Services federation.
- Domino Calendar integration with the IBM Domino Enterprise deployment.

Presence Services 6.2 supports Lync integration with a clustered deployment.

- The Do Not Disturb mechanism.
- Root Certificate Authority (CA) certificates and generates server certificates by using the SHA256 signature algorithm with a 2048 bit key.

---

## Key features of Presence Services

- Supports a presence model that uses complex rules in an algorithm to arrive at an aggregated presence for a user.
- Supports protocols, such as SIP/SIMPLE and XMPP. These protocols enable Presence Services to aggregate and federate presence with major IM and messaging solutions and a number of user-productivity tools.
- Supports an architectural design that improves network traffic management. To reduce traffic on the network, Presence Services uses server-to-server updates to collect and publish presence information.
- Supports robustness. 9600 Series IP Deskphones Release 6.5 and Avaya one-X® Communicator Release 6.2 support this Presence Services feature.

## Overview

Presence is an indication of the availability of an individual at a point in time and readiness to communicate across a set of services, such as telephony and instant messaging. The presence or availability of a person is indicated by states like Busy and Away. These states indicate the availability of the individual to communicate with other users at that point in time.

Presentity refers to the visibility of a person on a shared communication network. The persons who are a part of the presentity group have access to the presence status of another person while reflecting their own active status. They are referred to as Watchers. To receive presence updates for a given presentity, a watcher must subscribe to the feature or service.

Presence Services is a single point of reference where different Presence entities collect. It supports Presence information gathered from a diverse range of sources. This information is aggregated on a per-user basis, and then made available to applications that include the Presence feature.

Applications interested in a user's presence must first subscribe to receive Presence information. Presence aware applications may use the Local Presence Service (LPS) to subscribe to Presence Services.

When an application subscribes to Presence Services, it receives Presence change notifications containing aggregated presence for a user and the communication resources available to the user. LPS runs co-resident on the application server. Using this information, the application can provide visual indications about user presence to an end-user client Graphical User Interface (GUI).

Presence Services uses LPS to efficiently transfer Presence information between the Presence server and the application servers. Presence Services uses presentities and watchers to do this. Presence Services facilitates the secure exchange of telephony availability and instant messaging (IM) information between applications.

In the business world, users employ the exchange of presence information to locate other users in a workplace. They also know when to contact helpdesk executives to address customer inquiries and help customer services to troubleshoot problems in real time.

Presence Services provides a Presence aggregation service that collects Presence information from Avaya and third-party sources and distributes Presence information to Avaya tools. It also aggregates Presence information from a wide variety of Avaya endpoints, including the one-X<sup>®</sup> family of clients.

Presence Services also supports the XMPP instant messaging protocol. By using a set of collectors, Avaya Presence Services serves as a conduit between end-users allowing them to use the Presence Services core Presence capabilities with these other Presence sources.

Presence Services is compatible with client software from Microsoft, IBM Lotus, and open source. You can see on-the-phone status on several phones and Internet messaging status in the Microsoft Office Communicator and other Internet Messaging applications. Some of the main applications are:

- The AES Collector allows Presence Services to report telephony Presence from Connection Manager endpoints. The collector collects Presence from H323 and DCP telephones and SIP telephones administered as OPTIM extensions.

- The Exchange Collector allows Presence Services to collect and publish the Calendar and Out of Office Assistant information for Exchange Mailboxes.

### Related Links

[Components of the Presence Services system](#) on page 15

[External entities](#) on page 16

[Other Avaya applications](#) on page 16

---

## Components of the Presence Services system

Presence Services performs the administration, life-cycle management, and configuration management of these subsystems.

### \* Note:

Presence Services 6.2 can support and integrate with multiple Presence sources, such as Microsoft Office Communicator clients on Microsoft Office Communications Server (OCS), and XMPP clients on XMPP server. The integration and support for these Presence sources depends on the overall solution capability in which you deploy Presence Services.

- The Presence Services Core eXtensible Communication Platform (XCP) server. Maintains a list of Presence fragments for a given presentity and performs composition of these fragments. Core XCP is the conduit between the collectors and distributors of Presence information in the system.
- The SIP Bulk Subscription server. Supports bulk distribution of Presence so that the transfer of Presence information between Presence Services and LPS is efficient.
- The SIP Presence server. Supports SIP-based clients who need to subscribe to and publish Presence. LPS uses SIP Presence server to publish Presence.
- The Presence server. Collects Presence information from various sources, such as Application Enablement Services (AES), Microsoft Office™ Communicator Server (OCS), and eXtensible Messaging and Presence Protocol (XMPP) Server. This information is for presentities retrieved from User Data Store. Presence server distributes Presence of a given class, such as Phone, Enterprise IM, and Avaya one-X® Communicator to users.
- OCS Gateway. Provides federation capability between Presence server and an OCS server. Enables peer-to-peer Presence and IM between clients connected to both servers.

Some of the example that Presence Services use for naming the components are:

Component Name	Description
CORE-ROUTER-1	Global jabber core router
sip-ps-1	SIP Presence server
sip-bulksub-1	SIP Bulk Subscription server
cm-1	XMPP Connection Manager
idmapper-1	IdMapper

### Related Links

[Overview](#) on page 14

---

## External entities

The Presence server may interact with the following external entities:

- Application servers hosting presence-aware applications. In this case, Presence Services provides an LPS that runs co-resident on the application server. The LPS maintains local subscriptions, performs access control, and exchanges data with the regional/central Presence server using the SIP Server-to-Server (S2S) protocol. Applications using LPS may request Presence information (subscribe/notify) from Presence Services or may provide Presence information (publish) to Presence Services for aggregation.
- Presence sources. There are a variety of other Presence sources from which Presence Services can collect Presence information.
  - Avaya Aura<sup>®</sup> Communication Manager (through AES) for Avaya telephony devices.
  - Microsoft-RTC (OCS/Lync) for Microsoft Presence.
  - XMPP Server for XMPP Presence.
  - Microsoft Exchange for Exchange presence.
- System Manager user management services. There is sizable user data that Presence Services and Avaya Applications must share in order to provide a unified view of a specific user within the enterprise. This data includes the user identities within various Presence domains, such as enterprise handle, Communication Manager extension, and Microsoft-RTC. In addition, the user has access control lists that must be shared among various applications and Presence Services components, such as the Presence server and Presence Services LPS. Presence Services relies on System Manager to provide all the user data instead of implementing its own User Management administration infrastructure. Presence Services uses Database Replication to retrieve data from a centralized management service and get change notifications.

### Related Links

[Overview](#) on page 14

---

## Other Avaya applications

To successfully operate Presence Services, you must install the following Avaya applications that are compatible with the Avaya Aura<sup>®</sup> framework.

**\* Note:**

It is important to install each component with the correct version.

- Avaya Aura<sup>®</sup> System Platform 6.3.1.

If you are installing Presence Services on System Platform on the Avaya Aura<sup>®</sup> S8800/Dell<sup>™</sup> PowerEdge<sup>™</sup> R610/HP ProLiant DL360 G7 server, you require System Platform 6.2.2.

- Avaya Aura® Dell™ PowerEdge™ R620 and HP ProLiant DL360p G8 server.
- Avaya Aura® System Manager 6.3.8.
- Avaya Aura® Session Manager 6.3.8.
- Application Enablement Services (AES) 6.2 and later versions.
- Avaya Aura® System Manager 6.3.8 that manages Communication Manager 6.2.1.
- Avaya Aura® Unified Communication Manager 6.1 in System Manager that manages CS 1000 7.6.

 **Note:**

Non-SIP deployments require AES.

For information about the Avaya Aura® components, see *Avaya Aura® Core Solution Description*.

### Related Links

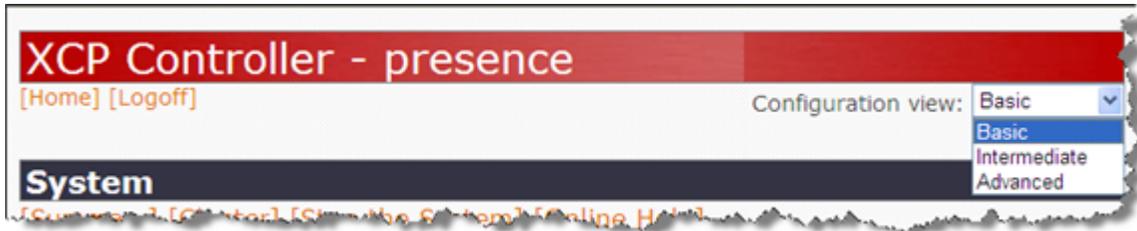
[Overview](#) on page 14

---

## Configuration views

The Presence Services XCP Controller Web interface offers three levels of configuration called Configuration views. The Configuration view menu is located in the top right corner of every controller configuration page. When you select a particular view, it remains in effect on all pages until you change it.

- The Basic configuration view. Displays the fewest configuration options and primarily uses the default values of the server. Configuring your system using this view is sufficient for most server components and enables you to get your XCP system up and running in the shortest amount of time.
- The Intermediate configuration view. Displays all of the options that are available in the Basic view in addition to some other options, such as those used for host name and command configurations and for logging. It also includes many of the options for components that are installed with the XCP extras installation package. The components whose configurations require you to use at least the *Intermediate* view includes a Message Archiver.
- The Advanced configuration view. Displays all of the options that are contained in the Basic and Intermediate views in addition to a number of fine-tuning options, such as buffer size, run level, and thread count. These options require a more advanced level of XCP server knowledge, and you can use them to adjust the performance of your XCP system. The components whose configurations require you to use the *Advanced* configuration view include:
  - Single Domain Name Support (SDNS)
  - Router-to-Router Connection



---

## Areas on the Controller's main page

---

### The System area

The links in the System area perform the following functions:

- **Summary.** Displays the complete jabber.xml file, which contains your configuration settings.

**\* Note:**

If you have modified the configuration of a plug-in or component, you must restart the system before the changes take effect and before they display in Summary.

- **Cluster.** Displays a page from which you can access all the controllers in this cluster.
- **Stop the System.** Stops the XCP server and all of its plug-ins and components.
- **Online Help.** Displays a help topic for the main page of the controller.
- **Full Help System.** Opens the complete online help system of the controller which is the online version of Administering Presence Services.



---

### The Router area

Router plug-ins are extensions of the Presence server core router, and always start and stop with the system. Each plug-in on your system is listed in the Router area of the controller.

You can add a new plug-in by selecting one from the list and clicking **Go** to display its configuration page. You can also modify the configuration of a plug-in by clicking the corresponding **Edit** link, or remove a plug-in (except for the core router) by clicking **Remove** link next to the plug-in.

**!** Important:

You cannot remove the Core Router, since it is the core of the Presence server.



Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	PresencePlugin	PresencePlugin	Edit, Remove		

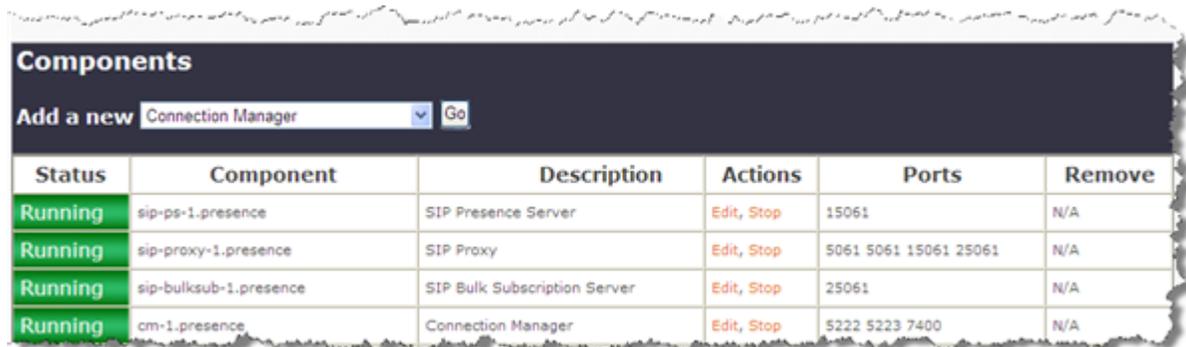
## Components area

Components are extensions of the Presence Services server that you can start and stop independent of the server. In the **Components** area, you can add, modify, start, stop, or remove server components.

**\*** Note:

Do not create multiple instances of components on a Presence Services server.

To add a new component, click the component from the **Add a new** drop-down box. To stop a component, click **Stop**. To modify the configuration of a component, click **Edit**. To remove a component, click **Remove**. You must stop a component before removing the component. These are tasks embedded in a concept topic. Also, not all the actions can be seen in the screen shot. Rewrite for clarity and to conform to DITA.



Status	Component	Description	Actions	Ports	Remove
Running	sip-ps-1.presence	SIP Presence Server	Edit, Stop	15061	N/A
Running	sip-proxy-1.presence	SIP Proxy	Edit, Stop	5061 5061 15061 25061	N/A
Running	sip-bulksub-1.presence	SIP Bulk Subscription Server	Edit, Stop	25061	N/A
Running	cm-1.presence	Connection Manager	Edit, Stop	5222 5223 7400	N/A

## Restarting the system

### Procedure

Log in to the Presence Services XCP Controller Web interface (<https://<IP address>:7300/admin>), do the following:

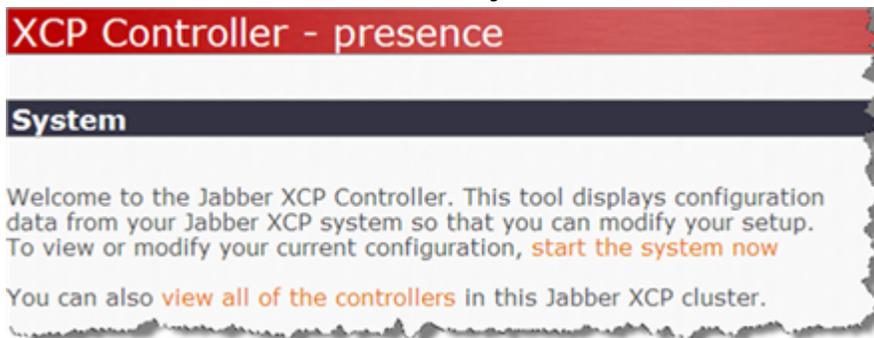
**\* Note:**

The default user name and password for the Presence Services XCP Controller Web interface. Contact Presence Services Support Personnel for the user name and password information.

- a. To stop the system, click **Stop the System**.



- b. To restart the server, click **start the system now**.



- c. To display the page from which you can access all the controllers in the current cluster, click **view all of the controllers**.

# Chapter 3: Administering System Manager for Presence Services

---

## System Manager and Presence Services

The presence administration pages of Avaya Aura<sup>®</sup> System Manager allow the administrator to manage:

- System Manager and Presence Services
- Viewing the details of the Presence server on System Manager
- Viewing the status of Presence server on System Manager
- Presence configuration properties

Also, you must add the new Presence server to the System Manager inventory manually using System Manager Web Console.

For information on the Geographic Redundancy feature, see the *Administering System Manager 6.3* guide and the *Configuring GR-unaware elements to work with System Manager Geographic Redundancy* guide.

To change the Presence Services host name, Avaya recommends that you install the Presence Services instance.

 **Note:**

For more information about installing Presence Services, see *Deploying Avaya Aura<sup>®</sup> Presence Services*.

The creation of the Presence Services instance on System Manager is automatic. For this reason, the steps required for adding a server are not included here.

To view the details and status of the Presence server on System Manager, use System Manager Web Console. You can also view the status of the Presence server on System Manager.

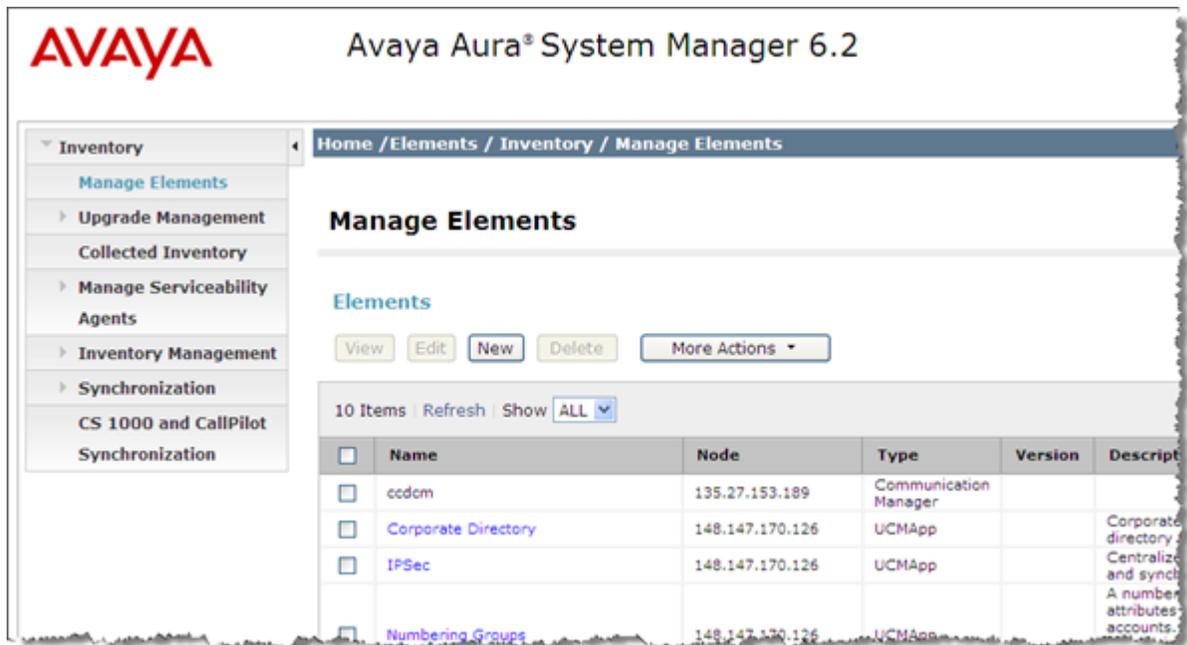
# Viewing the details of the Presence server on System Manager

## About this task

Perform this task to view the deployment status of the Presence Services elements with the System Manager.

## Procedure

1. Log in to System Manager by entering the System Manager virtual machine IP address in a Web browser: `https://< System Manager hostname>/SMGR`.
2. System Manager
3. On the Manage Elements page, click the associated check box to select an instance of Presence Services.



4. To view the details of the Presence server, click **View**.

On the View page, in the **General** area, you can view the server name, type, node, and an optional description.

In the **Port** area, you can view any configured ports. In a default installation, no ports are required.

In the **Access Point** area, you can view the access points. Access points are the ports that System Manager uses to access Presence Services. By default, System Manager displays two access points for each new Presence server. One of the access points defines the port that System Manager uses to view the status of Presence Services components. The other

access point defines the port that System Manager uses to launch the XCP Web Controller, which is also known as the Presence Services Web GUI for administrators.

---

## Viewing the status of the Presence server on System Manager

### Procedure

1. Log in to the System Manager web interface as an administrator.
2. Click **Services > Inventory > Manage Elements**.
3. Click the Presence Services instance.

On the Presence System Information screen, the system displays the name, host, and optional description.

4. Click **Open** to open the Presence Services XCP Controller web interface.
5. Click **Show** to display the status of the Presence Services components in a **Presence System Status** area.

The **Presence System Status** area displays the Presence Services components as a list of folders, which you can expand to view more details.

---

## Presence configuration properties

---

### Administering Presence configuration properties

#### Procedure

1. Log in to the Avaya Aura® System Manager web interface as an administrator.
2. Click **Elements > Presence > Configuration**.

The system displays the Presence Configuration Properties page.

3. To modify the configuration properties, perform the following steps:
  - a. Click **Edit**.
  - b. In the **Publish Presence with AES Collector - Default** field, specify whether Presence Services must publish the presence information with AES Collector.

You can override the system default on a per-Communication-Profile basis on the **Users > User Management > Manage Users > Communication Profile > Presence Profile** page.

- c. Click **Save**.

---

## User configuration in System Manager

Avaya Aura® users must be configured in System Manager, and typically have some or all of the following assigned:

- Avaya E.164 communication address: To configure this field, from the System Manager dashboard, navigate to **Users > User Management > Manage Users > Communication Profile > Communication Address**. Set the value of **Type** to **Avaya E.164**.
- Avaya SIP communication address: To configure this field, from the System Manager dashboard, navigate to **Users > User Management > Manage Users > Communication Profile > Communication Address**. Set the value of **Type** to **Avaya SIP**.
- CM Endpoint Profile: To configure this field, from the System Manager dashboard, navigate to **Users > User Management > Manage Users > Communication Profile > CM Endpoint Profile**.
- Session Manager Profile: To configure this field, from the System Manager dashboard, navigate to **Users > User Management > Manage Users > Communication Profile > Session Manager Profile**.

For more information, see the *Managing Users* section in *Administering Avaya Aura® System Manager*.

### Related Links

- [Configuring System Manager to enable Presence and IM services](#) on page 24
- [Creating SIP routing domains](#) on page 25
- [Assigning an Avaya Presence/IM communication address to a user](#) on page 26
- [Presence Profile](#) on page 27
- [Assigning a Communication Profile Password to a user](#) on page 32
- [Disabling cross-domain communication](#) on page 32

---

## Configuring System Manager to enable Presence and IM services

### About this task

Use the following procedure to support presence and IM services for an Avaya Aura® user. You can configure the attributes when a user is initially configured on System Manager, or by editing an existing user.

The presence-related attributes can also be assigned through User Provisioning Rules in System Manager. To create an Avaya Presence/IM communication address through User Provisioning Rule, you must assign a Login Name. To assign a Login Name, navigate to **Users > User Management > Manage Users > Identity > Login Name** from the System Manager dashboard. For more information, see the *Managing user provisioning rules* section in *Administering Avaya Aura® System Manager*.

When Presence Services is used to federate with third-party servers, users hosted by a third-party server might be configured in System Manager. For more information, see *Presence Services federation with third-party servers*.

Presence can only be configured against the default Communication Profile of a user.

### Procedure

1. Create SIP routing domains. These attributes are used during the creation of Avaya Presence/IM communication addresses. If a SIP routing domain already exists for use during the creation of Avaya SIP communication addresses, you can use the same SIP routing domain for both communication addresses. However, using the same SIP routing domain for both communication addresses is not mandatory. Multiple presence domains are supported on Presence Services. For example, you can create two or more SIP routing domains, and create two or more Avaya Presence/IM communication addresses with different SIP routing domains. For more information, see *Creating SIP routing domains*.
2. Assign an Avaya Presence/IM communication address to a user. This unique Presence identifier is used by other users, devices, or servers for exchanging IMs and presence information with this user. For more information, see *Assigning an Avaya Presence/IM communication address to a user*.
3. Assign a Presence Profile to a user. This is used to assign a user to a home Presence Services server, and assign attributes on a per-communication-profile basis. For more information, see *Assigning Presence Profile to a user*.
4. Assign a Communication Profile Password to a user. This password must be configured on Avaya endpoints, for example, Avaya OneX Communicator. Presence Services authenticates users with this password. For more information, see *Assigning a Communication Profile Password to a user*.
5. **(Optional)** Disable cross-domain communication: By default, users in different presence domains can exchange presence information. If needed, this setting can be disabled. However, the ability of users in different domains to exchange IMs cannot be disabled. For more information, see *Disabling cross-domain communication*.

### Related Links

[User configuration in System Manager](#) on page 24

---

## Creating SIP routing domains

### About this task

Use SIP routing domains to create both Avaya Presence/IM and Avaya SIP communication addresses. Using the same domain for both communication addresses is recommended but not mandatory.

### Procedure

1. Log on to the System Manager web console.
2. On the System Manager dashboard, click **Elements > Routing**.

The system displays the Introduction to Network Routing Policy page.

3. In the navigation pane, click **Domains**.

The system displays the Domain Management page.

4. Select **New**.
5. In the **Name** field, type the domain name.
6. In the **Type** field, select **sip**.
7. Click **Commit** to save the changes.

#### Related Links

[User configuration in System Manager](#) on page 24

---

## Assigning an Avaya Presence/IM communication address to a user

### Procedure

1. Log on to the System Manager web console.
2. On the System Manager dashboard, click **Users > User Management**.

The system displays the User Management page.

3. On the navigation pane, click **Manage Users**.
4. Select a user and click **Edit**.

The system displays the User Profile Edit page.

5. Click the **Communication Profile** tab, and select the Communication Profile with the **Default** check-box enabled.
6. In the **Communication Address** section, click **New**.
7. In the **Type** drop-down box, select **Avaya Presence/IM**.
8. The **Fully Qualified Address** section displays two fields:

- In the first field, enter the user portion of the Avaya Presence/IM communication address.
- In the second field, select the SIP routing domain.

9. Click **Add**.
10. Click **Commit** to save the changes.

The system updates the Avaya Presence/IM communication address on System Manager and Presence Services.

#### Related Links

[User configuration in System Manager](#) on page 24

---

## Presence Profile

You can assign Presence Profile in one of the following ways:

- Assigning Presence Profile to a user
- Assigning Presence Profile to bulk users
- Assigning Presence Profile by using the Presence Communication Profile Migrating tool

### Related Links

[User configuration in System Manager](#) on page 24

[Assigning Presence Profile to a user](#) on page 27

[Assigning presence profile using bulk export and import](#) on page 29

[Assigning Presence Profile by using the Presence Communication Profile Migrating tool](#) on page 30

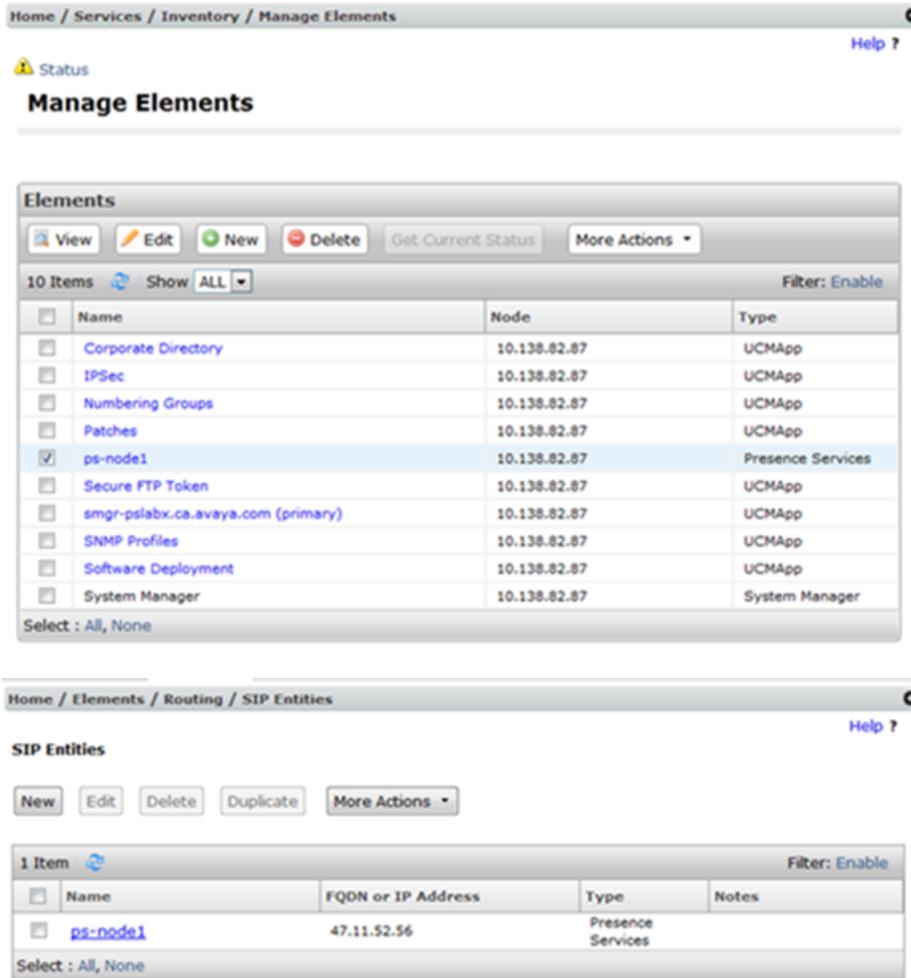
## Assigning Presence Profile to a user

### Before you begin

1. Verify that all Presence Services instances are listed on System Manager at **Services > Inventory > Manage Elements** with a **jsmld** assigned.

When a Presence Services instance is installed and successfully connects to System Manager, an entry with Type = Presence Services is created on System Manager at **Services > Inventory > Manage Elements**, and a non-blank **jsmld** is automatically assigned.

2. To verify the **jsmld** value is not blank, perform the following steps:
  - a. Navigate to **Services > Inventory > Manage Elements**.
  - b. Select a Presence Services instance, and click **Edit**.
  - c. In the Edit Presence Services page, click the **Attributes** tab.
  - d. Expand the Attributes window, and verify the value of the **jsmld** field.
  - e. Click **Cancel** to cancel the edit operation.
3. Verify that all Presence Services instances listed on System Manager at **Services > Inventory > Manage Elements** have matching SIP entities defined at **Elements > Routing > SIP Entities > Name**. If not, create the SIP Entities. Refer to the following figures.



Note the Presence Services instances that have the same name **ps-node1** at both the **Services > Inventory > Manage Elements > Name** page and the **Elements > Routing > SIP Entities > Name** page. These names must match exactly.

### Procedure

1. Log on to the System Manager web console.
2. Click **Users > User Management**.
3. In the navigation pane, click **Manage Users**.  
The system displays the User Management page.
4. Select a user, and click **Edit**.  
The system displays the User Profile Edit page
5. Click the **Communication Profile** tab, and select the Communication Profile with the **Default** check-box enabled.
6. Select the check box to the left of **Presence Profile**.

7. Click the arrow next to **Presence Profile** to expand the **Presence Profile** section.
8. In the **Presence Profile** section, enter values in the following fields:
  - a. In the **System** field, select the Presence Services instance that you want to use as the home server for the user.  
  
The system selects and displays the value of the **SIP Entity** field when you select the Presence Services instance. You cannot change the value of this field.
  - b. **(Optional)** In the **Publish Presence with AES Collector** field, specify whether Presence Services should publish presence with AES Collector.  
  
For more information about **Publish Presence with AES Collector**, see *Administering Presence configuration properties*.
9. Click **Commit** to save the changes.  
  
The system updates the Presence Profile information on System Manager and Presence Services.

#### Related Links

[Presence Profile](#) on page 27

[Administering Presence configuration properties](#) on page 23

## Assigning presence profile using bulk export and import

### Before you begin

Verify that all Presence Services instances have jsmlIDs and matching SIP entities.

### Procedure

1. On the System Manager web console, navigate to **Users > User Management > Manage Users**.
2. In the **More Actions** field, click **Export All Users** or **Export Selected Users**.
3. On the **Export Users** page, select the **Presence Profile** field.
4. Click **Export**.

The system displays the status as `SUCCESSFUL` in the **Export List** table.

5. In the **Download File** column, click the file link.
6. Extract the file in an Excel or Xml format, and edit the values of the following fields:
  - **System**: Select the Presence Services instance that you want to set as the home server.
  - **Publish Presence with AES Collector**: Specify whether Presence Services must publish the presence information with AES Collector.
  - **Communication Password**: Type the communication profile password.

**\* Note:**

In the Excel file, type the password in the **Communication Password** field. In the Xml file, add the `<commPassword></commPassword>` tag after the `<userPassword></userPassword>` tag.

7. Save the file.
8. In the navigation page, click **Manage Users**.
9. In the **More Actions** field, click **Import Users**.
10. In the **If a matching record already exists** field, click **Merge**.
11. Select the import file type: **Xml** or **Excel**.
12. Click **Choose File**, and select the file that you have edited.
13. Click **Import**.
14. Click **Done**.

### Next steps

To view the details of the import records that failed, select the check box next to the import job, and click **View job**.

### Related Links

[Presence Profile](#) on page 27

## Assigning Presence Profile by using the Presence Communication Profile Migrating tool

### Before you begin

1. Verify that all Presence Services instances are listed on System Manager at **Services > Inventory > Manage Elements** with a jsmlId assigned.

When a Presence Services instance is installed and successfully connects to System Manager, an entry with Type = Presence Services is created on System Manager at **Services > Inventory > Manage Elements**, and a non-blank jsmlId is automatically assigned.

2. To verify the **jsmlId** value is not blank, perform the following steps:
  - a. Navigate to **Services > Inventory > Manage Elements**.
  - b. Select a Presence Services instance, and click **Edit**.
  - c. In the Edit Presence Services page, click the **Attributes** tab.
  - d. Expand the Attributes window, and verify the value of the **jsmlId** field.
  - e. Click **Cancel** to cancel the edit operation.
3. Verify that all Presence Services instances are listed on System Manager at **Services > Inventory > Manage Elements** have matching SIP entities defined at **Elements > Routing > SIP Entities > Name**. If not, create the SIP Entities. Refer to the following figures.

Home / Services / Inventory / Manage Elements Help ?

Status

## Manage Elements

---

**Elements**

View Edit New Delete Get Current Status More Actions ▾

10 Items Show ALL ▾ Filter: Enable

<input type="checkbox"/>	Name	Node	Type
<input type="checkbox"/>	Corporate Directory	10.138.82.87	UCMApp
<input type="checkbox"/>	IPSec	10.138.82.87	UCMApp
<input type="checkbox"/>	Numbering Groups	10.138.82.87	UCMApp
<input type="checkbox"/>	Patches	10.138.82.87	UCMApp
<input checked="" type="checkbox"/>	ps-node1	10.138.82.87	Presence Services
<input type="checkbox"/>	Secure FTP Token	10.138.82.87	UCMApp
<input type="checkbox"/>	smgr-pslabx.ca.avaya.com (primary)	10.138.82.87	UCMApp
<input type="checkbox"/>	SNMP Profiles	10.138.82.87	UCMApp
<input type="checkbox"/>	Software Deployment	10.138.82.87	UCMApp
<input type="checkbox"/>	System Manager	10.138.82.87	System Manager

Select : All, None

---

Home / Elements / Routing / SIP Entities Help ?

**SIP Entities**

New Edit Delete Duplicate More Actions ▾

1 Item Show ALL ▾ Filter: Enable

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ps-node1	47.11.52.56	Presence Services	

Select : All, None

Note the Presence Services instances that have the same name **ps-node1** at both the **Services > Inventory > Manage Elements > Name** page and the **Elements > Routing > SIP Entities > Name** page. These names must match exactly.

### About this task

This procedure creates new Presence Communication Profiles for users in System Manager that currently do not have a Presence Profile, but have a Presence/IM handle. This utility works with only the default Communication Profile.

### Procedure

1. Log in to the System Manager command line interface as root.
2. Copy the `ps-comm-profile-migration-zip` file to System Manager by using a file transfer tool such as WinSCP..
3. Extract the contents of the `ps-comm-profile-migration-zip` file into the `/home/admin` folder.
4. Run the command `sh migrate.sh -ln` to validate the Presence Services nodes.

5. Run the `sh migrate.sh -lp` command to display the list of users that need communication profiles.
6. Run the `sh migrate.sh -m` to create Communication Profiles for the users that do not have Communication Profile, but have an XMPP handle.

**\* Note:**

The utility does not log the results. Therefore, you must redirect the console output to a file. For example, `sh migrate -m > migration.log`.

### Related Links

[Presence Profile](#) on page 27

---

## Assigning a Communication Profile Password to a user

### Procedure

1. Log in to System Manager Web Console.
2. On System Manager Dashboard, click **Users > User Management > Manage Users**.  
The system displays the User Management page.
3. To edit a user profile, select the user and click **Edit**.  
The system displays the User Profile Edit page.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Under the Communication Profile section, click **Edit** next to the **Communication Profile Password** field.
6. Enter the communication profile password, confirm the password, and then click **Done**.
7. To save the changes, click **Commit**. The system updates the user password to Presence Services as well.

### Related Links

[User configuration in System Manager](#) on page 24

---

## Disabling cross-domain communication

### About this task

This procedure is optional.

### Procedure

1. Log in to the Presence Services server as a root user.
2. Navigate to the `/etc/profile.d` directory.

3. Edit the `setpres.sh` file, and insert the following line: `export CROSS_DOMAIN_COMMUNICATION=false`.
4. Save the file.
5. Restart the Presence Services server.

### Related Links

[User configuration in System Manager](#) on page 24

---

## Licensing

To successfully deploy Presence Services in a customer site, you require a valid Presence Services license.

### **Note:**

You can find the license for Presence Services on the System Manager WebLM server.

The most important aspects of a license are:

- Number of users
- Expiration date
- Version number

At any given time, a license is in one of three states:

- Valid. The license is operational.
- Grace. The license is operational, but will expire soon. This state can last up to 30 days.
- Expired. The license is no longer operational and the grace period has elapsed.

When the license enters the grace period, it generates an error log. When a license expires, it generates a fatal log.

---

## Presence Services license renewal

Presence Services licenses operate in the same way as all of the other Avaya Aura<sup>®</sup> products that reside within the System Manager framework. That is to say, you must use Avaya Product Licensing and Delivery System (PLDS).

PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads. When you place an order for a PLDS-licensed software product such as Presence Services, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using the LAC, you can quickly find

and activate the newly purchased license entitlements in PLDS. You can then download the license file.

You must provide the WebLM host ID to activate the license file in PLDS. The WebLM host ID is the MAC address of the server and is obtained from the WebLM Web interface. The WebLM Web Host ID is the System Manager host ID.

**\* Note:**

WebLM host ID should be the System Manager host ID.

---

## Renewing your Presence Services license

### Before you begin

Before you perform this task, you must have a valid login and password for PLDS. You must also place an order for a license, for example, with your Avaya account manager. In response, your Avaya account manager sends you an e-mail containing a LAC.

### Procedure

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **Services > Licenses > Server Properties**.
3. Note the string in the **Primary Host ID** field. This is the WebLM host ID.
4. Type <http://plds.avaya.com> in your Web browser to access the Avaya PLDS Web site.
5. Enter your login ID and password to log on to the PLDS Web site.
6. In the **LAC(s)** field of the **Quick Activation** section, enter the LAC that you received in an e-mail message.
7. In the **License Host** field, enter the WebLM host ID.
8. Click **View Activation Record**.
  - The **Overview** tab displays a summary of the license activation information.
  - The **Ownership** tab displays the registration information.
  - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file is generated for each application.
  - From the **License/Key** tab you can view and download the license file. Each license file must be installed on the WebLM server associated with the License Host.
9. Save the license file to your computer.
10. Log in to System Manager Web Console by entering the System Manager virtual machine IP address in a Web browser.
11. On System Manager Dashboard, click **Services > Licenses > Install License**.
12. On the Install License page, enter the license file path. You can also click **Browse** to select the license file.

13. Click **Install** to install the license file.

WebLM displays a message on the successful installation of the license file.

---

## Presence Services Admin status check

**presstatus** is a Presence Status tool that collects Presence Services component status information, including the Presence server components that run under the Presence server container and the Presence server external processes.

Internal and contained components that are providing status includes umc, replicator, dbfactory, aclstorage, AES Collector, Presence transformer component, RLMS component, Id Mapper, IM and SDNS, also provide the status information of the Presence Services (IM Transcript Service) and Presence Services processes running under jabber user (Web Connection Manager, jabbered, sip\_proxy, sip\_ps, sip\_bulksub, and sip-gw).

### Related Links

[presstatus](#) on page 35

[Using the Interactive Mode](#) on page 35

[Using the Command line mode](#) on page 36

[Example output](#) on page 36

[Status description](#) on page 38

---

## presstatus

The presstatus script is installed in the folder `/opt/Avaya/Presence/presence/bin`. The presstatus is a stand-alone command line tool to generate the current state of the Presence Services components. This enables you to know the current state of Presence Services components.

You can run the presstatus in the interactive and the command line modes.

- Interactive mode – Use System Manager to view the status of Presence Services components.
- Command line mode – Run command line arguments to view the status of Presence Services components.

### Related Links

[Presence Services Admin status check](#) on page 35

---

## Using the Interactive Mode

### Procedure

1. Log in to System Manager Web Console as an administrator.

2. On System Manager Dashboard, click **Services > Inventory > Managed Elements**.

The system displays the Manage Elements page.

3. Click the element name and then click **View**.

**\* Note:**

The first part of hostname appears as name. For example, if `xPS.du.rnd.avaya.com` is the host name, the name appears as `xPS`.

4. Click **Show** displayed with the **Status** field.

The system displays the Presence Status System interface below the Presence System Information page.

You can view the Presence System Status as Contract Mode or Expand Mode by clicking the respective options.

### Related Links

[Presence Services Admin status check](#) on page 35

---

## Using the Command line mode

### Procedure

1. Log in to the Presence server as a root user.
2. Go to the bin folder. For example: `cd /opt/Avaya/Presence/presence/bin.`
3. At the command prompt, type `./presstatus.`

### Related Links

[Presence Services Admin status check](#) on page 35

---

## Example output

The following example illustrates an example of current status of all Presence Services components that are be generated.

```
Activity: Wed Aug 18 11:30:16 IST 2010
Component: Presence Server (Partially Enabled)
Process ID (PID): 1054
CPU%: 0.0
Activity: Wed Aug 18 11:30:16 IST 2010
Component: Replicator Component (Connected)
Activity: Wed Jul 28 10:55:15 IST 2010
Last Activity: addBatchListener ReplicationListMonitor to tables: [cscontactlist,
cscontactlistmember, csuser]

Component: User Management (Licensed)
license-detail: The product license is in the 30 day grace period since Mon Aug 16
10:59:11 IST 2010 because the number of users has been exceeded or there has not been a
valid license installed, there are 27 day(s) left before the license will expire.
```

The product license has not reached its expiration date and is valid.  
The product license is the correct version.  
Activity: Wed Aug 18 11:30:16 IST 2010  
Last Activity: Got replication event from replica component  
users: 0

Component: Avaya Application Enablement Services Integration (Started)  
Component: Microsoft Office Communications Server Integration (Unknown)  
Component: Avaya SES Integration (Started)  
Component: Sametime Component (Disabled)  
Component: Sametime Collector (Disabled)  
Component: Sametime Distributor (Disabled)  
Component: XMPP Collector (Connected)  
Activity: Wed Aug 18 03:52:19 IST 2010  
Component: 135.64.23.113 (Connected)  
Activity: Wed Aug 18 03:52:19 IST 2010  
Component: ID Mapper (Started)  
Component: IM Transcript Launcher (Started)  
Component: Single Domain Name Support Component (Disabled)  
Component: ACL Manager (Started)  
Activity: Wed Jul 28 10:55:05 IST 2010  
Last Activity: startup  
Component: Local Presence Database (Connected)  
Activity: Wed Aug 18 11:30:14 IST 2010  
Database Status: OK  
Last Status Change: Wed Jul 28 10:55:03 IST 2010  
Component: presence-model (Active)  
Component: provisioning (Active)  
Component: XMPP Daemon (Active)  
Process ID (PID): 3132  
CPU%: 0.0  
Component: SIP Proxy (Active)  
Process ID (PID): 3277  
CPU%: 0.0  
Component: Web Connection Manager (Active)  
Process ID (PID): 3237  
CPU%: 0.0  
Component: XMPP Connection Manager (Active)  
Process ID (PID): 3719  
CPU%: 0.0  
Component: SIP Presence Server (Active)  
Process ID (PID): 3716  
CPU%: 0.0  
Component: Microsoft Office Communications Server Gateway (Active)  
Process ID (PID): 3723

```
CPU%: 0.0

Component: SIP Bulk Presence Subscription Server (Active)
Process ID (PID): 3718
CPU%: 0.0

Component: Presence Web Server (Disabled)

Component: IM Transcript Web Service (Disabled)

Component: Certificates (Active)

Component: Cert 1 (Active)
SubjectDN: C=US/ O=Avaya/ CN=ips23-105.pres.avayainstall.com

Expiry: Fri Jul 27 10:42:03 IST 2012
Issued: Wed Jul 28 10:42:03 IST 2010
IssuerDN: O=AVAYA/ OU=MGMT/ CN=default
```

### Related Links

[Presence Services Admin status check](#) on page 35

---

## Status description

The following table describes the different status of components:

Status	Description
Partially Enabled	Some components are disabled.
Connected	Indicates connection of the component to the corresponding source.
Licensed	The current Presence Services instance is licensed.
Not Licensed	The current Presence Services instance is not licensed. Also provides a detailed description of the status.
Started	A particular component has started running.
Unknown	presstatus is unable to obtain the status of a particular component.
Disabled	A component is disabled.
Active	All noncontainer-based processes are active. For example, SIP-PS, SIP-GW, and so on.

### Related Links

[Presence Services Admin status check](#) on page 35

---

# Exporting and importing bulk users

---

## Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file or an Excel file as input file. While exporting data in bulk, the system can export the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles

The supported communication profiles are CM Endpoint, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, and Collaboration Environment.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

 **Important:**

System Manager does not support import and export of roles in bulk.

---

## Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk using an Excel file in addition to an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager supports. When you export data in bulk from System Manager Web Console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the .xlsx format. You can download the Excel template from the User Management page.

Import and export in bulk using the Excel template has the following features:

- Supports the following types of user information:
  - Basic. The identity data of the user
  - Handle. The communication address of the user
  - Session Manager profile
  - CM Endpoint Profile

- Messaging profile
- Conferencing profile
- IP Office Endpoint profile
- CS 1000 Endpoint profile
- Provides a description in the form of a tool tip for each attribute. The mandatory fields are marked.
- Provides the login name in the Basic worksheet as the key attribute that you use in other worksheets to link the user records.
- Supports only the primary communication profile set.

Append the loginname with #primary in all worksheets except Basic to specify the association of the records with the primary communication profile set. For example, jmillier@avaya.com#primary.

- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can perform one operation at a time.
- For updation, supports only the partial merge operation.

Bulk import and export using Excel does not support the following:

- All attributes that XML user import supports. For more information, see the Excel template.
- Complete or partial replace of the user for imports in bulk.

### Feature of the Excel template

- Though the header fields in the Excel template are editable, do not change any details of any headers in the worksheets. The import or export might fail if you modify the details of the header.
- The data in Excel might display the warning message `Number Stored as Text`. Ignore the warning.

 **Note:**

Do not change the data type of the cells in the Excel template.

In Microsoft Office Excel 2007 and later, click **Excel Options** and clear the **Numbers formatted as text or preceded by an apostrophe** check box to turn off the warning message.

---

## Bulk importing of users

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **ImportUser ManagementUsers**.

Also, to gain access to **Import users**, from System Manager Web Console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.

- On the Import users page, in the **Select Import File Type** field, select one of the following file type:

- XML
- Excel

**\* Note:**

Use the Excel template that System Manager supports. If you fail to use the template that System Manager supports, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release`. Use the Excel template that you downloaded or exported from the current System Manager release.

- On the Import users page, in the **Select File** field, type the complete path of the file or click **Browse** to locate and select a file.
- Select one of the following error configuration options:

- **Abort on first error**
- **Continue processing other records**

- For XML file type, click **Complete** in the import type.

If you select Excel file type, the system does not display the import type option.

- Select one of the following import options:

- To skip users in the import file that match the existing user records in the database, click **Skip**.
- To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.

If you select Excel file type, the system does not display the replace option

- To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
- To delete the user records in the database that match the records in the imported file, click **Delete**.

**\* Note:**

For import by using Excel, the system deletes the user records permanently.

- To run the job, in the **Job Schedule** section, select one of the following options:

- To import the users immediately, click **Run immediately**.
- To import the users at a specified time, click **Schedule later**, and set date and time.

- Click **Import**.

If you use the default configurations option **Importing Users > Add Users** in the database, the system imports the next user record even if the import user operation encounters an error while importing a user record. The system logs an error. Skip import of users that already exist in the database. The system schedules the import job to run immediately.

**\* Note:**

The operations, Communication Manager Synchronization and Bulk Import of users, must not overlap in time. If Bulk Import of users is in progress and Communication Manager Synchronization is started, the current records under process fail. After the synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail during synchronization.

---

## Exporting users in bulk using CLI

### Before you begin

Start an SSH session.

### Procedure

1. Log in to System Manager using SSH as `root`.
2. To change the directory to `exportutility`, at the prompt, type `cd $MGMT_HOME/bulkadministration/exportutility/`.  
*MGMT\_HOME* is an environment variable that represents the System Manager HOME path.
3. Type `# sh exportUpmUsers.sh ... [OPTIONS]`.
4. **(Optional)** To modify the default values for optional parameters, change the `$MGMT_HOME/bulkadministration/exportutility/config/bulkexportconfig.properties` file, where *MGMT\_HOME* is an environment variable that represents the home path for System Manager.

For example, `# sh exportUpmUsers.sh -f userExport -r 1000 -s 0 -e 1000`.

# Chapter 4: Integrating Presence Services with Session Manager

---

## Overview of Session Manager with Presence Services

Session Manager performs SIP routing and other session processing functions of an Avaya Aura® SIP network. Session Manager also routes SIP requests from Avaya SIP clients to Presence Services. This routing is based on a SIP request URI containing the IP address of Presence Services.

On startup, Presence Services sends the OOD Refer message to the endpoints through Session Manager. This message initializes the presence states of the endpoints.

When the Presence Services server goes down, for example, during server upgrade, and loses the endpoints subscription, the OOD Refer message notifies the endpoints that the endpoints must resubscribe to get presence information. This notification minimizes the down time or misleading presence states that occur in the time frame of the subscription being lost and the subscription being renewed. The OOD Refer message with a redirect option reconfigures the XMPP connection.

---

## Adding Session Manager to Presence Services

### About this task

At the time of installation, you might have entered the Session Manager Asset IP address in the Session Manager Configuration Setting panel for Presence Services to integrate with Session Manager. If you did not enter, you can enter after the Presence Services installation.

### Note:

You cannot add multiple Session Manager instances to the same Presence Services system.

### Procedure

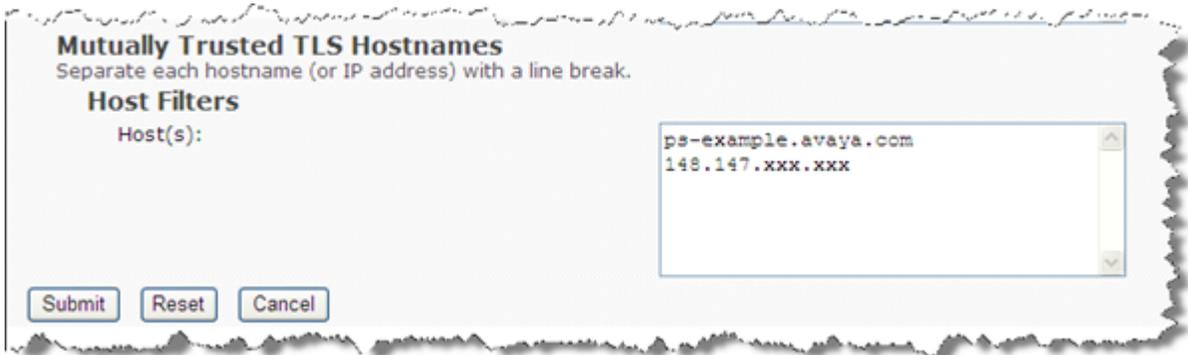
1. Log in to the Presence Services XCP Controller web interface.
2. On the Presence Services home page, select the **Intermediate or Advanced Configuration** view.

3. In the Router area, in the **Core Router (Global router settings)** section, click **Edit**.



The system displays the Global Settings Configuration page.

4. Scroll down to **Mutually Trusted Hostnames**, and type the Session Manager Asset IP address.



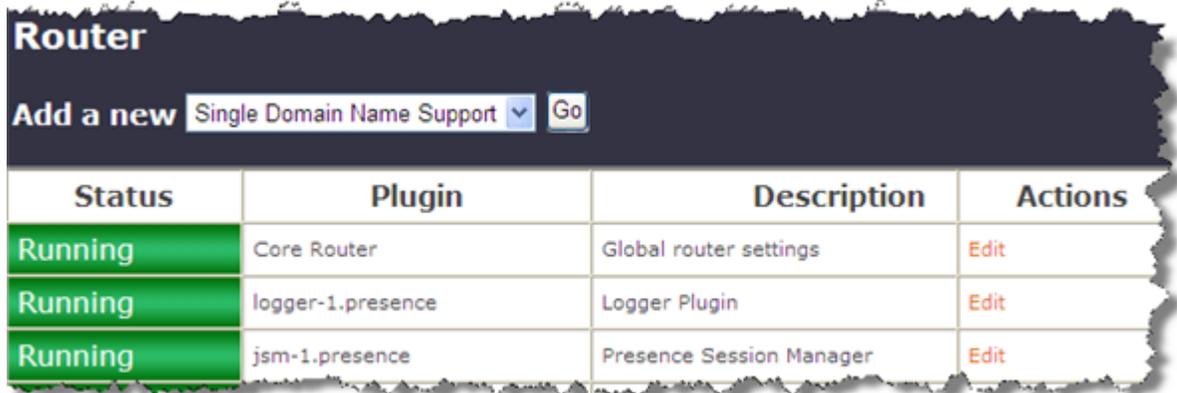
5. Click **Submit**.
6. Restart the Presence Services system.

---

## Verifying the hostname in the Presence Session Manager Procedure

1. Log in to the XCP Controller Web interface.

- On the Intermediate configuration view of the controller, under Router, click **Edit** next to Presence Session Manager.



Status	Plugin	Description	Actions
Running	Core Router	Global router settings	Edit
Running	logger-1.presence	Logger Plugin	Edit
Running	jsm-1.presence	Presence Session Manager	Edit

The system displays the Presence Session Manager Configuration page.

- Ensure that the new ID appears under Presence Session Manager.

---

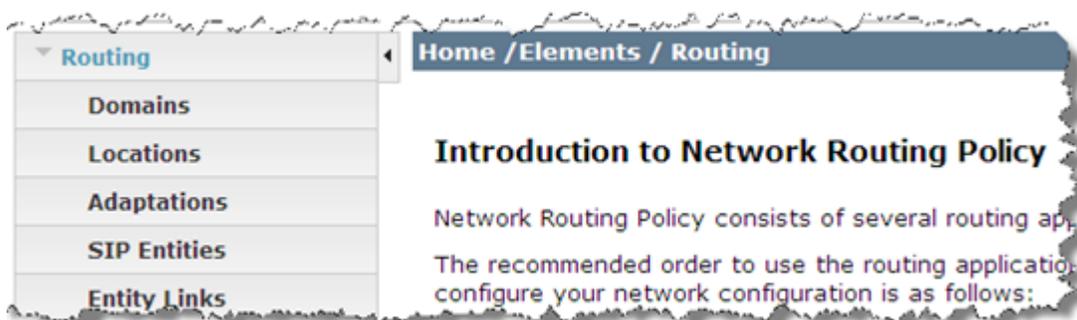
## Adding Presence Services as a SIP entity in System Manager

### Procedure

- Log in to System Manager Web Console as an administrator.
- On System Manager Dashboard, click **Elements > Routing**.

The system displays the Introduction to Network Routing Policy page.

- On the left navigation pane, click **SIP Entities**.



The system displays the SIP Entities page.

- Click **New**.

The system displays the SIP Entities Details page.

5. On the SIP Entities Details page, enter the following details:
  - a. **Name**. Example, PresenceServer
  - b. **FQDN or IP Address**. Presence Services IP address
  - c. **Type**. Other
  - d. **SIP Link Monitoring**. Use Session Manager Configuration
6. To save the changes, click **Commit**.

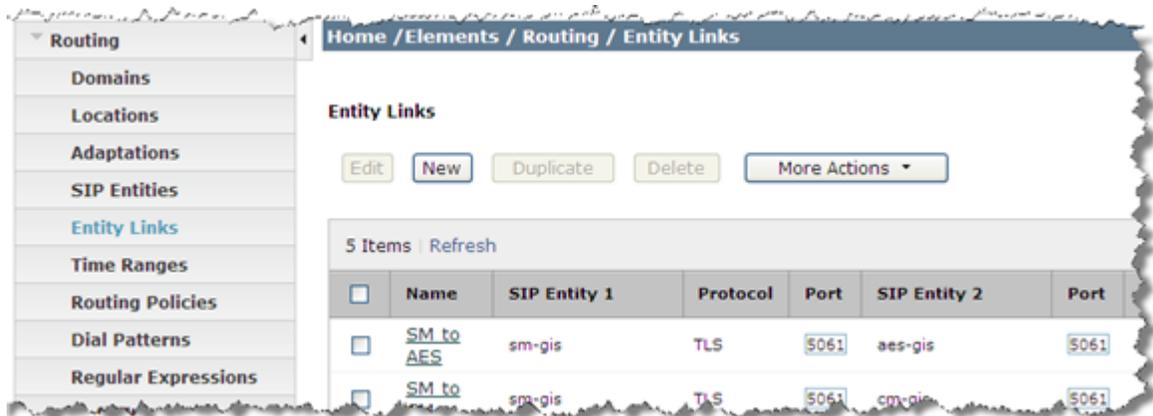
For more information, see the *System Manager* documentation.

---

## Adding an entity link

### Procedure

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **Elements > Routing > Entity Links**.



3. On the Entity Links page, click **New** and enter the following details:
  - a. **Name**. Link name (Example: PresenceServerLink )
  - b. **SIP Entity 1**. Select Session Manager from the list
  - c. **Protocol**. Select TLS.
  - d. **Port**. 5061
  - e. **SIP Entity 2**. Choose the same Presence Services name you created in the previous procedure (Example: PresenceServer )
  - f. **Port**. 5061
  - g. **Connection Policy**. Select **Trusted**.
4. To save the changes, click **Commit**.

For more information, see the *System Manager* documentation.

You must set up an end-to-end TLS connection between the Presence server and the endpoints, which includes:

- An entity link between Presence Services and Session Manager.
- Entity links between multiple Session Manager.
- SIP connections between Session Manager and Session Border Controller.
- A connection between endpoints and controllers of the endpoints.

For more information about end-to-end TLS connection for Session Border Controller and Session Manager, see the *Administering Avaya Session Border Controller for Enterprise* guide and the *Administering Avaya Aura® Session Manager* guide.

---

## Avaya SIP Client(s) support

SIP clients, such as Avaya one-X® Communicator 6.0/6.1 SIP, require the Presence Services SIP Client Support function to receive Presence information updates. This support extends the use of open IETF standards based on RFC 2543, 3265, 3903, and 3857 and open IETF standards from the family of documents collectively known as SIP for Instant Messaging and Presence Leveraging Extensions (SIP SIMPLE).

The SIP Client Support function utilizes several modules, such as:

- **mod\_simple** performs SIP SIMPLE functionality. SIMPLE is an open standard based on RFCs that describe the integration of SIP (RFC 3261) with the Instant Messaging and Presence (IMP) standards.
- **mod\_idmap** enables SIP-based clients to publish and subscribe for Presence information. To do this, it applies SIP identifiers to internal JID representation using ID Mapping.
- ID Mapping, you need ID Mapping for any SIP Presence Subscription where the SIP URI lies outside the Presence server domain. ID Mapping does the following:
  - Maps any SIP URI handle registered with System Manager to a single presentity.
  - Maps any Presence server presentity to its Primary SIP URI.
  - Supports mapping just the user (number) portion of E.164 handles to appropriate presentity.
  - Requires any SIP Presence Subscriptions where the SIP URI lies outside the Presence server domain.
  - Uses Resource list and winfo subscriptions to map the presentity to the most appropriate handle URI provisioned in System Manager.
- **mod\_authz** enables ACL-based Authorization through Authorization Management. It facilitates subscription to a list of contacts through Resource lists.

Using Authorization, you can make Authorization decisions with Access Control Lists (ACL) set up in System Manager (SMGR).

---

## Enabling required modules in Presence Session Manager

### Procedure

1. Log in to Presence Services XCP Controller Web interface.
2. On the Presence Services XCP Controller home page, select **Advanced Configuration View**.
3. In the Router area, click **Edit** next to the Presence Session Manager.
4. Under **Optional Modules**, select:
  - *mod\_idmap*
  - *mod\_authz*
  - *mod\_simple*
  - *mod\_winfo*
  - *mod\_peg*
5. Scroll down to **Module Configuration** to select and set **SIP URI Mapping Configuration** to *Yes*.
6. To save your choices, click **Submit**.
7. To see if the **Authz** component, the **IdMapper** component have been added to the Components page, go back to the Presence Services XCP Controller home page.
8. To open the SIP Presence Service Configuration page, click **Edit** next to the SIP Presence Server under Components .
9. Scroll down to set **Enable ID Mapping** to *Yes*.
10. To save your choices, click **Submit**.

# Chapter 5: Configuring Presence Services components

---

## Managing Presence components

---

### Presence components

Presence Services 6.2 can support and integrate with multiple Presence sources, such as Microsoft Office Communicator clients on Microsoft OCS, and XMPP clients on XMPP server. The integration and support for these Presence sources depends on the overall solution capability in which you deploy Presence Services. At the time of publication of Presence Services 6.1, Avaya one-X<sup>®</sup> Communicator 6.0 does not support any external Presence sources.

---

### Adding Presence components

#### Procedure

1. Log in to the Presence Services XCP Controller Web interface.  
The URL format to open the Presence Services XCP Controller Web interface is `https://<IP address>:7300/admin`.
2. Select the component that you want to add.
3. Click **Go**.
4. Enter details of the component as outlined under the component description.
5. Click **Save**.

---

### Removing Presence components

#### Procedure

1. Log in to the Presence Services XCP Controller Web interface.  
The system displays the Presence Services XCP Controller main page.
2. Click **Stop** if the component is already running.

3. Once the component stops, click **Remove**.

 **Caution:**

Do not remove the system default components.

---

## Configuring Presence Components

---

### AES Collector

#### Adding AES Collector

##### Before you begin

- From System Manager, get the following information:
  - The AES IP address
  - The AES host name
  - The name of the Communication Manager instance
- From the XCP configuration, get the following information:
  - AES user name with unrestricted access. The user with unrestricted access has the **CTI User** field set to **Yes**.
  - AES user password.

To monitor the presence information of a user through AES Collector, ensure that you meet the following minimum requirements:

- Avaya Aura<sup>®</sup> Application Enablement Services version 6.1.3, with ASAI link version 5
- Avaya Aura<sup>®</sup> Communication Manager version 6.3.0

To monitor the presence information of a user through AES Collector that includes login and logout events, ensure that you meet the following minimum requirements:

- Avaya Aura<sup>®</sup> Application Enablement Services version 6.1.3.0.16, with ASAI link version 6
- Avaya Aura<sup>®</sup> Communication Manager version 6.3 patch 20654 or version 6.3 combo-patch 2363

##### About this task

You can add AES Collector if you did not install the software at the time of Presence Services installation. You cannot add multiple instances of AES Collector on the same Presence Services instance.

AES Collector can be used to monitor a maximum of 2500 endpoints.

**\* Note:**

To add AES Collector at the time of Presence Services installation, select the **AES Collector Component** field on the Presence Components page.

**Procedure**

1. Log in to the Presence Services XCP controller web interface.
2. In the Components section, select **Add a new AES Collector**, and click **Go**.
3. Modify the required fields, and then click **Submit**.
4. Return to the Presence Services XCP Controller home page to determine if the system has successfully added AES Collector.

The system displays a new entry in the Components section. For example, `aes-collector-1.presence`.

## Adding Communication Manager in System Manager

**Procedure**

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **Services > Inventory > Manage Elements** .
3. On the Manage Elements page, click **New**.
4. Select **CM** from the drop-down box to open the configuration page for a new Communication Manager instance.
5. Complete the following fields:
  - **Name**. Use a unique name
  - **Connection type**. Communication Manager
  - **Node**. IP address of your Communication Manager server
  - **Login, password and port**. Access fields for your Communication Manager server
6. Click **Commit**.
7. On System Manager Dashboard, click **Services > Scheduler > Completed Jobs** to check if the Communication Manager synchronization job is complete

This ensures that extensions from this Communication Manager are available for configuration in System Manager.

## Adding AES in System Manager

**Procedure**

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **Services > Inventory > Manage Elements** .
3. On the Manage Elements page, click **New**.
4. From the **Type** drop-down box, select .

5. Complete the following fields:
  - **Name.** The name of the application instance. It must be unique.
  - **Connection type.** The type of the application to which the application instance belongs, Application Enablement Services.
  - **Description.** A brief description about the application instance, Application Enablement Services.
  - **Node.** IP address of your Application Enablement Services server.
6. Expand **Access Point** then click **New**.
7. In the Access Points Details section, complete the following fields:
  - **Name.** The name of the access point.
  - **Access Point Type.** Displays the type of the access point.
  - **Protocol.** The protocol that the application instance supports to communicate with other communication devices.
  - **Host.** The name of the host on which the application instance is running.
  - **Port.** The port on which the application instance is running.
  - **Path.** Uniform Resource Identifier.
  - **Order.** The order in which the access points are accessed.
8. Click **Save**.
9. Expand **Port** and then click **New**.
10. In the Port Details section, complete the following fields:
  - **Name.** Name of the port.
  - **Protocol.** The protocol associated with the corresponding port.
  - **Port.** The port on which the application instance is running.
  - **Description.** A brief description about the port.
11. Click **Save**.
12. Click the **Assign Application** tab on top of the screen.
13. On the Assign Applications screen, select an application, and then click **Assign**.
14. Select the assigned application and the click **Edit** to populate the Assignment Name.

The Assignment Name must contain the name of the Communication Manager as it is configured at the AES (Switch Connection Name).
15. Click **Commit**.

## Related Links

[AES certificates](#) on page 53

## AES certificates

Generally, you configure Presence Services with an AES Collector to connect to a particular AES. By default, an AES comes with a certificate that can be validated by the default Avaya CA certificate. Presence Services accesses this CA certificate when it connects to an AES through its AES Collector. So the connection between Presence Services (through the AES Collector) and AES works automatically.

However, an administrator can change the AES certificate. Then this automated validation of the AES certificate does not happen. In this case, you must update Presence Services with the CA certificate that can validate this new AES certificate. You can do this by moving the CA certificate, in PEM format, over to the Presence Services system. To do this, you must run:

```
$PRES_HOME/presence/bin/prescert addTrusted pem <path to CA cert> alias
<for example, "CACertForAES">
```

### \* Note:

For more information on using the prescert script, go to the *Maintenance Operations* chapter in *Administering Avaya Aura® Presence Services*.

When the AES certificate is self-signed, you can use the AES certificate itself as the CA certificate.

### Related Links

[Adding AES in System Manager](#) on page 51

## Adding AES user handles for H.323 on System Manager

### Procedure

1. Log in to System Manager Web Console as an administrator.
2. Click **Users > User Management > Manage Users**.  
The system displays the User Management page.
3. Select the relevant user and click **Edit**.  
The system displays the User Profile Edit page.
4. On the **Communication Profile** tab, in the Communication Address section, click **New**.
5. From the **Type** drop-down box, select **Avaya E.164**.
6. In the **Fully Qualified Address:** field, enter the handle and domain details. For example, in the **Handle** field, enter +35311230121.  
The system displays the value for the **Domain** field by default.
7. Click **Add**.

Traditional H.323 hard phones in a Avaya one-X® Communicator deployment do not work through SIP. Since the H.323 hard phones do not need SIP support in this solution, Session Manager is also not required. Therefore, the AES Collector collects the presence of H.323 hard phones and sends the presence to Presence Services.

**\* Note:**

1XC-H323 users do not need and should not be configured to collect presence through AES. The system capacity reduces if you configure AES collection for 1XC-H323 users.

## Using an AES Collector for monitoring an endpoint

### About this task

The Avaya users are of two categories:

- Those who have an endpoint device that is capable of publishing the presence state information. For example, Avaya one-X<sup>®</sup> Communicator is capable of publishing presence state by using SIP or XMPP. In this case, using AES Collector to monitor the presence state is not recommended.
- Those who have an endpoint device that is not capable of publishing the presence state information. For example, Avaya 96x0 or non-SIP 96x1 deskphones cannot publish presence state. In this case, AES Collector must be used to monitor the presence state.

### Procedure

1. Assign an AES Collector system default value. For more information, see *Assigning an AES Collector system default value*.
2. Enable an AES Collector on per-user basis. For more information, see *Enabling an AES Collector on per-user basis*.

### Related Links

[Assigning the system default value to AES Collector](#) on page 54

[Enabling an AES Collector on a per-user basis](#) on page 55

## Assigning the system default value to AES Collector

### About this task

After adding AES Collector, you can assign the system default value. This value specifies whether the endpoint devices use AES Collector to publish presence state information

### Procedure

1. Log in to the System Manager web console.
2. Click **Elements > Presence**.  
The system displays the Presence page.
3. Click **Configuration**.  
The system displays the Presence Configuration Properties page.
4. Click **Edit**.
5. For the **Publish Presence with AES Collector - Default** field, select one of the following options from the **Value** drop-down box:
  - **Off**: If you set the value to **Off**, users cannot publish presence information using AES Collector.

- **On**: If you set the field to **On**, users can publish presence information using AES Collector.
6. Click **Save**.

### Related Links

[Using an AES Collector for monitoring an endpoint](#) on page 54

## Enabling an AES Collector on a per-user basis

### About this task

During or after creating a user in System Manager , you can enable or disable AES Collector.

### Procedure

1. Log in to the System Manager web console as an administrator.
2. Click **Users > User Management > Manage Users**.  
The system displays the User Management page.
3. Select the user, and click **Edit**.
4. On the **Communication Profile** tab, select the **Presence Profile** check box.  
The system displays the Presence Profile fields.
5. From the **Publish Presence with AES Collector** drop-down box, select one of the following values:
  - **System Default**: The system default value is applied to the user. The system default value is specified in the **Publish Presence with AES Collector – Default** field on the **Elements > Presence** page.
  - **Off**: To prevent the user from publish presence information using AES Collector.
  - **On**: To allow the user to publish presence information using AES Collector.

#### **Note:**

To override the value of **System Default**, change the setting to **On** or **Off**.

6. Click **Commit** to save the changes.

### Related Links

[Using an AES Collector for monitoring an endpoint](#) on page 54

## AES Collector configuration reference

### Related Links

[AES Collector Configuration basic parameters](#) on page 56

[AES Collector Configuration advanced parameters](#) on page 56

## AES Collector Configuration basic parameters

### *Description*

This parameter figures in the Components area on the main page of Presence Services XCP Controller Web interface. It helps you distinguish between components of the same type when you have more than one configured components. You can change the description as needed.

### *AES Collector component*

The properties in this section are specific to the AES Collector Component.

### *Default AES Username*

The default user name that the collector uses when connecting to an AES. When Presence Services connects to an AES to monitor an endpoint, it uses this user name unless an Override by AES item has been created for the AES, in which case the user name supplied on the Override By AES page is used.

### *Default AES Password*

The default password that the collector uses when connecting to an AES. When Presence Services connects to an AES to monitor an endpoint, it uses this password unless an Override by AES item has been created for the AES, in which case the password supplied on the Override By AES page is used.

## AES Collector Configuration advanced parameters

### *AES Collector Component*

### *Default Publish DND Status*

The DND or Do Not Disturb feature can be configured for endpoints on an Avaya Communication Manager the feature button within Communication Manager is called **SendAllCalls**. If an endpoint is configured so that it has the use of the SendAllCalls feature, its handset can have a **SendAllCalls** button that can be used to turn on and off the endpoint's DND status. However, early versions of the AES (before 4.1) and Communication Manager (before 5.0) software are not able to dynamically transmit this information to Presence Services. Machines running these early versions of the AES/Communication Manager software transmits the **SendAllCalls** state of an endpoint just once when Presence Services first starts watching it. Later updates to the **SendAllCalls** state are not transmitted. An endpoint that had a basic status of closed when Presence Services first started watching it because its SendAllCalls state was on will retain this status for as long as Presence Services watches it, despite any later changes to the state of its **SendAllCalls** button. For this reason, the **Default Publish DND Status** must be set to **No**, if any of your servers runs AES software prior to version 4.1 or CM software that predates version 5.0.

If **Default Publish DND Status** is set to **No** then no DND information will be published by Presence Services for any endpoint whether **SendAllCalls** buttons are on or off.

If the **Default Publish DND Status** is set to **Yes** and if an endpoint's **SendAllCalls** button is on, Presence Services publishes a DND activity element for that endpoint and its basic status is set to closed.

The **Default Publish DND Status** can be overridden for a particular AES/CM combination with an Override by Communication Manager item embedded in an Override by AES item.

**Add a new parameter override by AES**

The Parameter Override XCP web pages cannot be used to tell the collector which AES or Communication Manager (CM) hosts to connect to but influences how a connection to the indicated AES or AES/CM is made and managed. The Parameter Override By AES page can be used to change the user name/password used with a particular AES.

**! Important:**

The IP Address field must match the Node field in System Manager. To verify the value:

1. Log in to System Manager Web Console.
2. On System Manager Dashboard, click **Services > Inventory > Manage Elements**.
3. Select the AES element and then click **Edit**.
4. Ensure that the value in the **Node** field matches with the IP Address field.

The value for the Node or IP Address field is case sensitive, ensure that you enter the same value for both the fields.

The Parameter Override By Communication Manager page can be used to prevent specific types of connections and control DND reporting for a specific AES/CM pair. For instance, prevent a Named Licensing connection to a host running AES 4.2.0.

**Time (minutes) endpoint is on-hook until being declared Away**

AES Collector starts the Time (minutes) endpoint is on-hook until being declared Away timer when an endpoint goes on-hook. The unit of the timer is Minutes. The default value of the field is 0. You can set values between 0 and 1440 (equivalent of 24 hours). If you enter 0, the system disables the Time (minutes) endpoint is on-hook until being declared Away timer.

When the Time (minutes) endpoint is on-hook until being declared Away timer expires, the system changes the presence of the endpoint from available to away.

**Time (minutes) endpoint is Away until being declared Out Of Office**

AES Collector starts the Time (minutes) endpoint is Away until being declared Out Of Office timer when the endpoint goes off-hook. The unit of the timer is Minutes. The default value of the field is 0. You can set the values between 0 and 10080 (equivalent of 1 week). If you enter 0, the system disables the Time (minutes) endpoint is Away until being declared Out Of Office timer. If the value of the Time (minutes) endpoint is on-hook until being declared Away timer is set to 0, the system disables the Time (minutes) endpoint is Away until being declared Out Of Office timer even if you enter a value greater than 0.

When the Time (minutes) endpoint is Away until being declared Out Of Office timer expires, the system changes the presence of the endpoint to Out of Office.

---

## **Adding Microsoft OCS/Lync SIP user handles to System Manager Procedure**

1. Log on to System Manager web Console as an administrator.

2. On System Manager Dashboard, click **User Management > Manage Users**.
3. On the User Management page, select the relevant user and click **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. On the Communication Profile page, click **New** in the Communication Address section.
6. From the **Type** drop-down list box, select **Microsoft OCS SIP**.
7. In the **Fully Qualified Address:** field, enter the handle and domain details.

For example, in the **Handle** field, enter `sip:handle` and in the **Domain** field, enter `ocsdomain.com`.

8. Click **Add**.

---

## SIP Proxy Configuration

The SIP Proxy configuration must be changed if you have added, removed, or reconfigured the SIP Gateway for OCS.

---

## SIP Proxy Transport field descriptions

### PS IP Address

IP address of the Presence server.

### PS FQDN

Fully Qualified Domain Name (FQDN) of the Presence server.

### Cm name

The name of the OCS Connection Manager component as displayed on the Presence Services XCP Controller Web page without the Presence Services Realm. By default, this is *cm-1* or *cm-2*.

### Bulksub name

The name of the SIP Bulk Subscription Server component as displayed on the Presence Services XCP Controller Web page without the Presence Services Realm. By default, this is *sip-bulksub-1*.

### Ps name

The name of the SIP Presence Server component as displayed on the Presence Services XCP Controller Web page without the Presence Services Realm. By default, this is *sip-ps-1*.

---

## SIP Proxy remote host field descriptions

### PS IP Address

IP address of the Presence server.

### PS FQDN

Fully Qualified Domain Name (FQDN) of the Presence server.

### OCS SIP edge

The host name of the OCS Edge server.

### OCS SIP domain

The SIP domain used by the OCS servers.

---

## SIP Proxy Routing Rules field description

### PS IP Address

IP address of the Presence server.

### PS FQDN

Fully Qualified Domain Name (FQDN) of the Presence server.

### OCS SIP edge

The host name of the OCS Edge server.

### OCS SIP domain

The SIP domain used by the OCS servers.

### CM name

The name that the AES associated with the parent override page uses to identify a CM. This field is required. If the collector needs to monitor an endpoint through a connection to this AES/CM combination, it will use the settings entered on the two override pages instead of the common settings entered on the AES Collector Configuration page.

### Bulksub name

The name of the SIP Bulk Subscription Server component as displayed on the Presence Services XCP Controller Web page without the Presence Services Realm. By default, this is *sip-bulksub-1*.

## Ps name

The name of the SIP Presence Server component as displayed on the Presence Services XCP Controller Web page without the Presence Services Realm. By default, this is *sip-ps-1*.

## Microsoft Exchange Collector integration

### Overview

Exchange Collector is a Presence Server component which provides integration with an Microsoft (MS) Exchange Enterprise deployment. Exchange Collector collects and publishes the Calendar and Out of Office Assistant information for Exchange Mailboxes. The Exchange Mailbox servers manage Exchange Mailboxes.

The Exchange server provides an availability service, which makes the free or busy information of the users available to the external clients. Exchange Collector functions as one of these clients. Exchange Collector uses the polling mechanism to collect the Calendar and Out of Office Assistant records from the Exchange server by using MS Exchange Web Service (EWS) and converts the Calendar and Out of Office Assistant records into the presence information in the PS PIDF format. Using the publishing services of the IPS framework, Presence Services publishes the presence information as a presence fragment.

Presence Services 6.2 supports the following versions of MS Exchange Server:

- 2007
- 2010
- 2010 Service Packs

 **Note:**

One Presence server supports only one Exchange Collector.

### Related Links

[Checklist for integrating Exchange Collector with Presence Services](#) on page 60

### Checklist for integrating Exchange Collector with Presence Services

#	Task	Server	Notes	✓
1	DNS Requirement: Ensure all Client Access Servers (CAS) in the Exchange deployments are resolvable by the Presence server.	Presence server		
2	Autodiscover Service: Ensure that the Presence server can resolve autodiscover.<yourExchangeDom	Presence server		

#	Task	Server	Notes	✓
	<i>ain</i> > to one of the CASs configured for autodiscovery.			
3	Add the Microsoft Exchange user handles to System Manager.	Presence server		
4	Create a new Active Directory user to be used as the Presence Services account.	MS Exchange server		
5	Set Full Access Permissions for Exchange Mailboxes.	MS Exchange server		
6	Configure Exchange Services for the autodiscover service on each CAS.	MS Exchange server		

### Related Links

[Overview](#) on page 60

## Install and configure Exchange Collector

### Exchange Collector XCP configuration

You can configure the Exchange Collector component during the installation or post installation of the Presence Services server. By default, Presence Services does not include the Exchange Collector component during the installation.

You can install Exchange Collector during:

- The Presence Services installation or post Presence Services installation
- The Silent installation
- The Software-only installation

### Parameters for configuring MS Exchange Collector on the Presence Services server

Configuration view	Field	Description	Default value	Required
Basic	Exchange Server Web Service URI	Specifies the MS Exchange Server Web services URI for one of the Exchange CASs in your organization. For optimum performance, set this server as Exchange Server which is CAS for most of the mailboxes of your organization.		Yes
Advanced	Calendar Refresh Interval, in mins	Specifies how often the system refreshes the Calendar information for users. This is the rate at	15	Yes

Configuration view	Field	Description	Default value	Required
		which the collector will poll the exchange server for users' availability and send the latest exchange presence tuple information internally to the XCP core.		
Advanced	Calendar Request Rate Per Minute	Specifies how many Calendar Information requests are forwarded to the Exchange server per minute.	10	Yes
Advanced	Out of Office Assistant Refresh Interval, in mins	Specifies how often the system must refresh the Out of Office Assistant information for users.	30	Yes
Advanced	Out of Office Assistant Request Rate Per Minute	Specifies how many Out of the Office Assistant requests must be forwarded to the Exchange Server per minute.   <b>Note:</b> The system makes the web service call for the Out of the Office Assistant information on a per user basis, unlike Calendar Information that the system calls for a batch of users.	360	Yes
Advanced	Publishing Interval, in mins	Specifies how often the system refreshes the published Calendar/Out of the Office Assistant Information for users.   <b>Note:</b> Only those users whose Calendar/Out of the Office Assistant Information has changed will be re-published each period.	5	Yes
Basic	Exchange User Name	Specifies the exchange user to authenticate with, when polling for Calendar/Out of the Office information from the Exchange Servers.		Yes

Configuration view	Field	Description	Default value	Required
		 <b>Note:</b> This should be the user login ID for a user with the required permissions to read mailbox information for the requested users.		
Basic	Exchange User Password	Specifies the password of the exchange user to authenticate with, when polling for Calendar/Out of the Office information from the Exchange Servers.		Yes
Basic	Confirm Password	Confirm password entered previously.		Yes

### Parameters for the Exchange Collector Component configuration during the silent installation

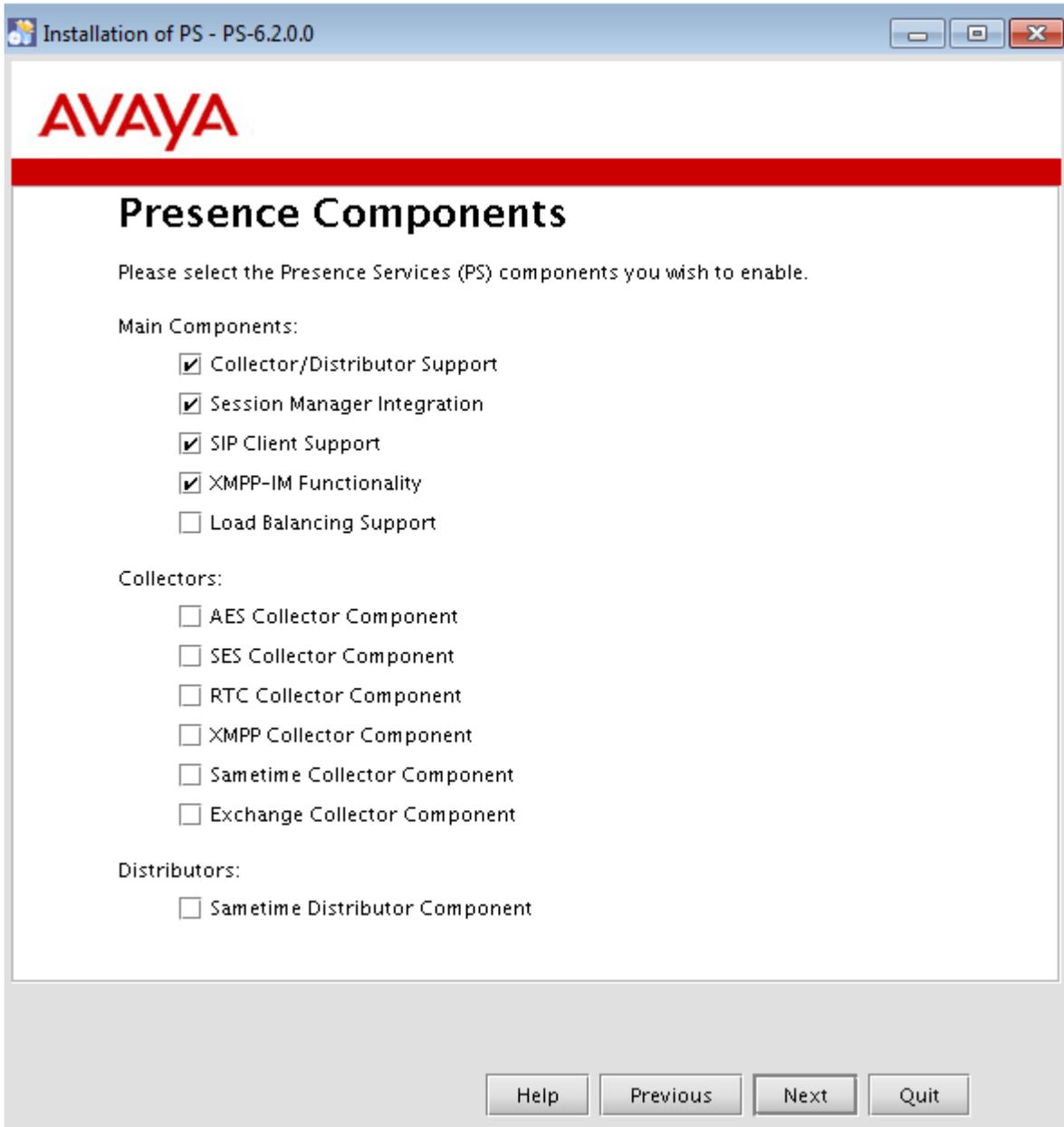
You can add Exchange Collector Component during the Presence Services silent installation by specifying the Exchange configuration parameters in the autoInstall\_PS.properties file. The following configuration parameters, except for inclEXC, have a one-to-one mapping with the XCP configuration parameters.

Field	Description
inclEXC	<ul style="list-style-type: none"> <li>To install Exchange Collector, set to <b>true</b>.</li> <li>To prevent the installation of Exchange Collector, set to <b>false</b>.</li> </ul>
EXC_URI	This corresponds to the XCP parameter: Exchange Server Web Service URI.
EXC_CALENDAR_REFRESH_RATE	This corresponds to the XCP parameter: Calendar Refresh Interval (mins).
EXC_CALENDAR_REQUEST_RATE	This corresponds to the XCP parameter: Calendar Request Rate Per Minute.
EXC_OOTO_REFRESH_RATE	This corresponds to the XCP parameter: Out of Office Assistant Refresh Interval.
EXC_OOTO_REQUEST_RATE	This corresponds to the the XCP parameter: Out of Office Assistant Request Rate Per Minute.
EXC_PUBLISHING_PERIOD	This corresponds to the XCP parameter: Publishing Interval (mins).
EXC_USERNAME	This corresponds to the XCP parameter: Exchange User Name.
EXC_USERPASS	This corresponds to the XCP parameter: Exchange User Password.

When you configure Exchange Collector Component during the installation, Exchange Collector Component starts automatically after you start the Presence Services server. There is a 2 minute delay during the Presence Services server start up process and before Exchange Collector attempts to connect to the configured Exchange server. This delay is to allow for the System Manager replication to complete. After the 2 minute delay, Exchange Collector publishes the initial calendar status, *Available*, for all the exchange handles. Subsequent status publishing occurs at each publishing period, and the system publishes only those mailboxes whose status information changes again.

### **Installing Exchange Collector Component during the Software-only installation Procedure**

1. On the Presence Components screen, select the **Exchange Collector Component** option and click **Next**.



2. On the Exchange Component Configuration screen, enter the following details:

Field	Value
<b>Exchange Server Web Service URI</b>	Enter the Web Service URI of Exchange Server.
<b>Calender Refresh Interval (mins)</b>	15
<b>Calender Request Rate Per Minute</b>	10
<b>Out Of Office Assistance Refresh Interval (mins)</b>	30

Field	Value
<b>Out Of Office Assistance Request Rate Per Minute</b>	360
<b>Publishing Interval (mins)</b>	5
<b>Exchange User Name</b>	Enter the Exchange user name.
<b>Exchange User Password</b>	Enter the Exchange user password.
<b>Retype Password</b>	Enter the password again.

3. To continue with the installation, click **Next**.

For information on the remaining installation steps, see *Deploying Avaya Aura® Presence Services*.

## Installing Exchange Collector Component after the Presence Services installation

### About this task

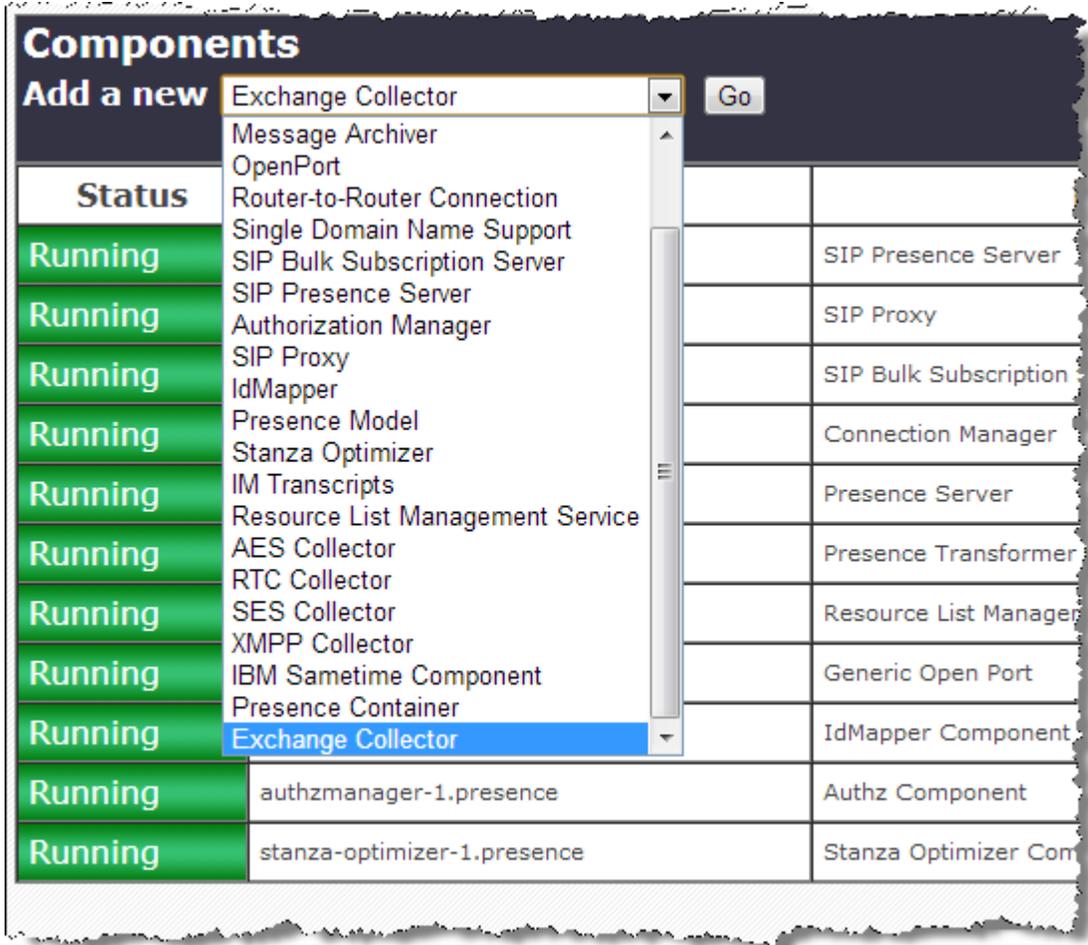
You can enable Exchange Collector Component after the Presence Services installation using the XCP Controller Web console.

 **Note:**

You cannot add multiple Exchange Collectors to the same Presence Services system.

### Procedure

1. Log in to the Presence Services XCP Controller Web console.
2. In the **Add a new** drop-down list, select **Exchange Collector** and then click **Go**.



The system displays the Exchange Collector Configuration page. By default, the system displays the basic configuration view, but you must switch to the advanced configuration view.

**Exchange Collector Component**  
**Exchange Collector Configuration**

Exchange Server Web Service URI	<input type="text"/>
Calendar Refresh Interval (mins)	<input type="text" value="15"/>
Calendar Request Rate Per Minute	<input type="text" value="10"/>
Out Of Office Assistant Refresh Interval (mins)	<input type="text" value="30"/>
Out Of Office Assistant Request Rate Per Minute	<input type="text" value="360"/>
Publishing Interval (mins)	<input type="text" value="5"/>
Exchange User Name	<input type="text"/>
Exchange User Password	<input type="password"/>
Confirm Password	<input type="password"/>

3. To save the changes, click **Submit**.

Click **Home** to go back to the Presence Services XCP Controller Home page and check if the system displays the new entry in the Components section. For example, exchange-collector-1.presence.

4. After the Exchange Collector configuration finishes, restart the Presence Services server.

There is a 2 minute delay after startup, before Exchange Collector attempts to connect to the configured Exchange server. This delay is to allow for System Manager replication to complete.

After the 2 minute delay, the system publishes an initial Calendar status *Available* for all exchange handles. Subsequent status publishing occurs at each publishing period, and only those mailboxes whose status information has changed gets a new publish fragment.

### **DNS requirements for the Exchange Collector support on the Presence server**

For Exchange Collector to communicate with the Exchange CAS servers, Exchange Collector must resolve the URI of Exchange Web Services configured on each of the URI. For example, if the Exchange Web Service internal and external URLs for one of the Exchange CASs is https://CAS1-FQDN.<MyExchangeDomain.com>/EWS/Exchange.asmx. Then the Presence server must be able to resolve the CAS1-FQDN.<MyExchangeDomain.com domain.

If the URIs on internal and external Exchange Web Service on an Exchange CAS are different, then the Presence server must resolve both URIs.

In an organization, all the Exchange CAS servers, the Presence server must resolve mailboxes monitored by Exchange Collector Component.

### **The Exchange Collector configuration for the Exchange Autodiscovery service**

Exchange Collector uses the Exchange Autodiscovery service to retrieve all Exchange CAS that hosts the mailboxes monitored for presence.

For the Autodiscovery service to work:

- The Presence server must be able to resolve 'autodiscover.<ExchangeDomain.com>'. For example, autodiscover.MyOrganizationName.com to an Exchange CAS, which supports autodiscovery. For more information on how to configure the autodiscover service on Exchange, see *Microsoft documentation*.
- The Presence server must be able to resolve all Exchange CAS that hosts the mailboxes monitored for presence.

The Exchange deployment of an organization might consist of several CASs. Exchange Collector creates a list of CASs, using autodiscovery, and route the web service requests to the relevant CAS for each mailbox. Exchange Collector starts and communicates with the configured Exchange Server URI. Based on the assumption that a percentage of the mailboxes is hosted on the Exchange server, Exchange server routes the first request for each mailbox. If the Exchange server is unsuccessful in retrieving mailbox information, the system uses the Exchange server to call the autodiscovery service for retrieving the correct Exchange server URI for that mailbox, and stores the correct URI for future requests.

## Manually adding the Exchange user handles on System Manager Procedure

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **User Management > Manage Users**.
3. On the User Management page, select the relevant user and click **Edit**.  
The system displays the User Profile Edit page.
4. Click the **Communication Profile** tab.
5. In the **Communication Address** section, click **New**.
6. In the **Type** drop-down box, select **Microsoft Exchange**.
7. In the **Fully Qualified Address:** field, enter the handle and domain details.  
For example, in the **Handle** field, enter <mailbox\_user\_name> and in the **Domain** field, enter <mailbox\_my\_domain>.
8. Click **Add**.

 **Note:**

Repeat the procedure for each user who wants the exchange presence information.

## Verifying the Exchange Collector configuration

### Verifying the Exchange Server connection status

#### Before you begin

Ensure that:

- The Presence server can resolve each Exchange CAS in the organization and resolve the autodiscover service endpoint.
- You have the Presstatus tool. Use the presstatus tool on the Presence Services server to verify the connection status to each Exchange CAS.

#### Procedure

Log in to the Presence server and run the `>>$PRES_HOME/bin/presstatus` command.

```
Component: Microsoft Exchange Server (Disconnected)
```

```
Component: https://135.64.28.130/EWS/Exchange.asmx (Disconnected)
```

When the Exchange Collector starts, during the first 2 minutes, the Exchange Collector is in a Disconnected state, and the system displays the one configured Exchange Client Access Server as its only sub-component, also in a Disconnected state.

Once the Exchange Collector makes its first web service call to the configured Exchange Client Access Server, if the connection is successful, the status for this Exchange Server should change to "Connected". In addition, if the web service call results in a failure to read mailbox information for a handle, the system calls the autodiscovery service to determine the correct Exchange CAS for the handle. If the autodiscovery service is successful, the system adds another sub-component to the

list, although its connection will not yet have been tried, so the system displays a “Disconnected” state until the next refresh period.

Component: Microsoft Exchange Server (Partially Connected)

Component: https://135.64.28.130/EWS/Exchange.asmx (Connected)

Component: https://ex2010-agnew.agnew.com/EWS/Exchange.asmx (Disconnected)

During the next refresh period, the second sub-component connection will now be tested, and if it is successful in returning mailbox information for its handles, the status should now be Connected:

Component: Microsoft Exchange Server (Connected)

Component: https://135.64.28.130/EWS/Exchange.asmx (Connected)

Component: https://ex2010-agnew.agnew.com/EWS/Exchange.asmx (Connected)

### Guidelines for Exchange Collector performance tuning

The default configuration values are based on supporting a deployment of Presence Services server at the full capacity of users. Do not increase the request rates or decrease the refresh schedules for retrieving Calendar Information or Out of the Office Assistant because changing the values might result in a degradation of the Exchange Collector performance. If support for full capacity users is not required, these rates may be improved accordingly. The recommended defaults were devised through stress tests on the Exchange Server to determine how many requests could be handled per minute. The Request and Refresh Rates are configurable in the Advanced XCP Configuration view.

The Publishing Period default of 5 minutes is specified to control the rate of publishing requests to the core publishing framework which handles publishing requests for all the collectors. If this period is reduced, to allow for a more frequent refresh of presence status, it may impact on the core publishing framework, if it becomes overloaded with requests.

Field	Default value
Calendar Refresh Interval ( mins)	15
Calendar Request Rate Per Minutes)	10
Out of Office Assistant Refresh Interval (mins)	30
Out of Office Assistant Request Rate Per Minute	360
Publishing Interval (mins)	5

## Configure Exchange Server for Presence Services integration

### Exchange Server configuration for Presence Services integration

to integrate the Exchange deployment of an organization with Presence Services, perform the following steps on each CAS in the deployment:

- Apply full access permissions for the XCP configured Exchange User on Exchange Mailboxes.
- Allow for Exchange Collector retrieval of Calendar Event Subject Information.

- Configure Exchange Services for the Autodiscover service.

## Related Links

[Applying full access permissions for the XCP configured Exchange Users on Exchange Mailboxes](#) on page 71

[Allowing for Exchange Collector retrieval of Calendar Event Subject information](#) on page 71

[Exchange Services configuration for the Autodiscover service](#) on page 72

## **Applying full access permissions for the XCP configured Exchange Users on Exchange Mailboxes**

### **About this task**

Using the configured Exchange user account, the Exchange Collector Component polls the Exchange servers for the mailbox information. To read the Out of Office Assistant information from mailboxes, the user account must have Full Access Permission on the mailboxes.

Using the Exchange Management Shell, you can set full access permissions.

### **Procedure**

On Exchange Management Shell, type `Get-MailboxDatabase -identity [MailBox Database Name] | Add-ADpermission -user [Exchange Collector Username] -AccessRights GenericAll`.

Where,

- [MailBox Database Name] is the name of the Exchange Server Mailbox Database Name.
- [Exchange Collector Username] is the Exchange Collector username that you configure in XCP Controller.

Run this command only once. When you add new users, the Exchange Collector user will have full access permission to the new users' mailboxes.

For more information on setting Full Access Permissions, see *MS Exchange documentation*.

## Related Links

[Exchange Server configuration for Presence Services integration](#) on page 70

## **Allowing for Exchange Collector retrieval of Calendar Event Subject information**

### **About this task**

When the Exchange Collector retrieves calendar events for a mailbox from the Exchange server, the event includes the Subject content for each event, only if that particular mailbox has applied a permission setting in their Calendar Folder options.

To receive calendar events information, all the users must set these permissions.

### **Procedure**

1. Open your Outlook client.
2. Click **Calendar View > File > Folder > Calendar Permissions > Permission Level**.
3. Set the default permission to, Free/Busy, Subject, and Location.

The Calendar Event Subject permissions are applied at the individual mailbox level. When you set a permission, the Exchange Collector only collects the content of the Subject for an event and displays the event as a <note> in the published Exchange tuple. If the permission is not set, the <note> element in the Exchange tuple contains only the type of the Calendar Event. For example, Tentative, Out-Of-Office, or Busy.

For more information on setting Calendar Folder permissions, see the *MS Exchange documentation*.

### Related Links

[Exchange Server configuration for Presence Services integration](#) on page 70

#### **Exchange Services configuration for the Autodiscover service**

Exchange Collector Component uses the Exchange Autodiscover service to retrieve Calendar information for the mailboxes. Configure Exchange Services for the Autodiscover service on the CASs in the domain. This involves setting the internal and external URIs for the Exchange Web Services virtual directory on each CAS.

Typically, the system sets the internal URI by default and you need to set the external URI manually.

For example, to manually set the external URI using the Exchange Management Shell, do the following:

```
Set-WebServicesVirtualDirectory -identity "CAS01\EWS (Default Web Site)" -externalurl https://mail.contoso.com/EWS/Exchange.asmx -BasicAuthentication:$True>>
```

Alternatively:

```
>> Set-WebServicesVirtualDirectory -server <CAS Server hostname> -externalurl https://mail.contoso.com/EWS/Exchange.asmx
```

#### **\* Note:**

The Presence server must resolve the internal and external URIs specified for each CAS.

### Related Links

[Exchange Server configuration for Presence Services integration](#) on page 70

## Troubleshooting Exchange Collector

### Changing the default logging level

#### **About this task**

#### **Procedure**

1. Log in to the Presence server.
2. Edit the file, \$PRES\_HOME/presence/lib/path/log4j.xml
3. Uncomment and change the level in:  

```
<logger name="events.operational">  
<level value="WARN#com.avaya.common.logging.client.LogLevel"/>  
</logger>
```

**\* Note:**

The lower the level you set, the more log records are generated. You may not want to set a lower level for a long period of time to avoid having to navigate through unwieldy log files.

## Enabling logging for Exchange Collector

### Procedure

1. Log in to the Presence Services server.
2. Navigate to the `$PRES_HOME/presence/lib/path` folder.
3. Edit the `log4j.xml` file.
4. To enable the Exchange Collector logs, add the following code in the `log4j.xml` file:

```
<logger name="events.operational.com.avaya.presence.server.ExchangeCollector">
<level value="FINEST#com.avaya.common.logging.client.LogLevel"/>
</logger>
```

You can reduce the logging output by specifying a higher level such as FINER, FINE, or INFO instead of FINEST.

5. To enable the debug logging for the Exchange Collector component, add the following code in the `log4j.xml` file:

```
<logger name="com.avaya.apas.exchange">
<level value="FINEST#com.avaya.common.logging.client.LogLevel"/>
</logger>
```

You can reduce the logging output by specifying a higher level such as FINER, FINE, or INFO instead of FINEST.

### Example

Examples of logs:

#### Example 1

```
<FATAL> 2012-03-26 13:07:27,658 [Timer-156]
events.operational.com.avaya.presence.server.ExchangeCollector: OOTO refresh to short
or request rate to high or server unreachable for collection
```

```
< FATAL> 2012-03-26 13:07:27,658 [Timer-156]
events.operational.com.avaya.presence.server.ExchangeCollector: Calendar refresh to
short or request rate to high or server unreachable for collection
```

Either or both the log entries can indicate one of the following:

- The rate at which Calendar or Out of the Office (OOTO) requests are sent to Exchange Server might be too high for the number of mailboxes.
- The frequency at which Calendar or OOTO requests are sent to Exchange Server might be too high for the number of mailboxes.
- Problems with one Exchange Server that is polled. For example, if one server is temporarily turned off, requests sent to this server time out resulting in performance degradation. If the server does not process the requests quickly, a backlog is created.

### Example 2

```
<ERROR> 2012-03-26 13:31:10,644 [pool-4-thread-1]
events.operational.com.avaya.presence.server.ExchangeCollector:
  EXCHANGE Exception thrown on Exchange Calendar Web Service call: The request failed.
connect timed out; Cause: connect timed out
```

This log indicates that the server generates a time-out message while attempting to read the calendar information for mailboxes. A timeout can occur due to an error with the Exchange Server URI. The configured Exchange Server URI might be incorrect, the DNS might need to be updated if an Exchange Server URI has changed, or Exchange Server might be temporarily disconnected.

### Example 3

```
<FINEST> 2012-03-26 14:07:07,943 [pool-5-thread-1]
events.operational.com.avaya.presence.server.ExchangeCollector:
  EXCHANGE Exception thrown on Exchange Auto Discovery call: The Autodiscover service
couldn't be located.
```

This log entry indicates a problem with the autodiscovery service. Either the Presence Services server is unable to resolve autodiscover.<your\_Exchange\_domain> or the configured Exchange Server is not correctly set up for the autodiscovery service on the web services.

### Example 4

```
<FINE > 2012-03-26 14:05:31,998 [pool-4-thread-1]
com.avaya.apas.exchange.collector.calendar.CalendarCollectionTask:
  WARNING : Exchange Web Service UserAvailability response Errors:
attendeeAvailability.getErrorCode()=ErrorMailRecipientNotFound for handle:
<nonexistingexchangehandle@domain.com>
```

This log entry indicates that a mailbox is not found and that a provisioned mailbox, which is no longer a valid mailbox in the exchange deployment, is found.

### Example 5

```
<ERROR> 2012-03-26 14:20:12,377 [pool-4-thread-1]
events.operational.com.avaya.presence.server.ExchangeCollector:
  EXCHANGE Exception thrown on Exchange Calendar Web Service call: The remote server
returned an error: (401)Unauthorized
```

This exception is thrown when the configured Exchange user credentials are invalid. Verify that the XCP configured credentials for the Exchange user account are correct.

### Example 6

```
<FINEST> 2012-03-28 09:39:37,010 [pool-10-thread-1]
events.operational.com.avaya.presence.server.ExchangeCollector:
  EXCHANGE Exception thrown on Exchange Auto Discovery call: The Autodiscover service
couldn't be located.
<FINE>2012-03-28 09:39:37,010 [pool-10-thread-1]
com.avaya.apas.exchange.collector.ooto.OOTOCollectionTask:
  getUserAvailability for handle: joanne6@james.com seq= 168 took:100208 msec
```

This exception means that the attempt to autodiscover the URL for the mailbox was not successful because the server could not contact the autodiscover service for the mailbox domain. Verify that the autodiscover service is correctly set and the Presence Services server can resolve the autodiscover URL to one of the Exchange CASs. For more information, see *Exchange Services configuration for the Autodiscover Service*.

**Example 7**

```
<ERROR> 2012-03-28 10:00:16,679 [pool-11-thread-1]
events.operational.com.avaya.presence.server.ExchangeCollector:
  EXCHANGE Exception thrown on accessing Out of Office for mailbox:
smtp_pm_9904@agnew.com. Permissions not set.Access is denied. Check credentials and try
again.
```

This exception is thrown when the configured Exchange user does not have the required permissions to view an exchange mailbox.

---

## Domino Collector integration

### Domino Collector

Domino Collector is a Presence Services component that provides integration with IBM® Domino enterprise deployment. Domino Collector collects and publishes the calendar and out-of-office information to Domino mailboxes. The Domino server manages Domino mailboxes. The Domino Calendar web service, which is included in Presence Services, must be installed on the Domino server. The Domino Calendar web service processes the calendar and out-of-office web service requests. The Domino Calendar web service also retrieves email addresses from the web service requests, finds the corresponding calendar and out-of-office information, and sends the results to the web service client.

Domino Collector performs the following functions:

- Runs as a web service client for the Domino Calendar web service.
- Uses a polling mechanism to send web service requests to the Domino Calendar web service on the Domino server.
- Converts the retrieved calendar and out-of-office information into the presence information format. The presence information is published as a presence fragment using the Presence Services publishing framework.

Presence Services 6.2 supports Domino Server 8.5.3.

### Checklist for integrating Domino Calendar with Presence Services

No.	Task	Server	Link	✓
1	Ensure that Presence Services can resolve the URI of the Domino server.	Presence Services		
2	Install the Domino Calendar web service database on the Domino server.	Domino Server	<a href="#">Installing the Domino Calendar web service database</a> on page 76	
3	Sign the Domino Calendar web service database.	Domino Server	<a href="#">Signing the Domino Calendar web service</a>	

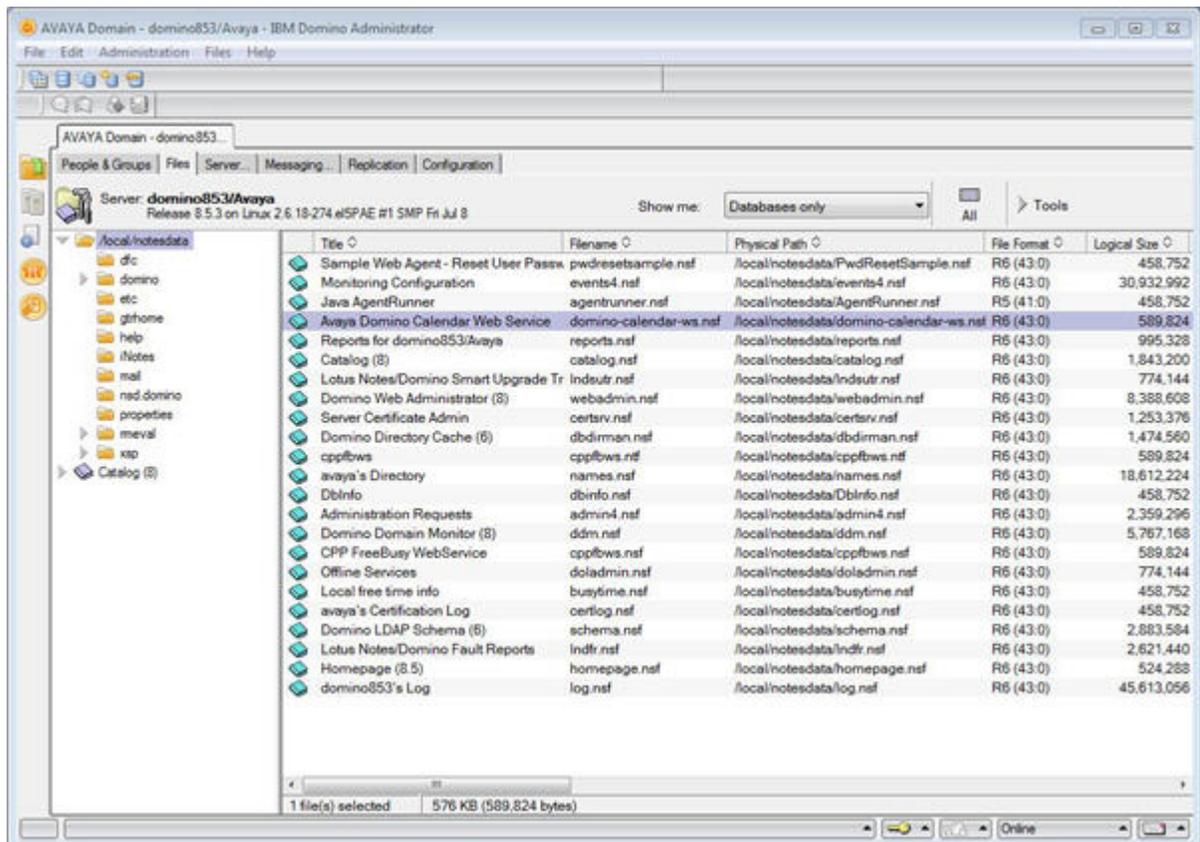
No.	Task	Server	Link	✓
			<a href="#">database</a> on page 77	
4	Create a new Domino user for Domino Collector.	Domino Server	<a href="#">Creating a Domino user for Domino Collector to authenticate</a> on page 79	
5	Provide access to the Domino user.	Domino Server	<a href="#">Providing reader access to the Domino user for Domino Collector to authenticate</a> on page 87	
6	Add Lotus Notes handle to the Domino user.	Presence Services	<a href="#">Adding Lotus Notes handle to a System Manager user</a> on page 91	
7	Configure Domino Collector.	Presence Services	<a href="#">Domino Collector configuration</a> on page 92	

## Installing the Domino Calendar web service database

### Procedure

1. Extract the Domino Calendar web service file, `domino-calendar-ws.nsf`, from the Presence Services software ZIP file.
2. Copy the `domino-calendar-ws.nsf` file to the `data` folder of the Domino server.  
For example, the location of the default data folder for a Domino server is:
  - `/local/notesdata` on a Linux installation.
  - `c:\Program Files (x86)\IBM\Lotus\Notes\Data` on a Windows installation.
3. Open the IBM Domino administrator client, and connect to the Domino server.

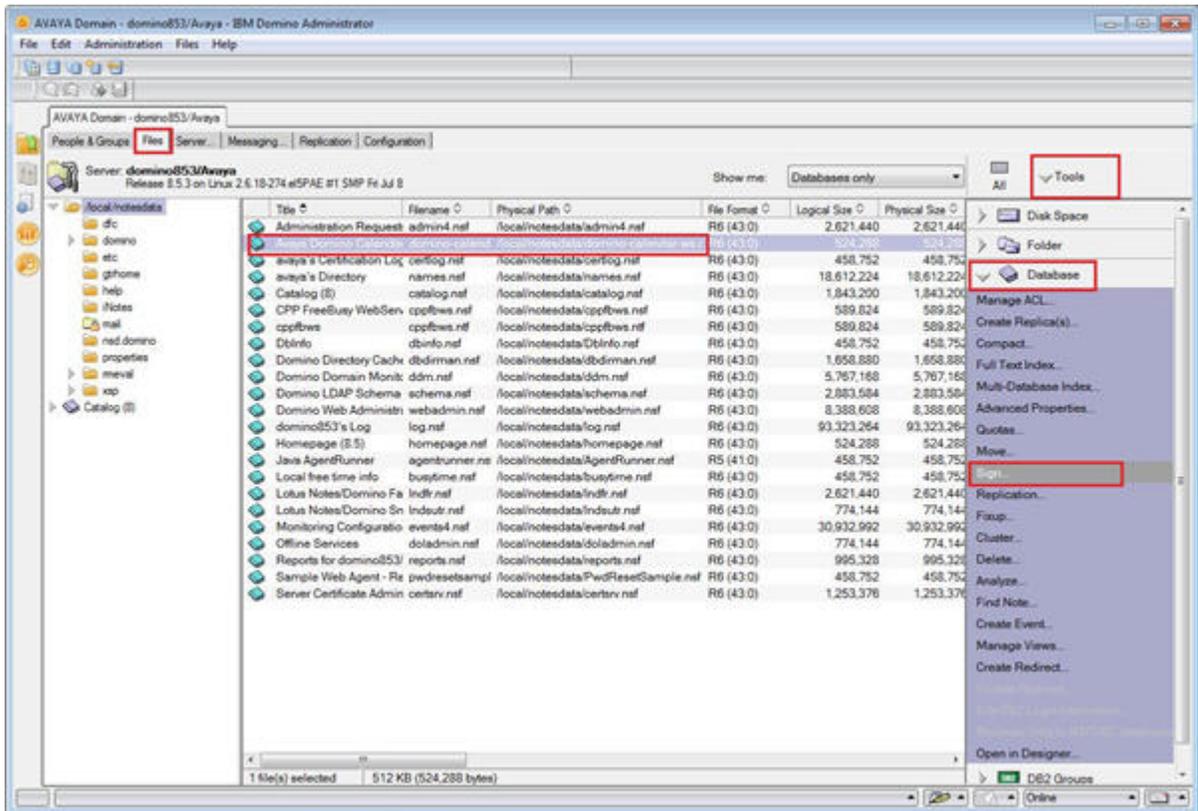
4. Ensure that the Avaya Domino Calendar web service is on the Domino server.



## Signing the Domino Calendar web service database Procedure

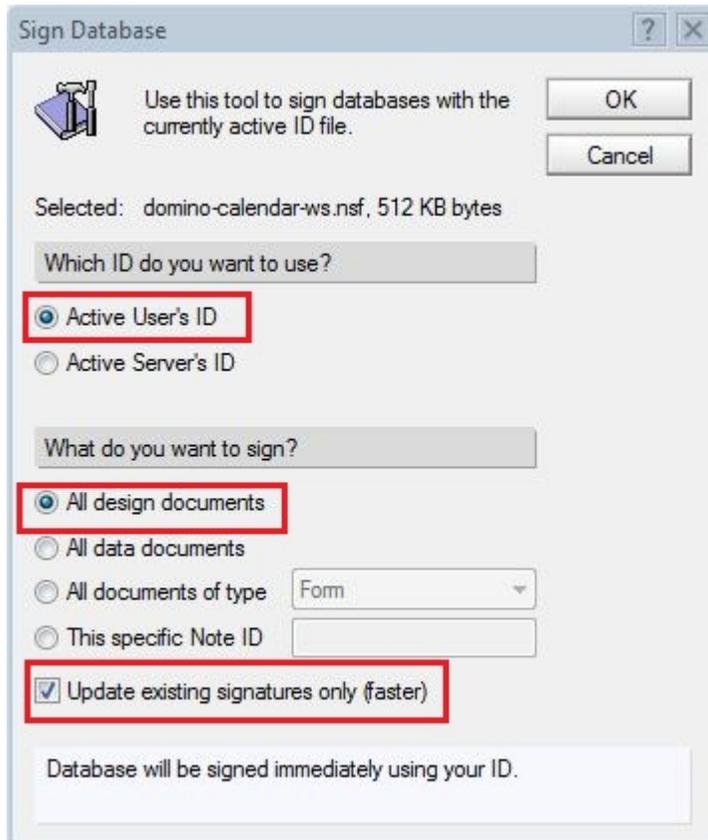
1. Log in to the Domino Administrator client with the administrator credentials.
2. Click the Domino server.
3. Click **Files**.

4. Select the **domino-calendar-ws.nsf** database.



5. Click **Tools > Database**.
6. Click **Sign**.
7. In the **Which ID do you want to use?** field, select **Active User's ID**.
8. In the **What do you want to sign?** field, select **All design documents**.

9. Select the **Update existing signatures only (faster)** check box.



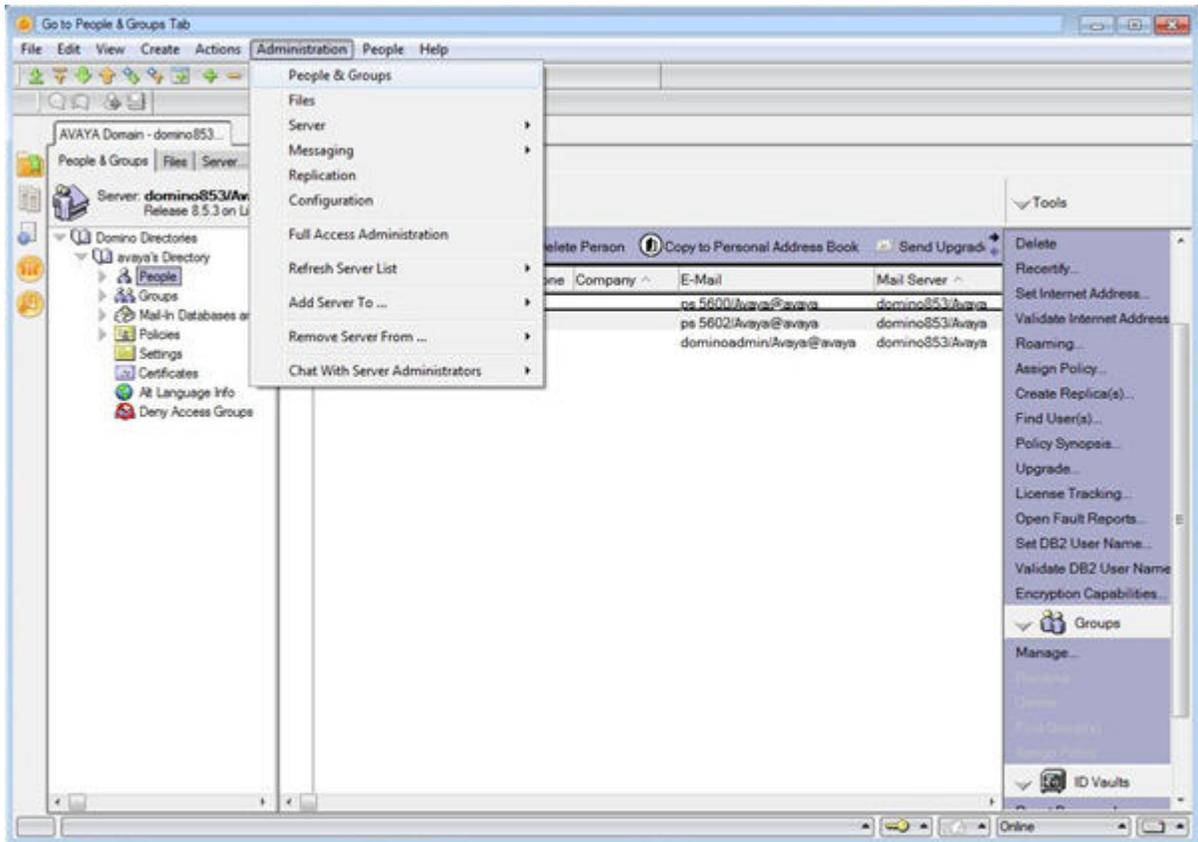
10. Click **OK**.

The system displays the **1 database processed - 0 errors** message.

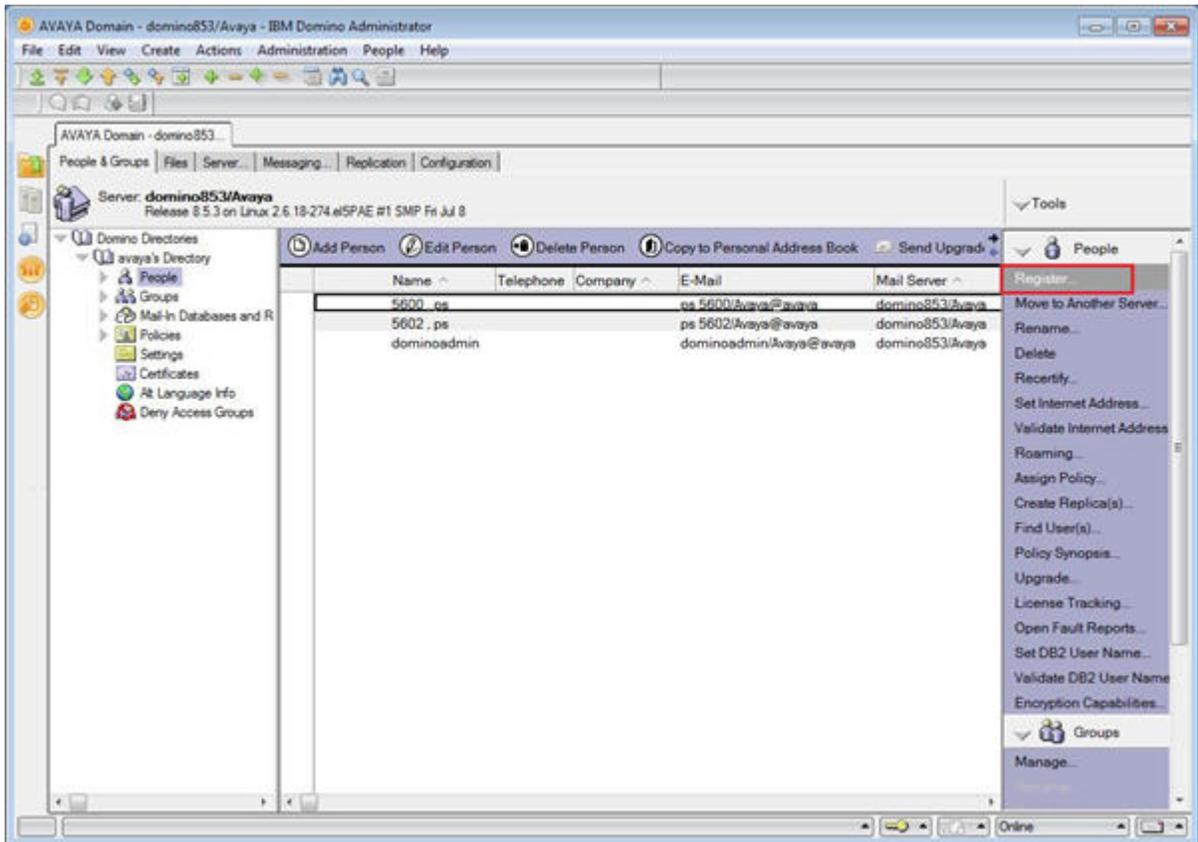
## Creating a Domino user for Domino Collector to authenticate Procedure

1. Log in to the Domino Administrator client.

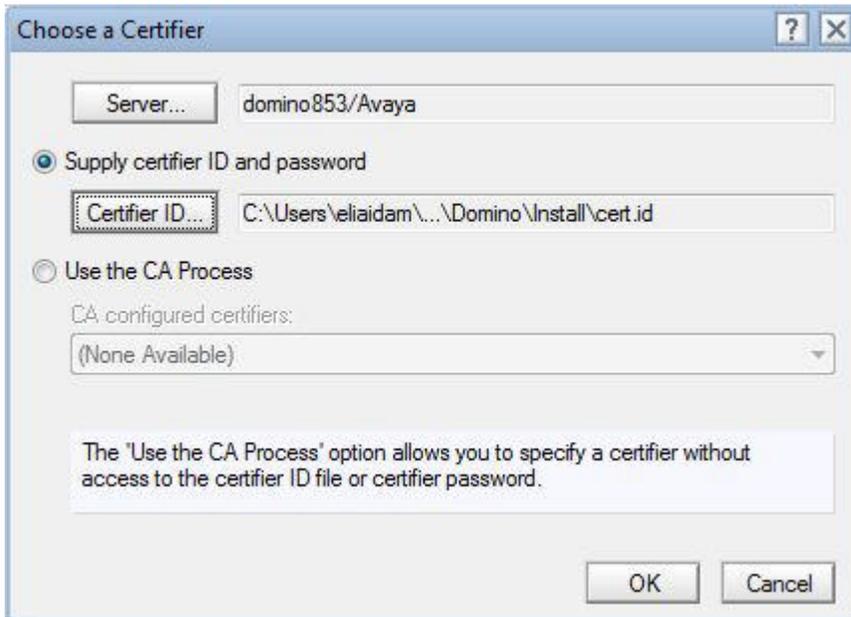
2. Click **Administration > People & Groups**.



3. Click **Register**.

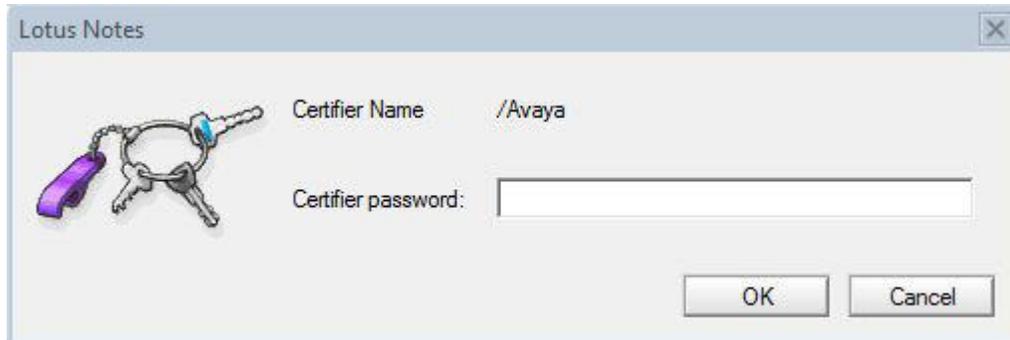


4. Click **Server**, and select the server.



## Configuring Presence Services components

5. Click **Certifier ID**, and select the Certifier ID.
6. Click **OK**.
7. In the **Certifier password** field, type the certifier password.



8. In the **Last name** field, type the last name.

9. In the **Password** field, type the password.

Register Person -- New Entry

**Basics**

Provide name, password and other basic information for the new person. To view/edit additional registration settings, check the 'Advanced' checkbox below.

Registration Server... domino853/Avaya

First name: Middle name: Last name: Short name:

psadmin psadmin

Password: 1234 Mail system: Lotus Notes Explicit policy: (None Available)

Password Options...

Enable roaming for this person

Create a Notes ID for this person

No organization policy assigned to this person

Policy Synopsis...

Advanced

New Person Migrate People... Import Text File... [OK] [Cancel]

Registration Queue (local):

^	User Name ^	Registration Status ^	Date ^

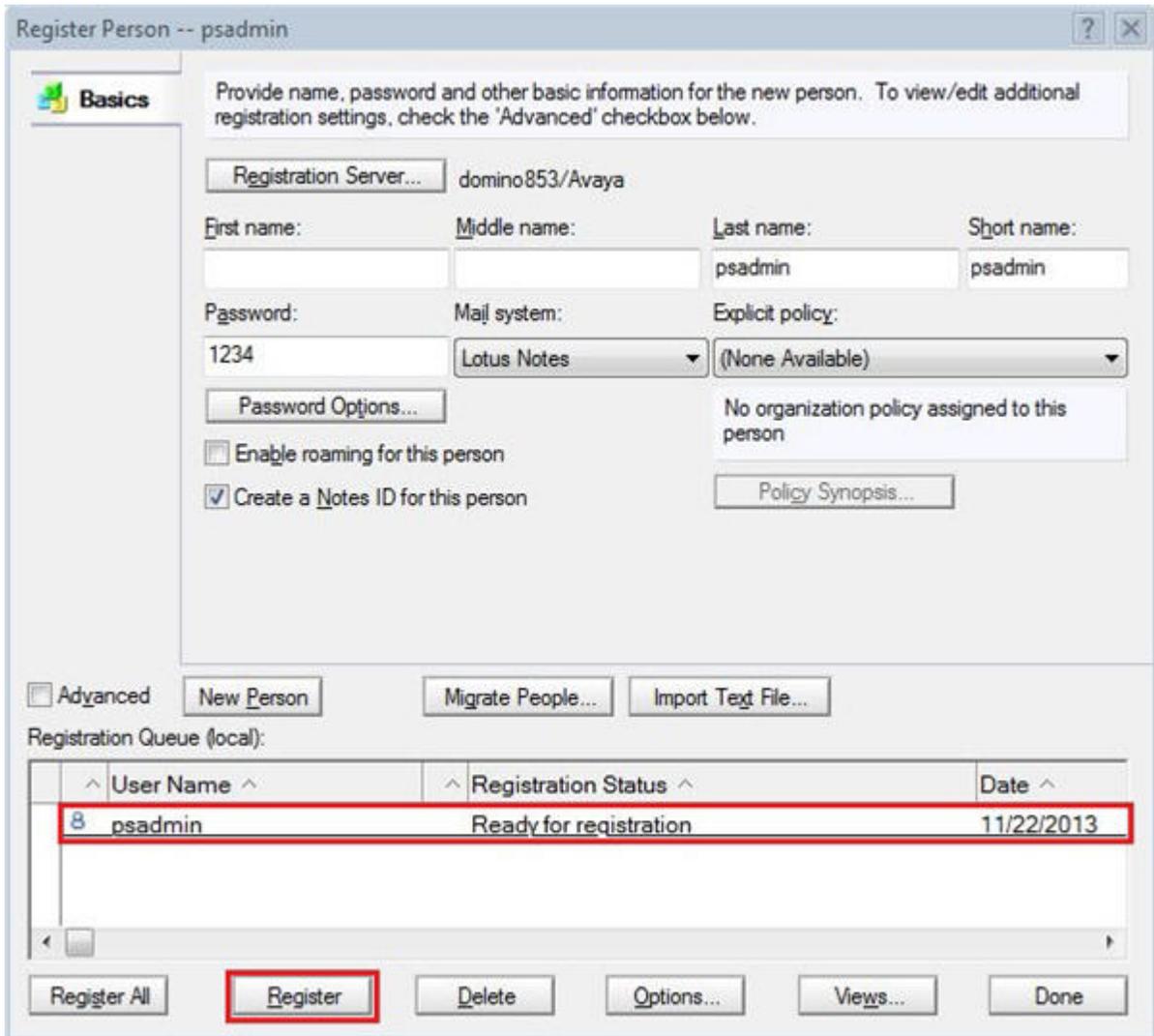
Register All Register Delete Options... Views... Done

10. On the **Password Options** page:
- Select the value of **Password Quality Scale**.
  - Select the **Set internet password** check box.
  - Click **OK**.



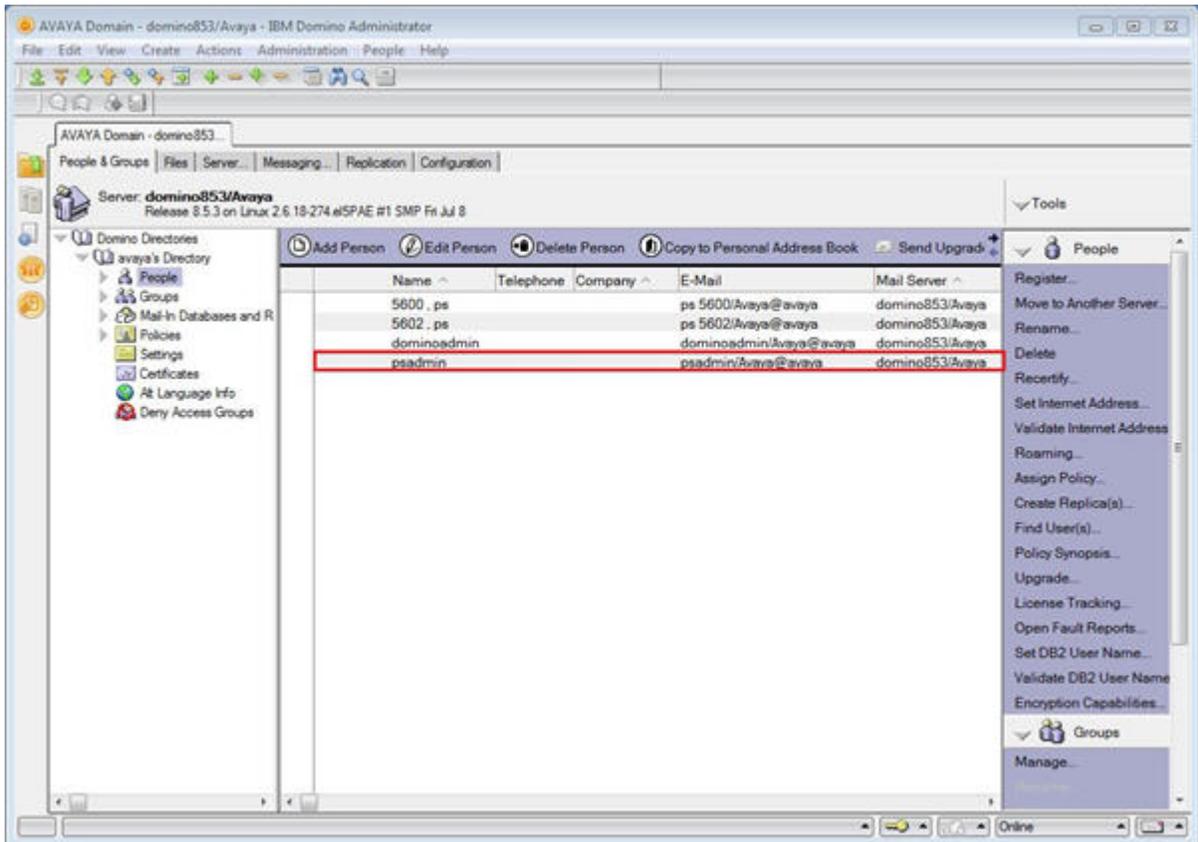
11. Select the green check mark box.

12. Select the user, and click **Register**.

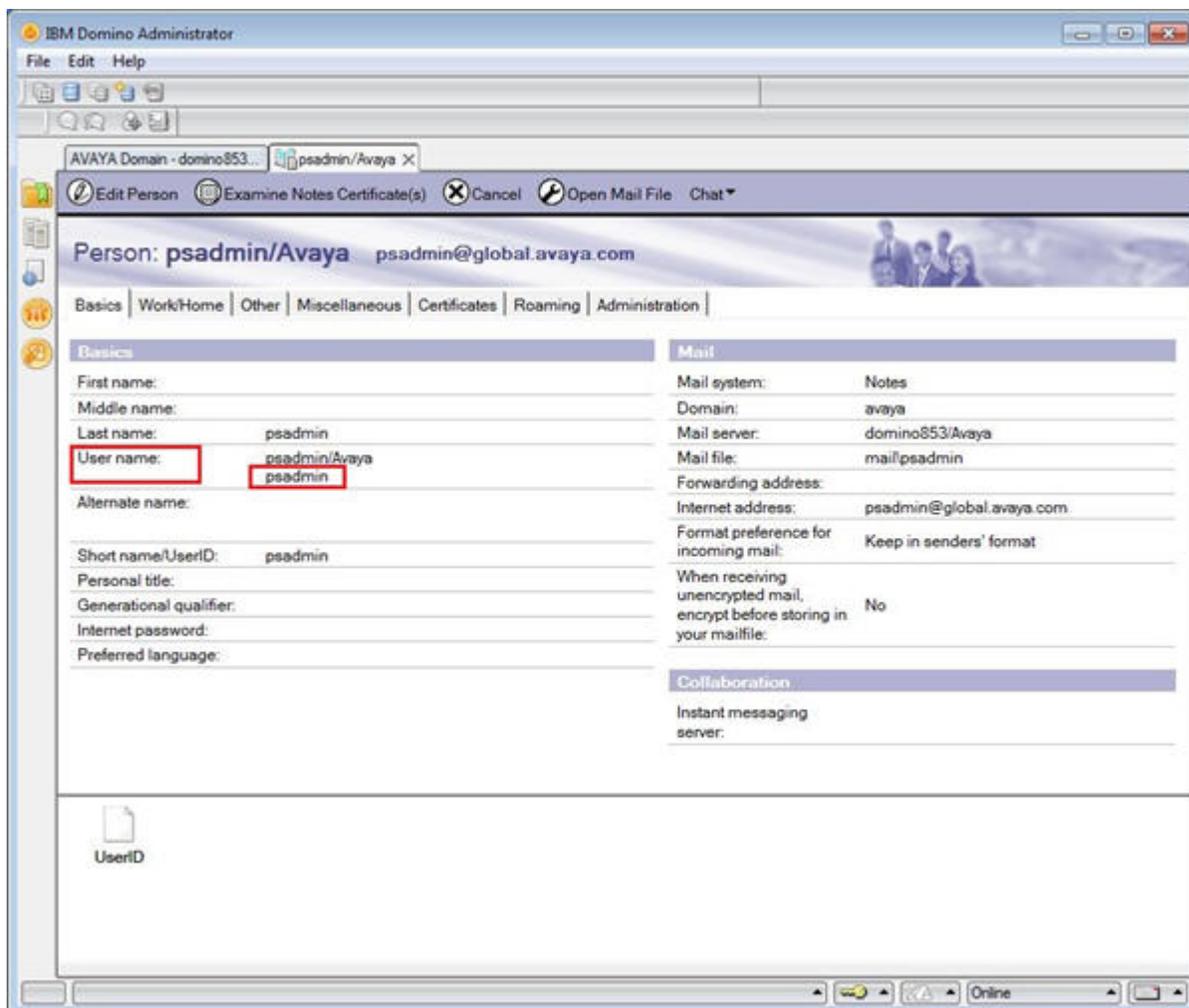


13. Click **OK**.
14. Click **Done**.

15. Verify that the new user is listed in the folder.



16. Double-click the user to see the information about the user.  
Note the entry in the **User name** field.



## Providing reader access to the Domino user for Domino Collector to authenticate

### About this task

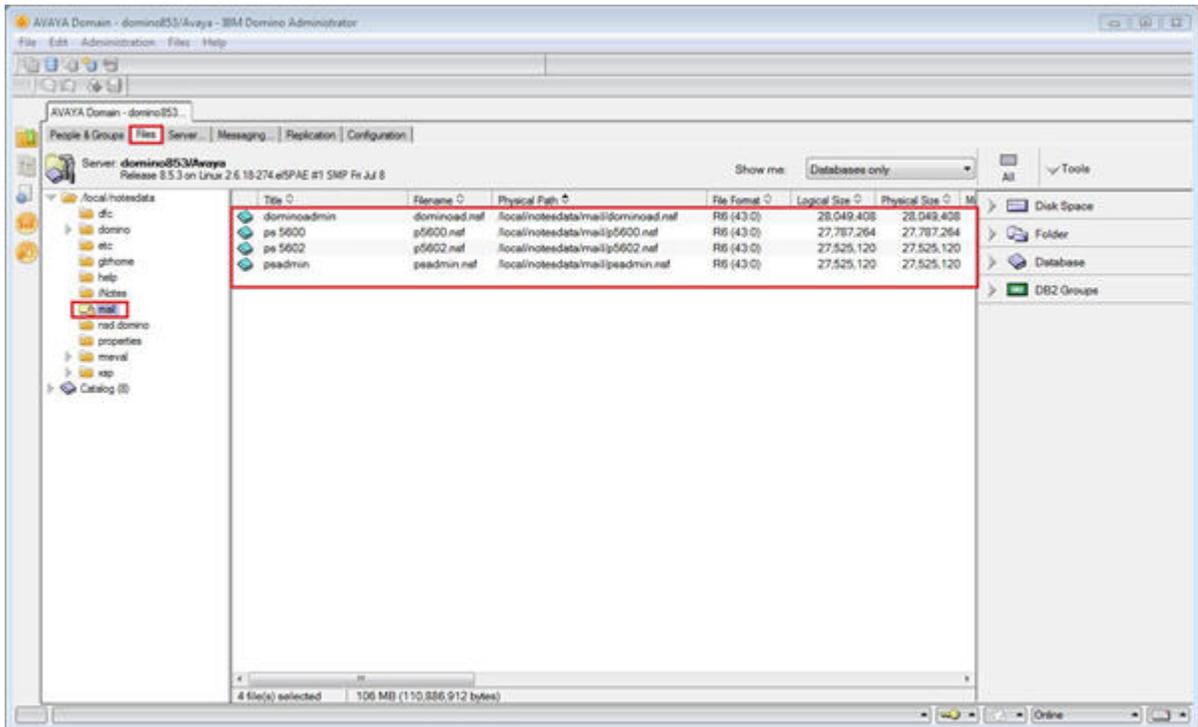
A Domino user needs reader access to mails of the users whose calendar or out-of-office information must be collected.

### Procedure

1. Log in to the Domino Administrator client.

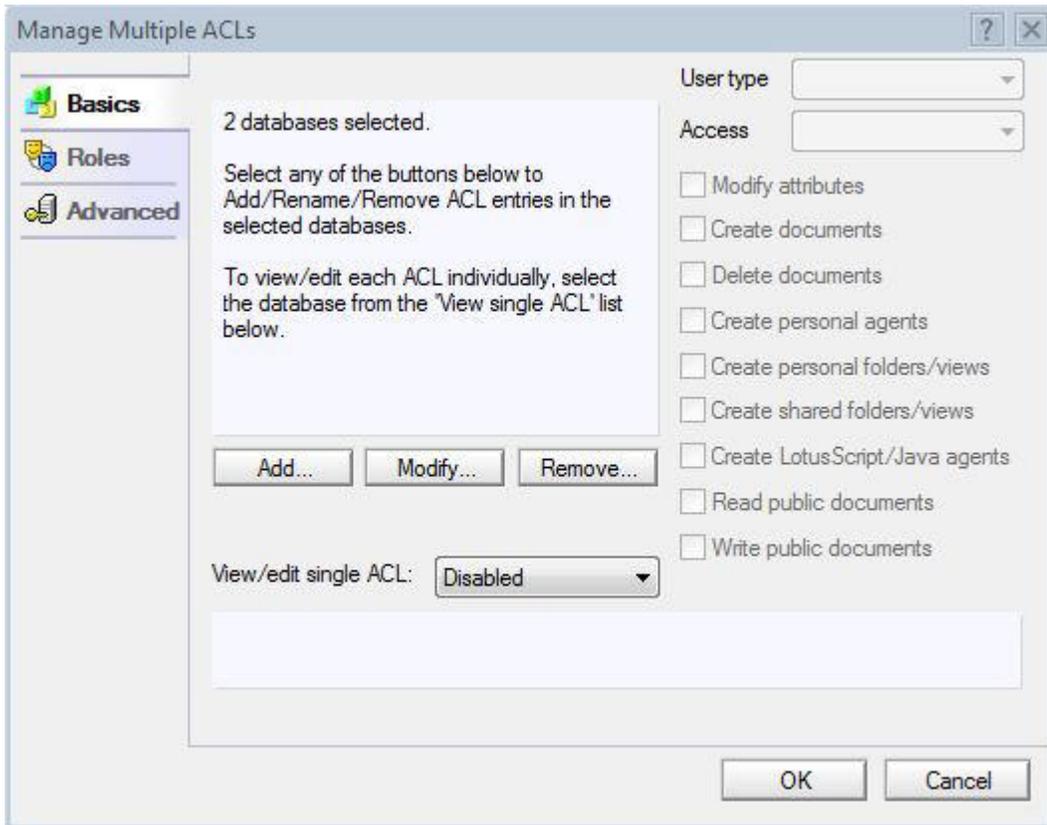
## Configuring Presence Services components

2. Click **Files**, and navigate to the `/local/notesdata/mails` folder.



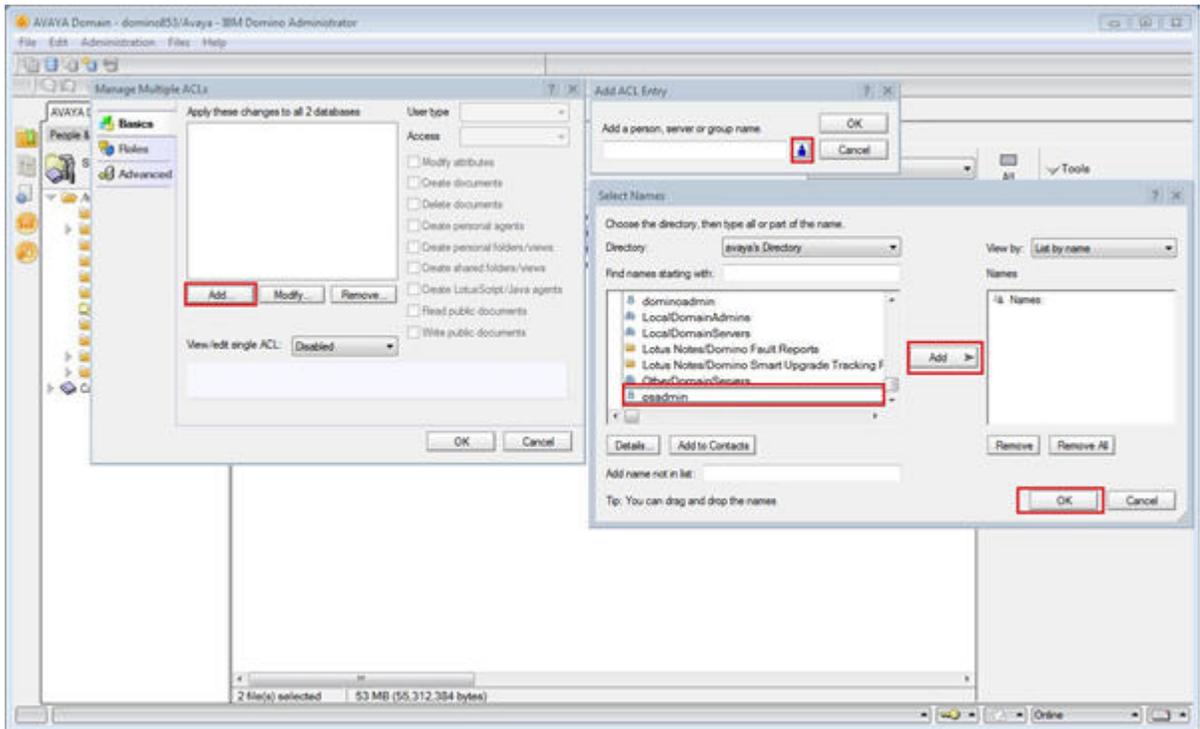
3. Select the mail files that you need to modify.

- Right-click the selected files, and click **Access Control > Manage**.



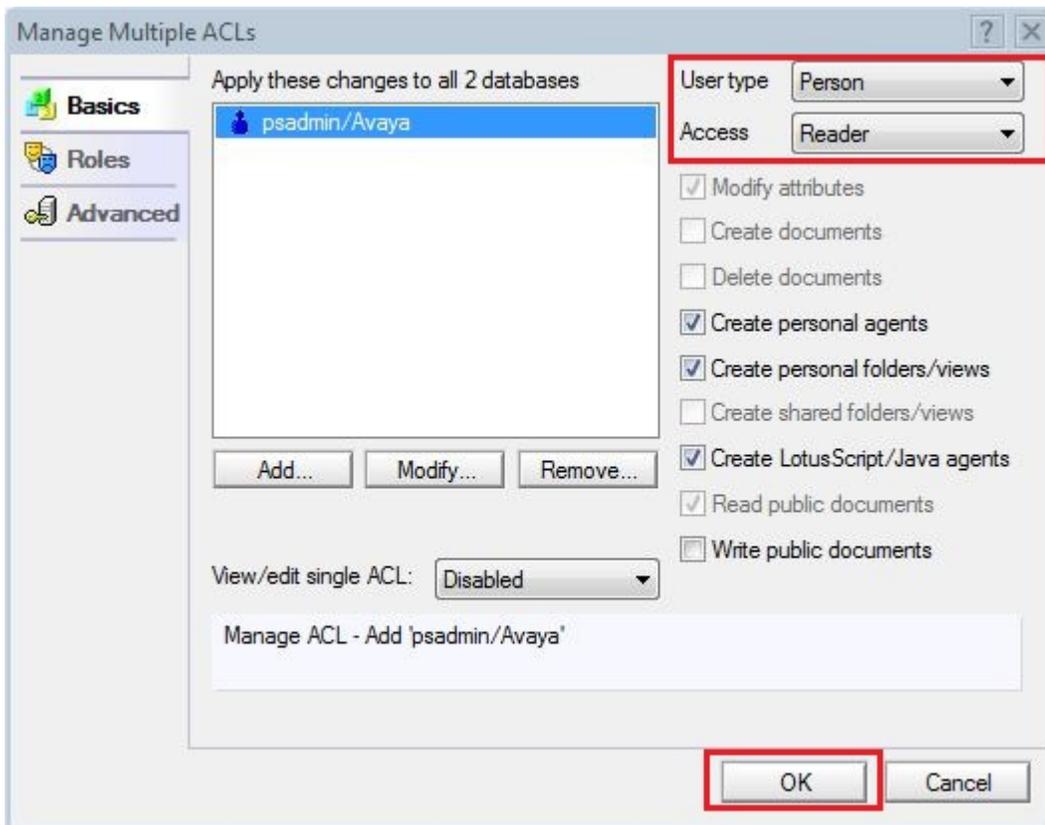
- Click **Add**.
- Click the person icon, and select the Domino user.
- Click **Add**.

8. Click **OK**.



9. In the **User type**, select **Person**.

- In the **Access** field, select **Reader**.



- Click **OK**.
- Click **OK**.

## Adding Lotus Notes handle to a System Manager user

### Procedure

- Log in to the System Manager web console as an administrator.
- Click **User Management > Manage Users**.
- Select the user, and click **Edit**.  
The system displays the User Profile Edit page.
- Click the **Communication Profile** tab.
- In the **Communication Address** section, click **New**.
- In the **Type** drop-down box, select **Lotus Notes**.
- In the **Fully Qualified Address** field, type the Internet address of the Domino user.

For example, if the Internet address of the user is ps5603@ca.avaya.com, in the **Handle** field, type ps5603 and in the **Domain** field, type ca.avaya.com.

8. Click **Add**.

## **Domino Collector configuration**

You can configure Domino Collector in one of the following ways:

- During Presence Services graphical installation
- During Presence Services silent installation
- After Presence Services installation

## **Configuring Domino Collector during the Presence Services graphical installation**

### **About this task**

You must perform this procedure during the Presence Services installation.

## Procedure

1. On the Presence Components screen, select the **Domino Collector Component** check box, and click **Next**.



2. On the Domino Component Configuration screen, type the values for the configuration parameters.

Installation of PS - PS-6.2.4.0-SNAPSHOT-design

**AVAYA**

## Domino Component Configuration

The following settings are used to configure the Domino Collector component.

Domino Server Web Service URI:

Calendar Polling Period (mins):

Calendar Requests Per Minute:

Out Of Office Polling Period (mins):

Out Of Office Requests Per Minute:

Publishing Period (mins):

Domino User Name:

Domino User Password:

Retype Password:

3. Click **Next** to continue with the installation.

For more information about the Presence Services installation, see *Deploying Avaya Aura® Presence Services*.

### Related Links

[Domino Collector Configuration field descriptions](#) on page 95

## Domino Collector Configuration field descriptions

Field	Description	Default value
<b>Domino Server Web Service URI</b>	Specifies the URI of the Domino server. For example, <code>http:// &lt; domino-server-fqdn &gt;</code> .  Domino Collector uses the URI to compose the web service URI. The web service URI is used to send the web service requests to the Domino server.	blank
<b>Calendar Polling Period (mins)</b>	Specifies how frequently Domino Collector polls the Domino server to get calendar information for users.	15
<b>Calendar Requests Per Minute</b>	Specifies how many Calendar Information requests are sent to the Domino server every minute.	10
<b>Out Of Office Polling Period (mins)</b>	Specifies how frequently Domino Collector polls the Domino server to get Out-of-Office information for users.	30
<b>Out Of Office Requests Per Minute</b>	Specifies how many Out-of-Office requests are sent to the Domino server every minute.	10
<b>Publishing Period (mins)</b>	Specifies how frequently Domino Collector sends the latest Domino presence tuple information to the XCP core for publishing.	5
<b>Domino User Name</b>	Specifies the user name of a Domino user who has the required permissions to read mail files for the requested users.	blank
<b>Domino User Password</b>	Specifies the password of the Domino user.	blank
<b>Retype Password</b>	Confirms the password of the Domino user.	blank

### Related Links

[Configuring Domino Collector during the Presence Services graphical installation](#) on page 92

## Configuring Domino Collector during the silent installation of Presence Services

### Procedure

1. Log in to the Presence Services server.

2. Navigate to the `/opt/Avaya` folder.
3. In the `autoInstall_PS.properties` file, specify the Domino Collector configuration parameters.

For example, see the following configuration:

```
# Name:      inclDomino
# System: Presence Components setting.# Use:      Domino Collector Component.
# Value: Set to "true" to enable, or "false" to disable.
inclDomino=false
# Name:      DOMINO_SERVER_URI
# System: Domino Component - Domino Server Web Service URI.
# Use:      Domino URI
# Value: A string value
# Note: Users must change this setting to something appropriate to their
environment
DOMINO_SERVER_URI=
# Name:      DOMINO_CALENDAR_POLLING_PERIOD
# System: Domino Component - Calendar Polling Period (mins).
# Use:      The periodic interval to retrieve calendar information.
# Value: A numeric value
DOMINO_CALENDAR_POLLING_PERIOD=15
# Name:      DOMINO_CALENDAR_REQUEST_RATE
# System: Domino Component - Calendar Request Rate Per Minute.
# Use:      Specifies how many Calendar Information requests are sent to the Domino
Server per minute.
# Value: A numeric value
DOMINO_CALENDAR_REQUEST_RATE=10
# Name:      DOMINO_OOTO_POLLING_PERIOD
# System: Domino Component - Out Of Office Polling Period (mins).
# Use:      The periodic interval to retrieve Out Of Office information.
# Value: A numeric value
DOMINO_OOTO_POLLING_PERIOD=30
# Name:      DOMINO_OOTO_REQUEST_RATE
# System: Domino Component - Out Of Office Request Rate Per Minute.
# Use:      Specifies how many Out Of Office Information requests are sent to the
Domino Server per minute.
# Value: A numeric value
DOMINO_OOTO_REQUEST_RATE=10
# Name:      DOMINO_PUBLISHING_PERIOD
# System: Domino Component - Publishing Period (mins).
# Use:      Specifies how often to send the latest Domino presence tuple information
internally to the XCP core for publishing.
# Value: A numeric value
DOMINO_PUBLISHING_PERIOD=5
# Name:      DOMINO_USERNAME
# System: Domino Component - Domino User Name.
# Use:      Specifies the Domino user to authenticate with, when polling for
Calendar/Out of the Office information from the Domino Server.
# Value: A string value
DOMINO_USERNAME=
# Name:      DOMINO_USER_PASSWORD
# System: Domino Component - Domino User Password.
# Use:      The password for the above Domino user.
# Value: A Alphanumeric value
DOMINO_USER_PASSWORD=
```

For more information about silent installation, see *Deploying Avaya Aura® Presence Services*.

### Related Links

[Domino Collector configuration parameters](#) on page 97

## Domino Collector configuration parameters

Name	Description	Default value
<b>inclDomino</b>	Specifies whether to install Domino Collector or not.  To allow the installation of Domino Collector, set this field to <code>true</code> . To prevent the installation of Domino Collector, set this field to <code>false</code> .	<code>false</code>
<b>DOMINO_SERVER_URI</b>	Specifies the URI of the Domino server. For example, <code>http:// &lt; domino-server-fqdn &gt;</code> .  Domino Collector uses the URI to compose the web service URI. The web service URI is used to send the web service requests to the Domino server.	blank
<b>DOMINO_CALENDAR_POLLING_PERIOD</b>	Specifies how frequently Domino Collector polls the Domino server to get calendar information for users.	15 minutes
<b>DOMINO_CALENDAR_REQUEST_RATE</b>	Specifies how many Calendar Information requests are sent to the Domino server every minute.	10
<b>DOMINO_OOTO_POLLING_PERIOD</b>	Specifies how frequently Domino Collector polls the Domino server to get Out-of-Office information for users.	30 minutes
<b>DOMINO_OOTO_REQUEST_RATE</b>	Specifies how many Out-of-Office requests are sent to the Domino server every minute.	10
<b>DOMINO_PUBLISHING_PERIOD</b>	Specifies how frequently Domino Collector sends the latest Domino presence tuple information to the XCP core for publishing.	5 minutes
<b>DOMINO_USERNAME</b>	Specifies the user name of a Domino user who has the required permissions to read mail files for the requested users.	blank
<b>DOMINO_USER_PASSWORD</b>	Specifies the password of the Domino user.	blank

### Related Links

[Configuring Domino Collector during the silent installation of Presence Services](#) on page 95

## Configuring Domino Collector after installing Presence Services

### Procedure

1. Log on to the Presence Services XCP Controller web console.
2. In the **Components** section, in the **Add a new** field, select **Domino Collector**.
3. Click **Go**.

The system displays the Domino Collector Configuration page. By default, the system displays the basic configuration view, which shows some of the configuration parameters. The system uses the default values for the parameters that are not listed in the basic configuration view. The advanced configuration view shows all the Domino Collector configuration parameters.

4. Click **Submit** to save the changes.
5. Click **Home** to go to the Presence Services XCP Controller page and to check if the system displays the new entry in the **Components** section.

 **Note:**

You cannot add multiple Domino Collectors to the same Presence Services system.

---

## IM Transcript Web service

### IM Transcripts Web Service configuration

Presence Services adds an extra layer of security for IM Transcript Web Service. You must modify the web.xml file for axis to ensure that SSL is used.

IM Transcript Web Service also ensures a basic authentication mechanism. The users in the following groups are authorized to use the IM Transcript Web Service:

- im-transcript-users
- ips box in the im-transcript-users group

For example, to allow a cust user to gain access to IM Transcript Web Service, use the `usermod -a -G im-transcript-users cust` command.

### IM Transcripts Web Service configuration reference

To meet regulatory requirements, Presence Services must be able to retrieve the transcripts of IM conversations. The IM Transcripts Web Service is an XCP component that is used to read the contents of the database. The server receives messages, and these messages are logged in the system database. According to regulatory requirements, Presence Services must be able to retrieve the transcripts of IM conversations. The IM Transcripts Web Service XCP component can read the contents of the database but cannot modify them.

### Related Links

[IM Transcripts Web Service Configuration basic parameters](#) on page 99

[IM Transcripts Web Service Configuration intermediate parameters](#) on page 99

[IM Transcripts Web Service Configuration advanced parameters](#) on page 100

## IM Transcripts Web Service Configuration basic parameters

### *Description*

The description is displayed in the Components area on the controller's main page.

#### **Note:**

Avaya does not recommend that you have more than one IM Transcripts Web Service component at active at once.

## IM Transcripts Web Service Configuration intermediate parameters

### *Router outbound connection information*

Enables the Presence Services router to connect to the component. For example, if the component is running outside your firewall, using this option, the router can connect to the component safely rather than introducing security risks by letting the component connect to it. By default, components connect to the router using the routers Master Accept Port.

### *Component IP*

The IP address or host name of the system on which the component is installed.

### *Port*

The port that the component uses for communications.

### *Password*

The password that the router uses to authenticate the component.

### *Execute an external command*

Using this option, the router can start the component automatically. If you prefer to start the component from a command line, disable this option.

### *Command line to run*

A default command runs the component automatically. You can modify it, if needed.

#### **Note:**

Do not use the `-B` argument with this component. Since the IPS logger is already a daemon process, its children must not be daemons.

Do not redirect output, because all output to STDOUT and STDERR are redirected to `/dev/null`.

### *Hostnames for this component*

This option specifies the hosts for which this component handles packets. Specify a host filter only if you want the component to be externally addressable. For example, if you want clients and other components or programs to communicate with it. This is because the `mod_disco` module in JSM uses host filters to return the component as something that is discoverable.

### **Host Filters**

The host names or IP addresses for which you want this component to handle packets. Separate each host name or address with a line break.

Host filters must be host names, or IPv4 or IPv6 addresses. If you use an IP address, the packet address must also use this IP address.

## **IM Transcripts Web Service Configuration advanced parameters**

### **Runlevel**

The order in which this component shuts down. The runlevel must be an integer value greater than or equal to 0. Component shutdown is executed in reverse order of the specified runlevel; components with the highest level (typically 80) shut down first.

#### **\* Note:**

Do not change the runlevel unless you know exactly what you are doing and understand the effects that changing it will have. The default runlevel is provided to help the system shut down as smoothly as possible, and is based on this component's dependencies upon other components.

### **Timeout for shutdown**

The number of seconds that the server waits to receive acknowledgement from the component that the shutdown process has completed. If the component has not shut down by the time this time period has elapsed, the router leaves the process in its current state and continues shutting down other processes.

### **Number of packets buffered when component is down**

The number of packets bound for the component that must be buffered if the component goes down.

### **Bounce error packets to stderr**

Enables the router to send warnings to stderr when the component is down.

### **Buffer size in bytes for outgoing data**

The number of bytes the router must buffer when it sends information to the component. You may want to modify this element when working on performance enhancements.

### **Buffer size in bytes for incoming data**

The number of bytes the router must buffer when it receives information from the component. You may want to modify this element when working on performance enhancements.

## **IM Transcripts Component Configuration**

### **Start command**

The command used to start the Web service container. This may contain command line arguments.

### **Stop command**

The command used to stop the Web service container, this may contain command line arguments.

**Database Driver**

JDBC driver the Web service use

**Database URL**

The URL used to connect to the database where the IM transcripts are stored.

**Database User Name**

The user name for the database where the IM transcripts are stored.

**Database Password**

The password associated with the Database user name.

## Connection Manager configuration

Using Connection Manager, IM clients and external servers can connect to the XCP server. You can configure multiple instances of the Connection Manager to increase the number of connections your server can handle, configure multiple instances of Connection Manager. This also facilitates communication over different protocols. At the time of server installation, Connection Manager is already configured to handle XMPP connections from IM clients. You can configure additional Connection Manager for other purposes. For example, to handle SMTP connections to redirect offline messages to an e-mail server. You can install multiple Connection Managers on your primary XCP server. You can also install them on remote servers as described in Deploying Remote Connection Managers.

Avaya strongly recommends that you configure a separate Connection Manager to handle each different communication task rather than configuring one Connection Manager to do everything. The reasons for this include:

- **Scalability.** Each Connection Manager has a maximum number of connections that it can handle. For example, the client Connection Manager can handle only 10,000 concurrent client connections. Your system can handle more client connections if you add additional client Connection Managers.

 **Note:**

More than 10,000 connections can cause operational difficulties and may result in hindered performance.

- **Different communication protocols.** Avaya recommends that you configure a separate Connection Manager to handle each communication protocol that you plan to use. For example, if you want to configure an SMTP Connection Manager to handle offline messages, add a Connection Manager strictly for this purpose rather than adding another JSM command processor to the default client Connection Manager.
- **Redundancy.** Configuring separate Connection Managers also helps to ensure that you experience as few communication problems as possible. If the system on which one Connection Manager is installed fails, other systems can pick up the slack.

**Related Links**

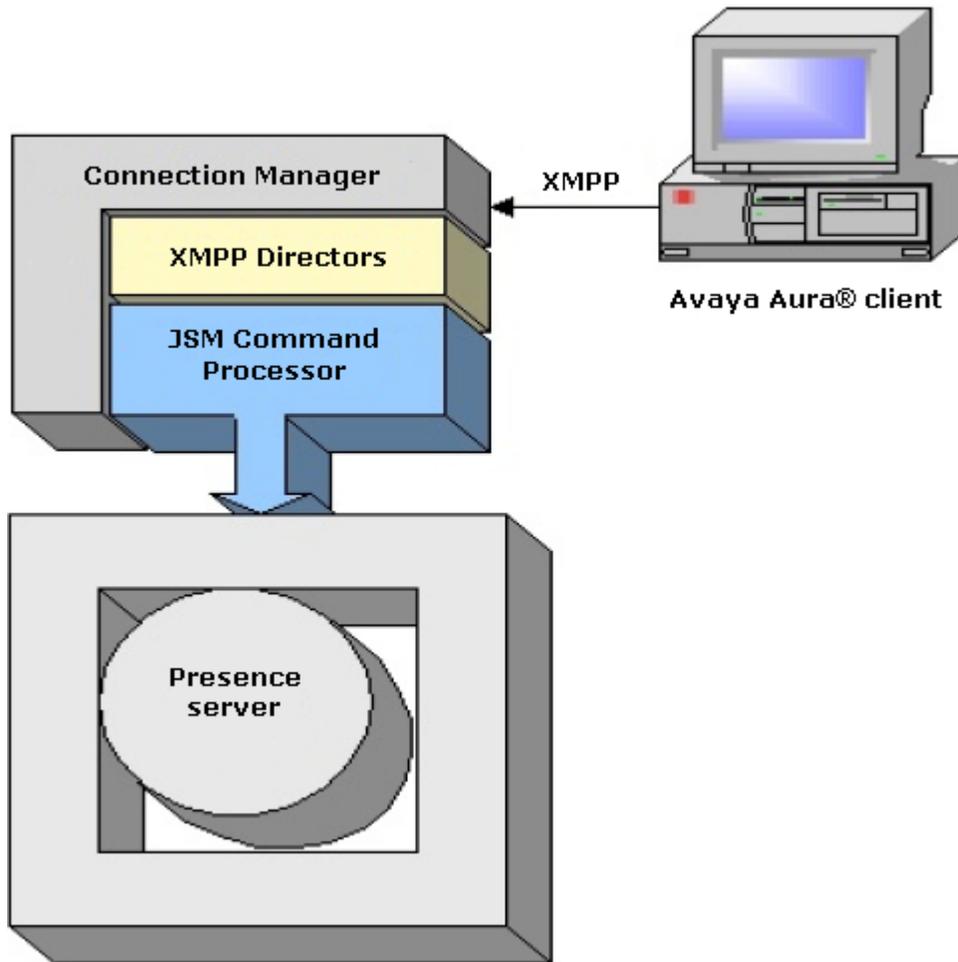
[Connection Manager](#) on page 102

[Configuring the basic Connection Manager](#) on page 102

[Simple Authentication and Security Layer \(SASL\)](#) on page 104

## Connection Manager

At the time of the Presence server installation, Connection Manager is configured by default. The following figure depicts the default Connection Manager running a JSM command processor to connect the Presence server to IM clients.



### Related Links

[Connection Manager configuration](#) on page 101

## Configuring the basic Connection Manager

The following instructions describe how to configure the Connection Manager (CM) using the parameters provided in the Basic configuration view of the controller. These parameters are sufficient to configure an operational CM. For descriptions of all of the CM parameters, see Connection Manager Parameter Reference. The command processors that you can configure within the Connection Manager are described in separate chapters.

## Procedure

1. Change to the controller's Basic configuration view
2. To add a Connection Manager, click **Go** in the Components area on the main page of the controller.

**XCP Controller - presence**  
[Home](#) [\[Logoff\]](#) Configuration view: **Basic**

**System**  
[\[Summary\]](#) [\[Cluster\]](#) [\[Stop the System\]](#) [\[Online Help\]](#)

**Router**  
 Add a new

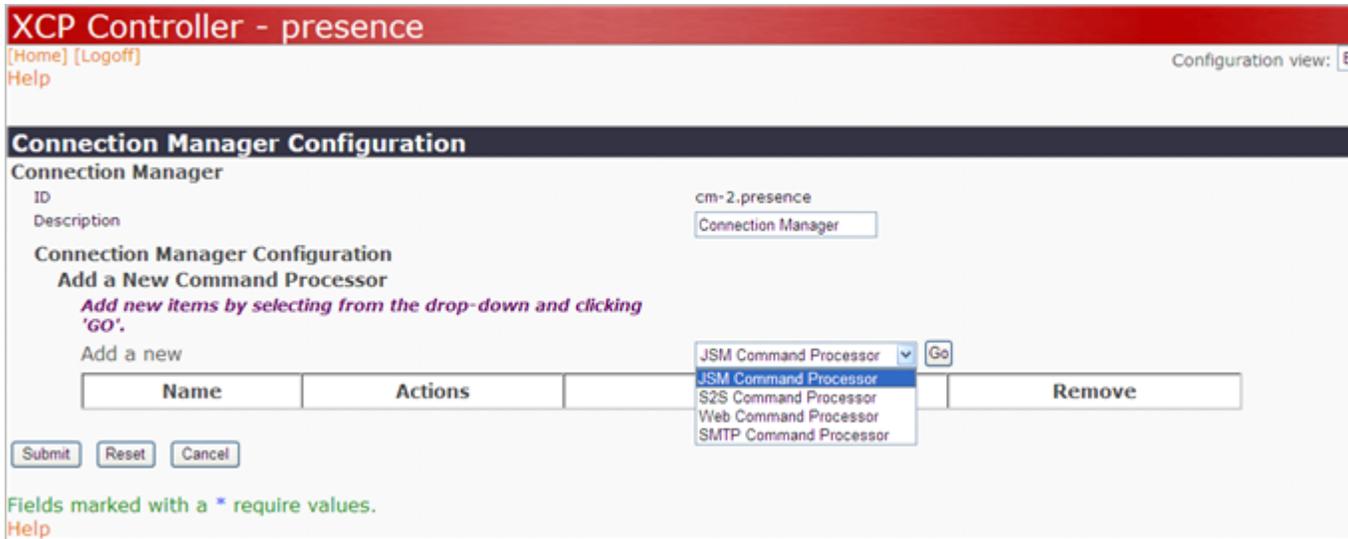
Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	<a href="#">Edit</a>	7400	N/A
Running	logger-1.presence	Logger Plugin	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	jsm-1.presence	Presence Session Manager	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	logger-2.presence	Statistics Logger	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	logger-3.presence	PS Core Logger	<a href="#">Edit</a>		<a href="#">Remove</a>

**Components**  
 Add a new

3. In the Connection Manager Configuration page, change the Description so that it describes this particular CM.
4. Under **Add a New Command Processor**, select a command processor in the list, and then click **Go**.

The command processors are described as follows:

- JSM Command Processor: Connects the XCP server to IM clients.
- S2S Command Processor: Enables XCP servers to communicate with each other server-to-server (S2S) across domains.
- Web Command Processor: Handles HTTP requests, and translates and transfers data between IM clients and the XCP router over the Web.
- SMTP Command Processor: Redirects offline messages to an e-mail server. Offline messages are IM messages that are sent to a client while the client is offline.



- When you finish configuring the command processor and return to the Connection Manager Configuration screen, click **Submit** to save your configuration.

#### Related Links

[Connection Manager configuration](#) on page 101

## Simple Authentication and Security Layer (SASL)

Presence Services uses the Simple Authentication and Security Layer (SASL) framework for the data security and user authentication. SASL uses a number of mechanisms for the authentication process, such as EXTERNAL, ANONYMOUS, and DIGEST-MD5. Presence Services use the DIGEST-MD5 mechanism to authenticate XMPP clients. In the DIGEST-MD5 mechanism, the system accepts MD5 hash instead of a user name and password to authenticate the clients. MD5 hash is a hexadecimal number.

Key features of DIGEST-MD5 authentication are:

- Presence server supports only DIGEST-MD5 mechanism for the SASL authentication.
- A cluster deployment does not support a heterogeneous configuration. In a heterogeneous configuration, you can set the SASL feature on more than one Presence Services nodes.
- SASL authentication is limited only to an XMPP interface. A SIP interface shares a trusted secure link with Session Manager.

#### **!** Important:

All endpoints must support the SASL feature. For an endpoint to be functional, the endpoint must support the SASL feature.

#### Related Links

[Connection Manager configuration](#) on page 101

[Configuring DIGEST-MD5 authentication using SASL](#) on page 105

## Configuring DIGEST-MD5 authentication using SASL

### About this task

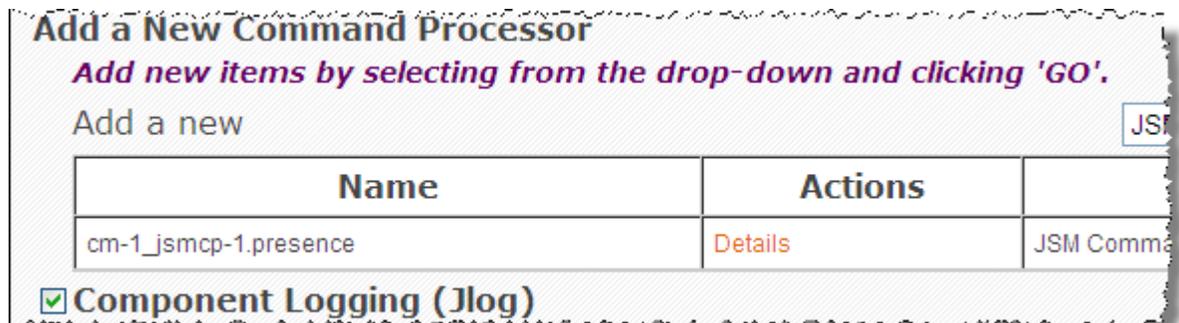
If you enable the DIGEST-MD5 authentication using SASL, you do not need to provide the user name and password at the time of authentication.

### Procedure

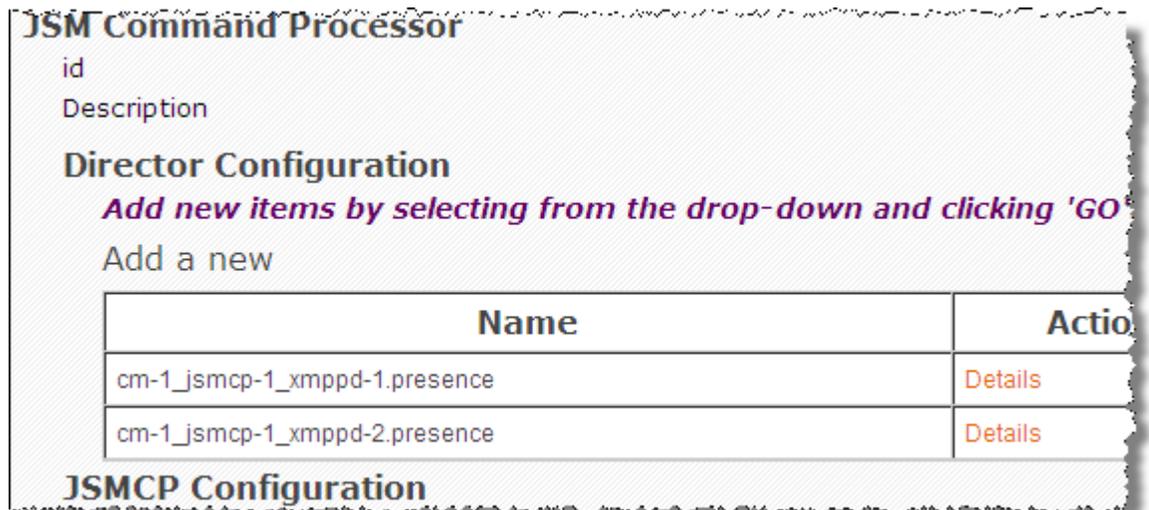
1. Log in to the Presence Services XCP Controller web interface.
2. On the Presence Services home page, select the **Advanced** configuration view.
3. In the **Components** area, select the connection manager component, and click **Edit**.

The system displays the Connection Manager Configuration page.

4. In the **Add a New Command Processor** section, click **Details** next to the command processor.



5. In the **JSM Command Processor** section, click **Details**.



The system displays the XMPP Director Configuration page.

6. In the **XMPP Director** section, perform the following steps:
  - a. Select the **SASL Settings** check box.

- b. In the **SASL Realm** field, type the name of the SASL realm.

For example, `ps.avaya.com`.



7. Click **Submit** to save the changes.
8. Repeat Step 5 to Step 7 for all XMPP Directors.
9. On the JSM Command Processor Configuration page, click **Submit**.
10. On the Connection Manager Configuration page, click **Submit**.
11. To restart the Presence Services server, perform the following steps:
  - a. Click **Stop the System**.
  - b. Click **Start the System**.

**\* Note:**

In a cluster deployment, repeat these steps for each Presence Services node.

### Related Links

[Simple Authentication and Security Layer \(SASL\)](#) on page 104

---

## Connection Manager parameter reference

### Related Links

[Connection Manager basic parameters](#) on page 106

[Connection Manager intermediate parameters](#) on page 107

[Connection Manager advanced parameters](#) on page 108

## Connection Manager basic parameters

### Description

The description is displayed in the Components area on the controller's main page and should help you distinguish between components of the same type when you have more than one configured. You can change the description as needed.

## Add a New Command Processor

Select a command processor in the list and click Go to gain access to its configuration page.

JSM Command Processor. Connects the XCP server to IM clients. S2S Command Processor. Enables XCP servers to communicate with each other across domains. S2S stands for Server-to-Server.

Web Command Processor. Handles HTTP requests, and translates and transfers data between IM clients and the XCP router over the Web.

SMTP Command Processor. Redirects offline messages to an email server. Offline messages are IM messages that are sent to a client while the client is offline.

## Connection Manager intermediate parameters

### Router outbound connection information

Enables the Presence Services router to connect to the component. For example, if the component is running outside your firewall, using this option, the router can connect to the component safely rather than introducing security risks by letting the component connect to it. By default, components connect to the router using the routers Master Accept Port.

### Component IP

The IP address or host name of the system on which the component is installed.

### Port

The port that the component uses for communications.

### Password

The password that the router uses to authenticate the component.

### Execute an external command

Using this option, the router can start the component automatically. If you prefer to start the component from a command line, disable this option.

### Command line to run

A default command runs the component automatically. You can modify it, if needed.

#### Note:

Do not use the `-B` argument with this component. Since the IPS logger is already a daemon process, its children must not be daemons.

Do not redirect output, because all output to STDOUT and STDERR are redirected to `/dev/null`.

### Hostnames for this component

This option specifies the hosts for which this component handles packets. Specify a host filter only if you want the component to be externally addressable. For example, if you want clients and other components or programs to communicate with it. This is because the `mod_disco` module in JSM uses host filters to return the component as something that is discoverable.

## Host Filters

The host names or IP addresses for which you want this component to handle packets. Separate each host name or address with a line break.

Host filters must be host names, or IPv4 or IPv6 addresses. If you use an IP address, the packet address must also use this IP address.

## Maximum number of sockets

The maximum number of sockets for this CM across all client and SMTP connections. For example, if you have 10,000 clients who can connect to the server, enter 10,000 for the number of sockets. We recommend a maximum of 10,000 clients per CM.

This number does not include the sockets used by the processors to connect to the core router.

## Component Logging (Jlog)

Enables to configure filtered level loggers that log messages to syslog and to a stream (stderr or stdout). You can enable either or both the syslog and stream loggers. These parameters are displayed in the controller's Intermediate and Advanced configuration views.

## SNMP Configuration

Select this option if you want to configure SNMP for the component.

### Enable SNMP

Leave this parameter set to Yes.

## Connection Manager advanced parameters

### Runlevel

The order in which this component shuts down. The runlevel must be an integer value greater than or equal to 0. Component shutdown is executed in reverse order of the specified runlevel; components with the highest level (typically 80) shut down first.

#### Note:

Do not change the runlevel unless you know exactly what you are doing and understand the effects that changing it will have. The default runlevel is provided to help the system shut down as smoothly as possible, and is based on this component's dependencies upon other components.

### Timeout for shutdown

The number of seconds that the server waits to receive acknowledgement from the component that the shutdown process has completed. If the component has not shut down by the time this time period has elapsed, the router leaves the process in its current state and continues shutting down other processes.

### Number of packets buffered when component is down

The number of packets bound for the component that must be buffered if the component goes down.

**Bounce error packets to stderr**

Enables the router to send warnings to stderr when the component is down.

**Buffer size in bytes for outgoing data**

The number of bytes the router must buffer when it sends information to the component. You may want to modify this element when working on performance enhancements.

**Buffer size in bytes for incoming data**

The number of bytes the router must buffer when it receives information from the component. You may want to modify this element when working on performance enhancements.

**Send keepalives**

Enables the router to send keep-alives to the component. The keep-alive helps prevent firewalls from dropping an unused connection to the component. If this option is set to `No`, keep-alives are disabled.

**Log the delivery of packets to this component**

Enables to log the data that the router delivers to the component. The information is logged to the loggers you set up during Presence Services Logger configuration (syslog, file, or stderr). Socket-level logging happens only at the debug level.

**Maximum interval in seconds to wait before restarting component**

The maximum number of seconds after which the router tries to restart the component. If the component goes down, the router tries to restart it after 1 second. If the component does not start, the router multiplies the wait time by 1.5, and tries again. Once the maximum time interval that you specify for this parameter is reached, the router continues to retry after waiting this amount of time.

**Maximum number of times to restart component**

The total number of restarts allowed. The default setting, `-1`, means unlimited.

**Interval in seconds at which to reset this value to 1 second**

The number of seconds that the component has been up and running, after which to set the restart time back to 1 second.

**Path to binary**

The directory path to the shell that launches the component. You can change the default setting if needed.

**Maximum size of threadpool**

The number of concurrent threads of execution to use to process client and SMTP connections. The default setting of 3 should be sufficient for most environments. However, if you have numbers of users approaching 10,000, you might want to change this value to 4 or 5.

This number does not include the threads used to talk to the XCP core router.

## User to run the CM as

If you want to listen on a port lower than 1024, you must be logged in as root user. For example, to listen on port 80, open the port as a root user. However, to listen to traffic more securely than as root, change your user ID to a nonroot ID immediately thereafter. Using this parameter, you can specify the user ID to which you want the CM to switch from root user as soon as the Connection Manager starts listening.

To listen on more than one port at the same time, such as 80 and 443, you must set up two Connection Managers, one to listen on each port.

## Add a new custom logger

If you create a custom logger for logging component information using the libjcore library, click **Go** to access the Custom Logger Configuration page.

## Count errors

Enables SNMP error counting.

### **Note:**

This option takes a great deal of server resource. Therefore, use it with caution.

---

## Connection configuration for an IM client

The JSM Connection Manager establishes connections with IM clients. The JSM Connection Manager contains a JSM Command Processor (JSMCP), which can be configured with one of three different directors - XMPP, HTTP binding, or polling - depending on the type of client being used and the type of connection you want to use to connect to it. Each director receives data over a socket from a client, converts the protocol into a form that the JSM Command Processor can understand, and sends it to the JSMCP. The JSMCP then sends the data to the XCP router, which sends it on to its final destination.

### **Warning:**

You must add a Connection Manager for an IM client in the supervision of an Avaya Support personnel.

## Related Links

[XMPP connection configuration](#) on page 110

[Configuring XMPP director](#) on page 111

[XMPP director and HTTP Binding Director parameter descriptions](#) on page 111

## XMPP connection configuration

The Connection Manager runs by default when you install the XCP server. It is configured with a JSM Command Processor and two XMPP directors. The XMPP directors handle communication with IM clients. One of the directors is configured to use port 5222 and the other is configured to use port 5223 for secure communications.

**Related Links**

[Connection configuration for an IM client](#) on page 110

**Configuring XMPP director****Procedure**

1. On the JSM Command Processor Configuration page, under **Director Configuration**, click **Details** beside one of the existing directors if you want to change its configuration.

The first director listed is configured to listen on port 5222, and the second director listens on port 5223.

2. On the XMPP Director Configuration page, change the default settings only if needed.
3. Click **Submit** in each configuration page until you return to the main page of the controller .

**Related Links**

[Connection configuration for an IM client](#) on page 110

**XMPP director and HTTP Binding Director parameter descriptions****IP address of external channel**

The IP address of the external channel on which this director listens for connections from IM clients. By default, the IP address is set to that of the server on which this Connection Manager is running.

**Port**

The port that the component uses for communications.

**Timeout for response**

The maximum number of seconds that the HTTP binding director waits to respond to a request from the client.

**Timeout for client inactivity**

The maximum number of seconds that a client can be inactive before the HTTP connection shuts down.

**Shortest allowable polling interval**

The shortest allowable polling interval (in seconds) after which the client may send a polling request. If polling requests are sent in shorter time intervals, the HTTP connection shuts down.

**Maximum simultaneous requests from client**

The number of simultaneous requests that the client can make with the requests attribute. The recommended value is 2, which is the default setting. If a client makes more simultaneous requests than the number specified here, the HTTP connection shuts down.

## HTTP binding director configuration

The HTTP Binding Director is used for configuring connections to the Presence Messenger for the Web client. The HTTP binding feature complies with XEP-0124: HTTP Binding. The following figure illustrates the HTTP binding connection configuration.

HTTP binding connections wrap XMPP traffic in HTML, enabling XEP-0124-compliant, Web-based clients to gain access to the XCP server without requiring any changes to network or firewall settings.

The process for configuring an HTTP binding connection involves adding a new Connection Manager to your XCP server, configured with a JSM Command Processor with an HTTP Binding Director, and a Web Command Processor with an HTTP Director and an HTTP Binding Handler.

### Related Links

[Configuring the HTTP binding director](#) on page 112

[Web Command Processor](#) on page 112

[Configuring a Web Command Processor](#) on page 113

## Configuring the HTTP binding director

### About this task

The HTTP Binding Director interprets HTTP-wrapped XMPP packets, strips off the HTTP wrapper, and forwards the packets to the JSM.

### Procedure

1. Using the Basic configuration view of the controller, add a new Connection Manager and configure it with a JSM Command Processor.
2. In the JSM Command Processor Configuration page under Director Configuration, click **Remove** beside the two existing XMPP directors to delete them.
3. Select HTTP Binding Director in the list, and then click **Go**.
4. In the HTTP Binding Director Configuration page, accept the default settings or change them as needed.
5. To save your configuration, click **Submit**. The system displays the JSM Command Processor Configuration page.
6. To save the JSM Command Processor configuration, click **Submit** again. You are returned to the Connection Manager Configuration page.

### Related Links

[HTTP binding director configuration](#) on page 112

## Web Command Processor

After you configure the JSM Command Processor with the HTTP Binding Director, configure a Web Command Processor in the same Connection Manager. The Web Command Processor can be

configured with an HTTP director and an HTTP binding handler, which work in conjunction with the JSM Command Processors HTTP Binding Director. The HTTP binding handler intercepts XEP-124-compliant packets and forwards them to the HTTP Binding Director.

### Related Links

[HTTP binding director configuration](#) on page 112

## Configuring a Web Command Processor

### Procedure

1. Change to the Advanced configuration view of the controller.
2. On the Connection Manager Configuration page under **Add a New Command Processor**, select **Web Command Processor** in the list, and then click **Go**.
3. On the Web Command Processor Configuration page under **Director Configuration**, click **Go** to add an HTTP director.
4. To configure the HTTP director, use the online help or accept the default settings.
5. Click **Submit** to save the director.
6. On the Web Command Processor Configuration page under **Handlers**, select **HTTP Binding Handler** in the list, and then click **Go**.
7. On the HTTP Binding Handler Configuration page, change the **Path**, if needed, or accept the default setting, `/httpbinding`. The Path is the HTTP URI path on which this handler listens for HTTP binding traffic. For example, in the URI, `http://www.example.com:7300/httpbinding`, the path is `/httpbinding`.
8. To save your configuration, click **Submit**.  
The system displays the Web Command Processor Configuration page.
9. In the Web Command Processor Configuration page, click **Submit**.  
The system displays the Configuration Manager Configuration page.
10. On the Connection Manager Configuration page, perform any additional configuration if needed. To save your configuration, click **Submit**.

#### **Note:**

No additional configuration is required. You can submit the Connection Manager using its remaining default settings.

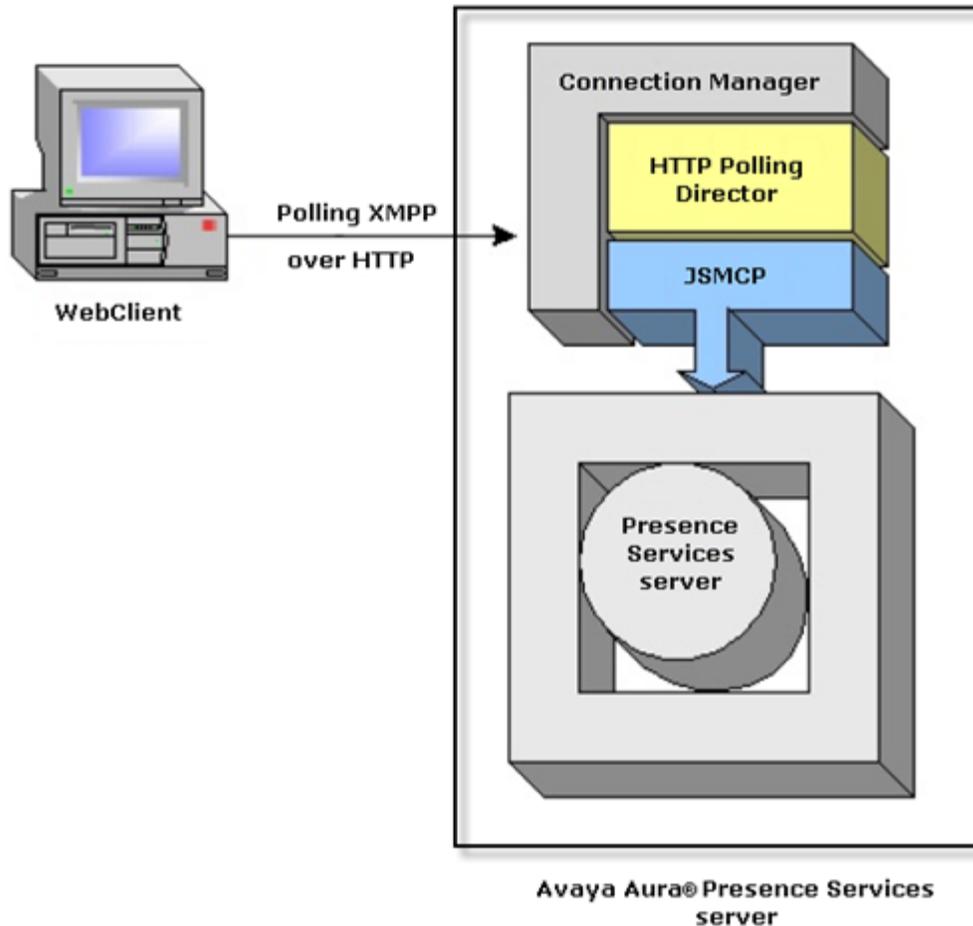
### Related Links

[HTTP binding director configuration](#) on page 112

## Polling Connection configuration

This section provides instructions for configuring the HTTP polling director in the JSM command processor. With HTTP polling connections, you can use HTTP clients, and IM users can access your XCP server without requiring any changes to network or firewall settings.

The following figure illustrates the Connection Manager that WebClient uses to connect to the XCP server using polling XMPP over HTTP. The polling director uses HTTP to communicate over firewalls using port 80.



### Related Links

- [HTTP polling connection configuration](#) on page 115
- [Configuring HTTP polling connection](#) on page 115
- [Server-to-Server connections](#) on page 116
- [S2S Connection Manager configuration](#) on page 117
- [Configuring an OpenPort Connection](#) on page 117
- [Configuring OpenPort](#) on page 118
- [Configuring the dialback password](#) on page 118

[Hosts and IP Addresses for blacklists and whitelists](#) on page 119

[Blacklisting and Whitelisting Hosts and IP Addresses](#) on page 119

[Packet handling for blacklisted hosts](#) on page 120

## HTTP polling connection configuration

Parameter	Description
IP address of external channel	IP address of external channel.
Port	Port number.  <b>Note:</b> Enter 8080. If you want to start the CM as root user, you must use port 80 or 443.
SSL Settings	Configures secure socket layer settings to enable this director to establish a secure connection with the server.  <b>Note:</b> The XCP server does not support private keys for SSL certificates that have pass phrases. If you have a pass phrase or encrypt your private key, your private key/ public certificate pair will not load into XCP.
Root directory for files served to WebClient	Root directory on the XCP server that contains the files served to WebClient.

### Related Links

[Polling Connection configuration](#) on page 114

## Configuring HTTP polling connection

This section provides instructions for configuring the HTTP polling director using the parameters provided in the Intermediate configuration view of the controller. These parameters are sufficient to configure an operational director.

### Procedure

1. Change to the Intermediate configuration view of the controller .
2. In the JSM Command Processor Configuration page, select **Polling Director > Go** .
3. Configure the parameters using the HTTP polling connection configuration field descriptions.
4. To save the polling directors configuration, click **Submit**.

The system displays the JSM Command Processor Configuration page.

5. Click **Submit** on the JSM Command Processor Configuration page.

The system displays the Connection Manager Configuration page.

6. In the Connection Manager Configuration page, perform any additional configuration if you want, then click **Submit** to save your configuration.

**\* Note:**

No additional configuration is required. You can submit the CM using its remaining default settings.

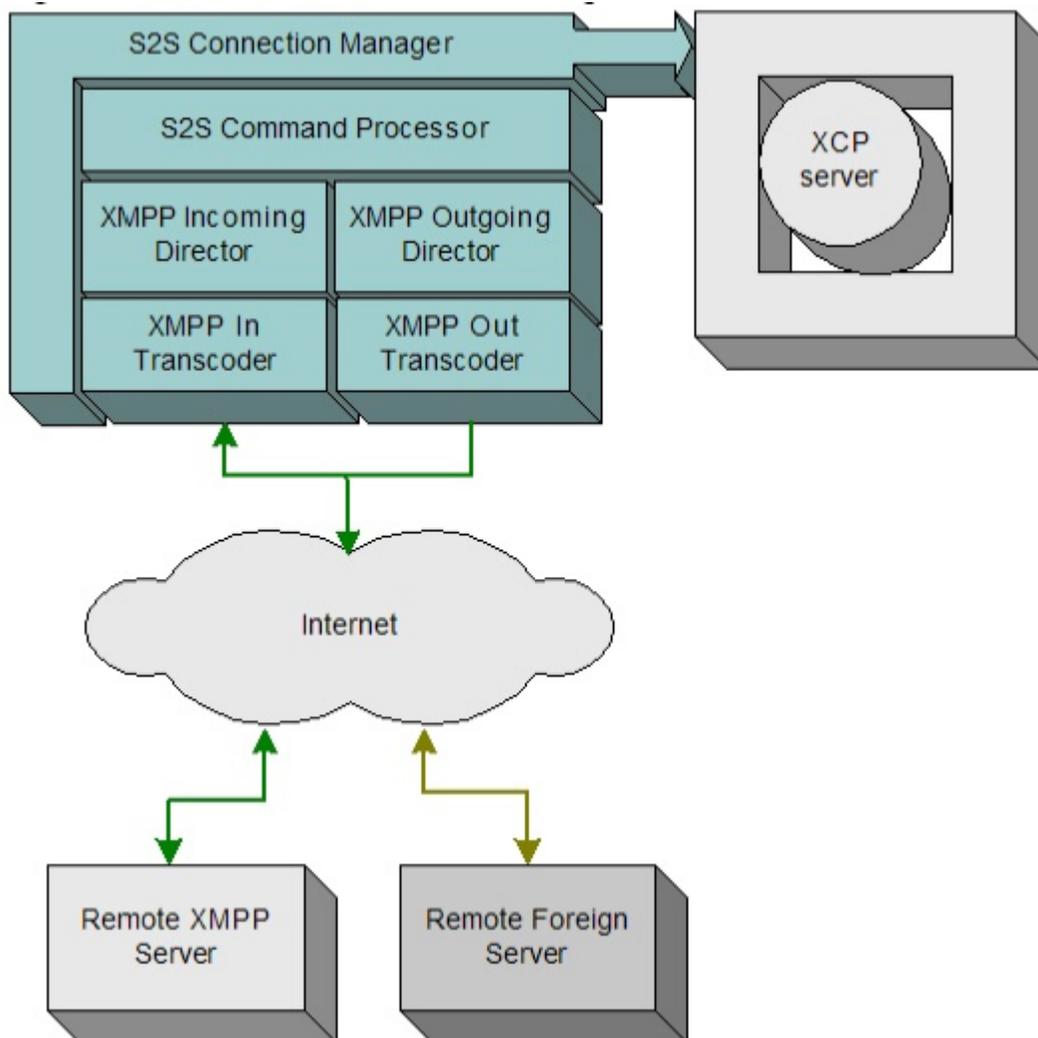
**Related Links**

[Polling Connection configuration](#) on page 114

**Server-to-Server connections**

Using the Server-to-Server connection manager (S2S CM), XCP servers can communicate with remote servers across domains. It also supports the dialback protocol, which determines whether or not to trust a connection from another server.

The following figure illustrates the S2S CM configuration.



**Related Links**

[Polling Connection configuration](#) on page 114

## S2S Connection Manager configuration

The S2S CM is configured with an S2S command processor, which contains an XMPP incoming director and an XMPP outgoing director for XMPP server-to-server communications. Using these directors, you can blacklist and whitelist specific hosts that are inside or outside of your XCP system. The incoming director handles incoming packets that are being sent to the XCP router from remote servers; the outgoing director handles packets that are being sent from the router to remote servers.

Avaya recommends that you configure a new separate server-to-server connection manager in order to maximize the efficiency with which the XCP server can handle S2S communication.

The default rules are configured as follows, where **n** is the number of the CM.

Director ID	DNS SRV lookup	Port
cm-n_s2scp-1_xmppoutd-1	_xmpp-server._tcp	
cm-n_s2scp-1_xmppoutd-1	_jabber._tcp	
cm-n_s2scp-1_xmppoutd-1		5269

Each time a new outbound connection is required, the S2SCP goes through the rules asking the specified director to attempt the outgoing connection. If a director successfully establishes a connection, then that director will always handle stanzas bound for that particular host. Otherwise, the S2SCP asks the next director (using the defined rules) to attempt an outbound connection for the host.

You only need to add a new rule if you want to change how the DNS lookups happen for outbound servers.

### Related Links

[Polling Connection configuration](#) on page 114

## Configuring an OpenPort Connection

### Procedure

1. Change to the Intermediate configuration view of the controller.
2. In the Components area on the main page of the controller, select **OpenPort** in the list, and click **Go**.
3. Enter the S2S Command Processors ID, without the realm , as the ID of the OpenPort. For example, cm-2\_s2scp-1.
4. The OpenPort must use the opposite connection type than that used by the S2S command processor. If you used the default connection type of connect for the S2S command processor, skip to step 5.

If you configured the S2S command processor with an accept connection type, you must select the **Router Outbound Connection Information** option for the **OpenPort**, and specify the same Component IP, Port, and Password that you used for the command processor.

5. Under **Hostnames** for this Component, enter a host filter to allow packets destined for external domains to reach the S2S command processor. In most cases, you should enter an asterisk (\*) in the **Host Filters** text box.
6. Click **Submit** to save your configuration.
7. Restart your XCP system.

#### Related Links

[Polling Connection configuration](#) on page 114

## Configuring OpenPort

You must configure an OpenPort connection to enable the AFT Handler to connect to the router, in addition to providing the information in the Advanced File Transfer Handler Configuration page.

#### Procedure

1. In the Components area on the controller's main page, select **OpenPort** from the list, and then click **Go**.
2. When you are prompted for an ID for the OpenPort, enter the ID of the AFT Handler without the realm. For example, `cm-2_webcp-1.aft`.
3. Click **OK** to display the OpenPort Configuration page.
4. Change the Description to AFT Open Port (or to something similar).

The OpenPort must use a connection type that is opposite the one used by the AFT Handler. If you use the default connection settings for both the AFT Handler and the OpenPort, you do not have to change the OpenPorts connection type.

If you configured the AFT Handler to use an **accept** connection type and therefore must change the OpenPorts connection type to **connect**, select the **Router Outbound Connection Information** option, and specify the same component IP, port, and password configured for the AFT handler.

5. In the **Hostnames for this Component** text box, enter the AFT handlers host name. For example, `aft.example.com`.
6. Click **Submit** to save your configuration.
7. Click **Submit** in the Web Command Processor and Connection Manager Configuration pages to return to the controller's main page.
8. Restart your XCP system.

#### Related Links

[Polling Connection configuration](#) on page 114

## Configuring the dialback password

### About this task

The S2S CM supports the dialback protocol, which determines whether or not to trust a connection from another server.

## Procedure

1. Change to the Intermediate configuration view of the controller.
2. In the **Dialback Secret** box, enter the password used to prove the authenticity of another server.

By default, the dialback secret is set to the XCP routers password. If you have multiple S2S command processors in your XCP system, they must all have the same dialback secret.

## Related Links

[Polling Connection configuration](#) on page 114

## Hosts and IP Addresses for blacklists and whitelists

If you want to blacklist and whitelist certain hosts and IP addresses from sending and receiving packets, you can configure one or more of the authorized outgoing and incoming, to and from addresses. Using these four configuration options displayed in the Intermediate configuration view of the controller, you can specify exactly which hosts and IP addresses may or may not send or receive incoming or outgoing packets.

Each authorization option has a Default behavior parameter, which controls the way your system handles packets for all hosts or IPs except for those listed under Host Filters and IP addresses. Specified hosts and IP addresses behaves in a manner opposite to the default behavior.

## Related Links

[Polling Connection configuration](#) on page 114

## Blacklisting and Whitelisting Hosts and IP Addresses

### Procedure

1. Change to the Intermediate configuration view of the controller.
2. Configure one or more of the following authorization options:

<b>Authorized Outgoing From Addresses</b>	Using Authorized Outgoing From Addresses, you can specify the hosts and IP addresses within your organization from which outgoing packets can be sent. If you set the default behavior to allow, all hosts and IPs except for those listed are allowed to send outgoing packets. If you set the default behavior to deny, only the listed hosts and IPs can send outgoing packets. Outgoing from addresses are usually paired with incoming to addresses.
<b>Authorized Outgoing To Addresses</b>	Using Authorized Outgoing To Addresses, you can specify the hosts and IP addresses to which users within your organization can send outgoing packets. If you set the default behavior to allow, users can send packets to all hosts and IPs except for those listed. If you set the default behavior to deny, users can send packets only to the hosts and IPs listed. Outgoing to addresses are usually paired with incoming from addresses.
<b>Authorized Incoming From Addresses</b>	Using Authorized Incoming From Addresses, you can specify the hosts and IP addresses from which incoming packets can be

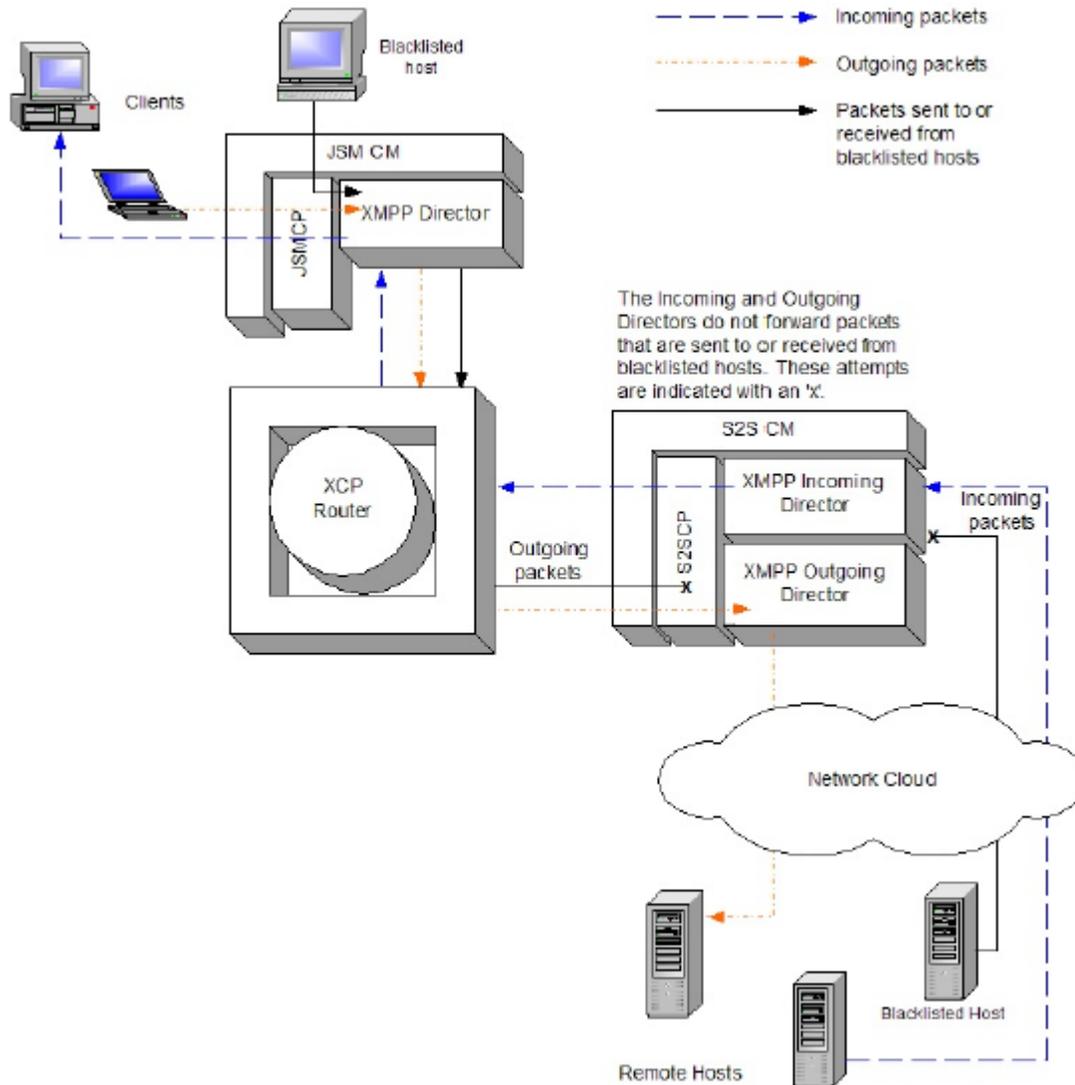
	received by users in your organization. If you set the default behavior to allow, users can receive packets from all hosts and IPs except for those listed. If you set the default behavior to deny, users can receive packets only from the hosts and IPs listed. Incoming from addresses are usually paired with outgoing to addresses.
<b>Authorized Incoming To Addresses</b>	Using Authorized Incoming To Addresses, you can specify which hosts and IP addresses within your organization can receive incoming packets. If you set the default behavior to allow, all hosts and IPs except for those listed can receive packets. If you set the default behavior to deny, only the listed hosts and IPs can receive packets. Incoming to addresses are usually paired with outgoing from addresses.

**Related Links**

[Polling Connection configuration](#) on page 114

**Packet handling for blacklisted hosts**

The following figure illustrates the handling of packets that are sent to or received from blacklisted hosts.



**Related Links**

[Polling Connection configuration](#) on page 114

## S2S Command Processor Parameter Reference

### S2S Command Processor basic parameters

**Description**

The description displays in the list of command processors on the Connection Manager Configuration page.

## Director Configuration

The directors are described as follows:

XMPP Incoming Server Director handles incoming packets that are being sent to the XCP router from remote servers.

XMPP Outgoing Server Director handles outgoing packets that are being sent from the XCP router to remote servers.

## Component IP

If you are using the default connection type of connect, shown in the Advanced configuration view, enter the IP address or the FQDN of the server where the Connection Manager is installed. The CMs IP address is provided by default.

If you change to an accept connection type, enter the IP address or the FQDN on which the XCP router listens for the command processor.

## Port

If you are using the default connection type of connect, shown in the Advanced configuration view, enter the port that this command processor uses for communication. By default, the port is set to the Master Accept Port that is specified during XCP server installation.

If you change to an accept connection type, enter the port on which the XCP router listens for the command processors connection. The router allows only a single connection over this port at a time. Therefore, multiple versions of the command processor cannot connect to the same port.

## Password

The password that the XCP server uses to authenticate the command processor.

## Outgoing Connection Attempt Rules

Outgoing Connection Attempt Rules Three rules are supplied by default. They specify the order and DNS lookup properties for each outbound director. By default, these three rules are configured with the ID of the XMPP Outgoing Server Director. However, if you add another director, you must edit the rules or add additional ones, and specify the ID of the director to which the rules apply.

## S2S Command Processor intermediate parameters

### Dialback Secret

The password used to prove the authenticity of another server. All S2S control processors for a single XCP system must have the same dialback secret.

The XCP server uses dialback to verify that a connection between two servers is trusted. One XCP server uses DNS to verify that a connecting XCP server is authorized to represent a given network. Dialback prevents the connecting server from spoofing a particular server name and sending false data. Although the dialback protocol resembles reverse DNS or IP lookups, it is more complex, since it must accommodate server farms and complex environments.

For example, when server A attempts to connect to server B, it sends an XML stream to see if server B supports the dialback protocol. Server B returns a stream indicating that it does. Server A

then sends a dialback key to server B. Server B now dials back and initiates a separate connection to server A using a DNS/host name lookup to connect to the correct server. Server B returns the dialback key over the second connection. If server A can confirm the key, the dialback is successful.

For a complete description of dialback, see the Internet Engineering Task Force (IETF) documentation of the protocol: <http://www.ietf.org/ids.by.wg/xmpp.html>.

## Authorized Outgoing From Addresses

Outgoing from addresses are hosts or IP addresses within your organization from which outgoing packets may be sent. Outgoing from addresses are normally paired with incoming to addresses.

### Default behavior

Default behavior of your system for handling outgoing from addresses: either allow or deny . The hosts and IP addresses listed below are exceptions to the default behavior. For example, if you set the default behavior to allow, the specified hosts and IPs are not allowed to send outgoing packets. If you set the default behavior to deny, the specified hosts and IPs are allowed to send outgoing packets.

### Host Filters

The host names for which you want to apply the opposite of the default behavior.

### IP Addresses

The IP addresses for which you want to apply the opposite of the default behavior.

## Authorized Outgoing To Addresses

Outgoing to addresses are hosts or IP addresses to which people or entities in your organization may send outgoing packets. Outgoing to addresses are normally paired with incoming from addresses.

### Default behavior

Default behavior of your system for handling outgoing from addresses: either allow or deny . The hosts and IP addresses listed below are exceptions to the default behavior. For example, if you set the default behavior to allow, the specified hosts and IPs are not allowed to send outgoing packets. If you set the default behavior to deny, the specified hosts and IPs are allowed to send outgoing packets.

### Host Filters

The host names for which you want to apply the opposite of the default behavior.

### IP Addresses

The IP addresses for which you want to apply the opposite of the default behavior.

## Authorized Incoming From Addresses

Incoming from addresses are hosts or IP addresses from which people or entities in your organization may receive incoming packets. Incoming from addresses are normally paired with outgoing to addresses.

## **Default behavior**

Default behavior of your system for handling outgoing from addresses: either allow or deny . The hosts and IP addresses listed below are exceptions to the default behavior. For example, if you set the default behavior to allow, the specified hosts and IPs are not allowed to send outgoing packets. If you set the default behavior to deny, the specified hosts and IPs are allowed to send outgoing packets.

## **Host Filters**

The host names for which you want to apply the opposite of the default behavior.

## **IP Addresses**

The IP addresses for which you want to apply the opposite of the default behavior.

## **Authorized Incoming To Addresses**

Incoming to addresses are hosts or IP addresses in your organization that cannot receive incoming packets. Incoming to addresses are usually paired with outgoing from addresses.

## **Default behavior**

Default behavior of your system for handling outgoing from addresses: either allow or deny . The hosts and IP addresses listed below are exceptions to the default behavior. For example, if you set the default behavior to allow, the specified hosts and IPs are not allowed to send outgoing packets. If you set the default behavior to deny, the specified hosts and IPs are allowed to send outgoing packets.

## **Host Filters**

The host names for which you want to apply the opposite of the default behavior.

## **IP Addresses**

The IP addresses for which you want to apply the opposite of the default behavior.

## **Number of outgoing connection attempts**

The number of times to try making an outbound connection.

## **Seconds to wait between connection attempts**

The number of seconds to wait between connection attempts.

## **IP Addresses to Prevent Loopback Connections**

The address of any S2S Command Processor that listens for incoming packets.

## **Administrators JIDs**

Enter the JIDs of those you want to enable to query the S2S Command Processor.

The S2SCP can be queried from a client that supports the Service Discovery protocol described in XEP-0030.

Queries must be sent to the S2SCPs ID.realm; for example, `cm-2_s2scp-1.denver`.

## Users who can discover/view s2s connections

The users who can query the S2S Command Processor for a list of connected hosts.

## S2S Command Processor advanced parameters

### Connection Type

With a connect connection type (the default setting), the router connects to the component.

With an accept connection type, the router opens a specific port and listens on that port for a connection from the component.

For the Open Port, you must configure a connection type that is opposite the type configured for the S2SCP. Therefore, if you use the accept connection type for the S2SCP, you must configure the Router Outbound Connection Information parameters for the Open Port.

### Timeout for failed outgoing cache (seconds)

The number of seconds after which the cache table is cleared. This table must be cleared periodically to prevent DOS attacks and to prevent a temporarily unresolvable host name from becoming permanently unresolvable. The default setting is 1800 seconds.

---

## Discovery protocol for querying the S2S Command Processor

The XMPP protocol examples, based on XEP-30, of how to discover the inbound and outbound S2S connections are as follows. For more information, see XEP-0030.

### Related Links

[S2SCP query for information](#) on page 125

[Outbound and inbound lists query](#) on page 126

[S2SCP query for all items](#) on page 126

## S2SCP query for information

### Example

The following XMPP query asks for information about the S2SCP whose ID is

```
cm-2_s2scp-1.jabber:
<iq id='disco-info-10' to='cm-2_s2scp-1.jabber' type='get'>
<query xmlns='http://jabber.org/protocol/disco#info' />
</iq>
```

The following response from the server identifies the S2SCP as a component of type s2s.

```
<iq xmlns='jabber:client'
from='cm-2_s2scp-1.jabber'
id='disco-info-10'
to='asmith@example.com/Example Messenger Desktop Corp'
type='result'
xml:lang='en'
>
<query xmlns='http://jabber.org/protocol/disco#info'>
component/>
```

```
<query>  
</iq>
```

## Related Links

[Discovery protocol for querying the S2S Command Processor](#) on page 125

## Outbound and inbound lists query

### Example

```
<iq id='disco-info-10'  
to='cm-2_s2scp-1.jabber'  
type='get'  
>  
<query xmlns='http://jabber.org/protocol/disco#items'  
node='-outbound'  
>  
</iq>  
<iq id='disco-info-10'  
to='cm-2_s2scp-1.jabber'  
type='get'  
>  
<query xmlns='http://jabber.org/protocol/disco#items'  
node='-inbound'  
>  
</iq>
```

## Related Links

[Discovery protocol for querying the S2S Command Processor](#) on page 125

## S2SCP query for all items

### Example

The following XMPP query asks for a list of all items associated with the S2SCP:

```
<iq id='disco-info-10'  
to='cm-2_s2scp-1.jabber'  
type='get'  
>  
<query xmlns='http://jabber.org/protocol/disco#items'>  
</iq>
```

The following response received from the server lists the items, which include an inbound node and an outbound node:

```
<iq xmlns='jabber:client'  
from='cm-2_s2scp-1.jabber'  
id='disco-info-10'  
to='ardiederich@example.com/Sample Messenger Desktop'  
type='result'  
xml:lang='en'  
>  
<query xmlns='http://jabber.org/protocol/disco#items'>  
<item jid='cm-2_s2scp-1.jabber'  
name='Inbound Connections'  
node='-inbound'  
>  
<item jid='cm-2_s2scp-1.jabber'  
name='Outbound Connections'  
node='-outbound'  
>  
</query>
```

```
</query>  
</iq>
```

## Related Links

[Discovery protocol for querying the S2S Command Processor](#) on page 125

---

# Configuring Authorization ACLs on System Manager

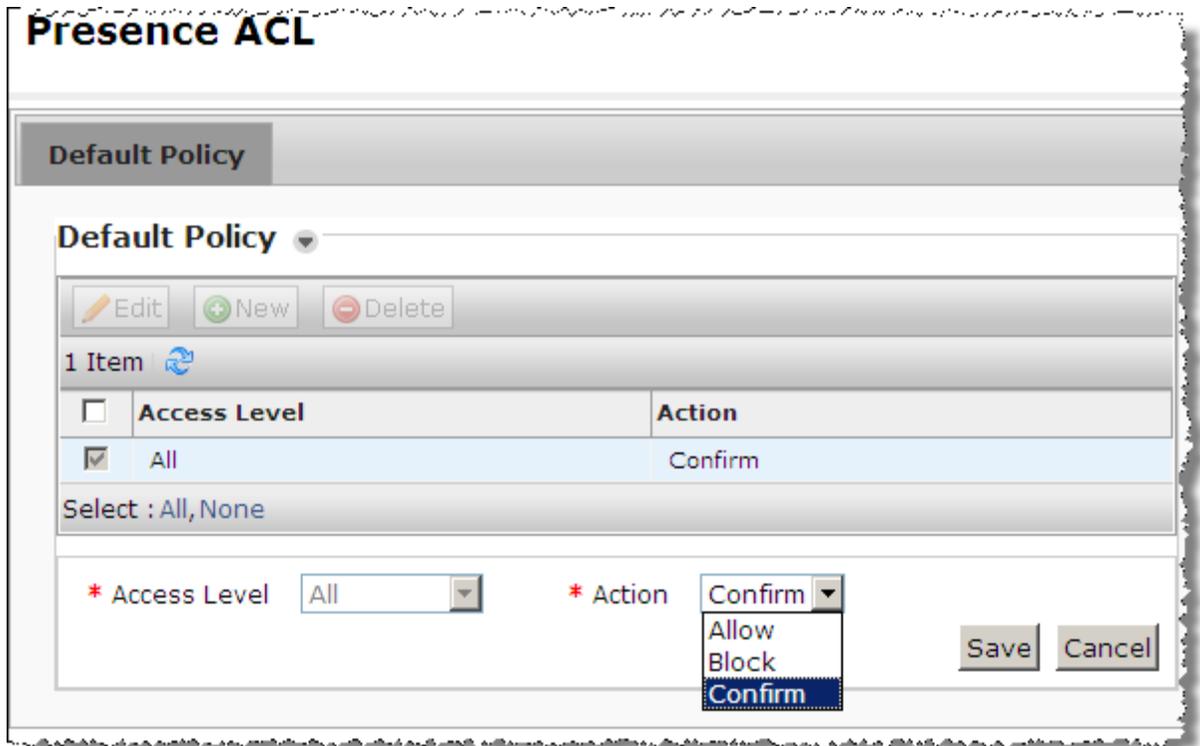
## About this task

Presence Services supports the Allow, Block, and Confirm ALC options. You can set the ACL options through the System Manager web console.

Use this procedure to define the policy for accessing the presence information.

## Procedure

1. Log in to the System Manager web console as an administrator.
2. On the System Manager dashboard, click **User Management**.
3. On the User Management page, click **System Presence ACLs**.
4. To set the default policy, perform the following steps:
  - a. In the Presence ACL section, click the **Default Policy** tab.
  - b. On the **Default Policy** tab, select the **All** check box, and click **Edit**.
  - c. From the **Action** drop-down box, select **Confirm** to implement the watcher authorization.  
  
The default value of the **Action** field is **Allow**.
  - d. Click **Save** to save the changes.



## Adding other presentities to the resource list of a user

### About this task

You can add presentities using the Avaya SIP devices like Avaya one-X<sup>®</sup> Communicator. However, you can also add them in System Manager, if required.

### Procedure

1. Log in to System Manager Web Console as an administrator.
2. On System Manager Dashboard, click **User Management**.
3. On the User Management page, click **Manage Users** on the left navigation pane.
4. On the Users page, select the relevant user and then click **Edit**.
5. On the User Profile Edit page, click the **Contacts** tab, and then click **Add** under **Associated Contacts**.
6. On the Attach Contacts page, select the presentity to add and click **Select**.
7. On the User Profile Edit page, again select the presentity, and then click **Edit**.

The system displays the Edit Contact List Member page.

8. Select the **Presence Buddy** check box and then click **Add**.

The system displays the User Profile Edit page.

- To save the changes, click **Commit**.

For more information, see the *System Manager* documentation.

---

## Multiuser chat

Presence Services supports all the variants of Avaya one-X<sup>®</sup> Communicator for extended stanza addressing, such as XEP-0033. You can send a message to multiple contacts, which enables you to have multiple chat sessions at the same time.

This feature is available by default. However, if you are unable to initiate multiple chats at the same time, you must enable the feature.

### \* Note:

End-points must maintain a list of participants and perpetuate the thread ID when they respond to a XMPP <message>with an XEP-033 <address> element.

### Related Links

[Enabling multiuser chat](#) on page 129

[Stanza optimizer parameters](#) on page 129

## Enabling multiuser chat

### Procedure

- Log in to the XCP Controller Web interface and change to the **Advanced** configuration view.
- On the Home page, under Components, from the **Add a new** drop-down list box, select **Stanza Optimizer** and then click **Go**. The system displays the Stanza Optimizer Configuration page.
- To enable stanza optimizer, enter the stanza optimizer parameters and then click **Submit**.

### Related Links

[Multiuser chat](#) on page 129

## Stanza optimizer parameters

Parameter	Description
Description	The description is displayed in the Components area on the controller's main page and should help you distinguish between components of the same type when you have more than one configured. You can change the description as needed.
Runlevel	Enter the order in which this component shuts down. The runlevel must be an integer value greater than or equal to zero. Component shutdown is executed in reverse order of the specified runlevel; components with the highest level (typically 70) shut down first.

Parameter	Description
	Do not change the runlevel unless you know exactly what you are doing and understand the effects that changing it will have. The default runlevel is provided to help the system shut down as smoothly as possible, and is based on this component's dependencies upon other components.
<b>Timeout for shutdown</b>	Enter the number of seconds that the server waits to receive acknowledgement from the component that the shutdown process has completed. If the component has not shut down by the time this time period has elapsed, the router leaves the process in its current state and continues shutting down other processes.
<b>Component Properties</b>	
<b>Number of packets buffered when component is down</b>	Enter the number of packets bound for the component that should be buffered if the component goes down.
<b>Bounce error packets to stderr</b>	Select Yes if you want the router to send warnings to stderr when the component is down.
<b>Router Outbound Connection Information</b>	Select this option only if you want the XCP router to connect to the component. For example, if the component is running outside your firewall, this option allows the router to connect to the component safely rather than introducing security risks by letting the component connect to it. By default, components connect to the router using the router's Master Accept Port.
<b>Component IP</b>	Enter the IP address or host name of the system on which the component is installed.
<b>Port</b>	Enter the port that the component uses for communications.
<b>Password</b>	Enter the password that the router uses to authenticate the component.
<b>Buffer size in bytes for outgoing data</b>	Enter the number of bytes the router should buffer when it sends information to the component. You may want to modify this element when working on performance enhancements.
<b>Buffer size in bytes for incoming data</b>	Enter the number of bytes the router should buffer when it receives information from the component. You may want to modify this element when working on performance enhancements.
<b>Send keepalives</b>	Select Yes if you want the router to send keep-alives to the component. The keep-alive helps prevent firewalls from dropping an unused connection to the

Parameter	Description
	component. If this option is set to No, keep-alives are disabled.
<b>Log the delivery of packets to this component</b>	Select Yes if you want to log the data that the router delivers to the component. The information is logged to the logger(s) you set up during Jabberd Logger configuration (syslog, file, or stderr). Socket-level logging happens only at the debug level.
<b>Execute an External Command</b>	This option allows the router to start the component automatically. If you prefer to start the component from a command line, disable this option.
<b>Maximum interval in seconds to wait before restarting component</b>	Enter the maximum number of seconds after which the router tries to restart the component. If the component goes down, the router tries to restart it after one second. If the component does not start, the router multiplies the wait time by 1.5, and tries again. Once the maximum time interval that you specify for this parameter is reached, the router continues to retry after waiting this amount of time.
<b>Maximum number of times to restart component</b>	Enter the total number of restarts allowed. The default setting, -1, means unlimited.
<b>Interval in seconds at which to reset this value to 1 second</b>	Enter the number of seconds that the component has been up and running, after which to set the restart time back to one second.
<b>Path to binary</b>	Enter the directory path to the shell that launches the component. You can change the default setting if needed.
<b>Command line to run</b>	<p>A command that runs the component automatically is provided by default. You can modify it if needed.</p> <p> <b>Note:</b></p> <p>Do not use the -B argument with this component. Since jabberd is already a daemon process, its children must not be daemons.</p> <p>You should not redirect output, because all output to STDOUT and STDERR will be redirected to /dev/null.</p>
<b>Hostnames for this Component</b>	This option specifies the hosts for which this component will handle packets. Specify a host filter only if you want the component to be externally addressable; for example, if you want clients and other components or programs to communicate with it. This is because the mod_disco module in JSM uses host filters to return the component as something that should be discoverable.
<b>Host Filters</b>	By default, the XCP server's host name prepended by stanza-optimizer is provided.

Parameter	Description
	<p>Enter the host names or IP addresses for which you want this component to handle packets. Separate each host name or address with a line break.</p> <p>Host filters must be host names, or IPv4 or IPv6 addresses. If you use an IP address, the packet address must also use this IP address.</p>
<b>Stanza Optimizer Configuration</b>	
<b>Number of threads to dedicate to stanza optimizer tasks</b>	<p>Enter the number of threads that you want to have processing tasks in the component. Increasing this value enables the component to handle more tasks at a time. However, it spends more time scheduling the tasks as this number increases.</p> <p>We recommend that you set this number to one more than the number of processors on your system.</p>
<b>Timeout (in seconds) for XEP-033 disco attempts</b>	<p>Enter the number of seconds to wait for the server to determine if non-local domains can handle stanza optimization. If a non-local domain cannot handle stanza optimization, one packet is sent per recipient.</p>
<b>Disco Cache Timeout (in minutes)</b>	<p>Enter the number of minutes that a discovery answer (positive or negative) should exist. The maximum number of minutes that you can specify is 1440 (24 hours).</p>
<b>Multiple optimizer address threshold</b>	<p>This parameter is to be used mainly for fine tuning your system. In most cases, the default value should be sufficient.</p> <p>The threshold refers to the number of recipients who are located in a remote domain. The value is the maximum number of recipients required for extended stanza addressing to take effect.</p>
<b>List of local domains</b>	<p>Enter the list of local domains. The Stanza Optimizer dynamically determines which domains are local, but you can enter them here to short circuit this discovery process. The Stanza Optimizer does not send optimized packets to local domains.</p>
<b>Component Logging (Jlog)</b>	<p>Select the <b>Component Logging (Jlog)</b> option only if you want to configure filtered level loggers that log messages to syslog and to a stream (stderr or stdout). You can enable either or both the syslog and stream loggers. These parameters are displayed in the controller's Intermediate and Advanced configuration views.</p>
<b>Add a new custom logger</b>	<p>If you have created a custom logger for logging component information using the libjcore library, click Go to access the Custom Logger Configuration page.</p>

Parameter	Description
<b>SNMP Configuration</b>	Select this option if you want to configure SNMP for the component.
<b>Enable SNMP</b>	Leave this parameter set to Yes.
<b>Count errors</b>	Select Yes only if you want to enable SNMP error counting. This option takes a great deal of server resource, so use it with caution.

**Related Links**

[Multiuser chat](#) on page 129

# Chapter 6: Presence Services federation with third-party servers

---

## Overview

Presence Services provides presence and IM services to Avaya Aura® users that are hosted by a single Presence server or a cluster of Presence servers. Through federation, Presence Services provides presence and IM services between Avaya Aura® users, and users that are hosted by a third-party server. Federation can also be used connect two separate Avaya Aura® presence domains.

Presence Services federation is certified with the following servers:

- Microsoft Lync/OCS, using a Microsoft-proprietary SIP protocol
- Ignite Realtime Openfire, using standard XMPP protocol
- Another Avaya Aura® Presence server, using standard XMPP protocol

In all of the above cases, federation is supported whether the Presence server is deployed as a standalone server or cluster of servers, and federation is supported whether the Presence server supports a single or multiple presence domains.

Since Presence Services federation is non-proprietary, federation with other third-party XMPP servers that conform to IETF XMPP and Server to Server (S2S) standards should be direct. For assistance, contact Avaya Aura® Professional Services.

To enable interoperability with a Microsoft Lync /OCS system, Presence Services must be configured with an OCS Gateway. For more information, see *Configuring OCS Gateway*.

To enable interoperability with a third-party XMPP server, Presence Services must be configured with an XMPP Connection Manager and an Open Port component. For more information, see *Configuring the basic Connection Manager* and *Configuring OpenPort*.

### Related Links

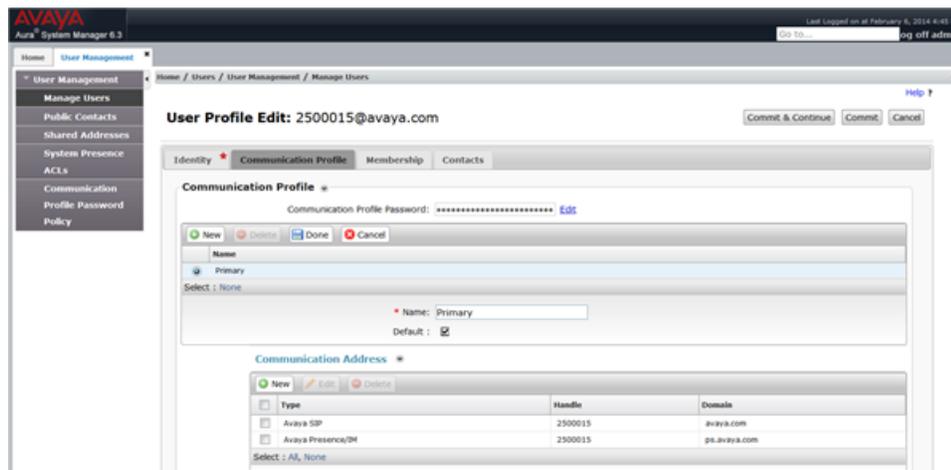
[Overview - Configuring OCS](#) on page 175

[Configuring the basic Connection Manager](#) on page 102

[Configuring OpenPort](#) on page 118

## Overview of user configuration in System Manager

Avaya Aura® users are configured in System Manager and can be assigned one or more communication addresses. For example, in the following figure, both Avaya SIP and Avaya Presence/IM communication addresses are assigned to the user.



For more information, see *User configuration in System Manager*.

### Related Links

[User configuration in System Manager](#) on page 24

## Watcher and Presentity

Users can be categorized as:

- **Watcher:** A user who is monitoring the presence state changes of another user or presentity.
- **Presentity:** A user whose presence state changes are being monitored by another user or watcher. Presentity is also referred to as contact or buddy.

For example, if User A adds User B to the contact list, then User A is the Watcher and User B is the Presentity.

### \* Note:

A user can simultaneously be watcher as well as presentity.

In federation, watchers and presentities can be categorized:

**Table 1: Federated Presentity categories**

Presentity category name	Description	Applicable devices	Communication addresses in System Manager
Presentity Category 1 (PC1)	A presentity that is hosted and managed by a federated server.	Microsoft OCS / Lync, or third-party XMPP client	None. These users are not configured in System Manager.
Presentity Category 2 (PC2)	A presentity with a device that is hosted by a federated server, but is configured in System Manager for Category 2 watchers.	Microsoft OCS / Lync, or third-party XMPP client	<ul style="list-style-type: none"> <li>• Avaya Presence/IM</li> <li>• Other XMPP, or Microsoft SIP</li> </ul>
Presentity Category 3 (PC3)	A presentity with a device that is hosted by a federated server, with another device that is hosted by Aura, and the user is configured in System Manager.	<ul style="list-style-type: none"> <li>• Microsoft OCS / Lync, or third-party XMPP</li> <li>• Avaya Aura client, for example, Avaya one-X<sup>®</sup> Communicator</li> </ul>	<ul style="list-style-type: none"> <li>• Avaya Presence/IM</li> <li>• Other XMPP or Microsoft SIP</li> <li>• Avaya SIP or Avaya E.164</li> </ul>

The key difference between PC1, and PC2 or PC3, is that PC2 or PC3 users need to be configured in System Manager with a Microsoft SIP or Other XMPP communication address, whereas PC1 users are not configured in System Manager. The key difference between PC2 and PC3 users is that a PC3 user has an Avaya Aura<sup>®</sup> device and an associated Avaya Aura<sup>®</sup> SIP or Avaya Aura<sup>®</sup> E.164 communication address, along with a third-party device and an associated Microsoft SIP or Other XMPP communication address. A PC2 user does not have an Avaya Aura device, and does not have an Avaya SIP or Avaya E.164 communication address.

**Table 2: Aura Watcher categories**

Aura Watcher Category name	Description	Applicable devices
Aura Watcher Category 1 (WC1)	The watcher is logged in to an Avaya Aura <sup>®</sup> device capable of directly adding a federated user as a contact.	Avaya one-X <sup>®</sup> Communicator
Aura Watcher Category 2 (WC2)	The watcher is logged in to an Avaya Aura <sup>®</sup> device that is incapable of adding a federated user as a contact.	All other Avaya Aura devices, except Avaya one-X <sup>®</sup> Communicator.

## Aura watcher and federated presentity behaviors

In a federated deployment, the interactions between users depend on the type of presentity and watcher. The following table summarizes the possible combinations that occur when the watcher is an Avaya Aura<sup>®</sup> user and the presentity is a federated user.

The scenario in row 1 provides the ideal federated solution:

- The end-user experience is intuitive and correct, particularly with respect to how federated users authorize Aura watchers.
- The least amount of System Manager administration is required as federated users are not configured in System Manager, and there is no need to run an ACL script.

Avaya recommends this deployment model. However, if the solution contains Category 2 Aura Watchers (WC2), then this deployment model may not be possible.

For the scenario in row 5, you may need to run the `user-default-policy-domain.sh` ACL script on System Manager. For more information see, *user-default-policy-domain.sh ACL script*.

**Table 3: Aura watcher and federated presentity behaviors**

Combinations		Behaviors				
Aura Watcher	Federated Presentity	Address to use when watcher adds presentity as a contact	Server responsible for Access Control when watcher adds presentity as contact	Access Control behavior	How Aura user initiates Instant Messaging to federated user	Ability for watcher to see presentity's presence state within search results <sup>1</sup>
WC1	PC1	External Address	Federated Server	See Note <sup>2</sup>	Direct IM	None, polite blocked <sup>3</sup>

<sup>1</sup> Some Aura devices support the ability to temporarily display the presence state of another user without adding that user as a contact. For example, using an Aura device, a watcher can search a corporate directory for other users or presentities, and within the search results that are displayed to the watcher the presence state of presentities is temporarily displayed. The ability for watchers to see the presence state of federated users within search results depends on the type of presentity being watched.

<sup>2</sup> The federated server and/or third-party device controls whether to allow or block presence to the watcher. If the federated server and/or third-party device have an effective ACL setting of Confirm, the federated user is prompted to individually authorize watchers when the watchers attempt to watch the presentity.

<sup>3</sup> Watchers who search for users by using their external address cannot see the presence status for the users in the search results, regardless of the effective ACL setting on either server.

Combinations		Behaviors				
WC1	PC3	Avaya Presence/IM communication address	Presence Server	See Note <sup>4</sup>	Selectable <sup>5</sup>	Determined by ACL <sup>6</sup>
WC2	PC1	N/A <sup>7</sup>	N/A <sup>7</sup>	N/A <sup>7</sup>	N/A <sup>7</sup>	N/A <sup>7</sup>
WC2	PC2	Avaya Presence/IM communication address	Presence Server	See Note <sup>8</sup>	Choose external device <sup>9</sup>	Determined by ACL <sup>6</sup>
WC2	PC3	Avaya Presence/IM communication address	Presence Server	See Note <sup>4</sup>	Selectable <sup>5</sup>	Determined by ACL <sup>6</sup>

**Related Links**

[user-default-policy-domain.sh ACL script](#) on page 139

- 
- <sup>4</sup> The Presence server is primarily responsible for controlling whether to allow or block presence to the watcher. If, on the Presence Services server, the effective ACL setting for this watcher-presentity pair is Confirm, the authorization dialogs appear only on the Aura device of the user, and watchers are only visible from this device. If the effective ACL setting on the third-party server or device is Confirm, then the first time the PC3 user logs on to the third-party device, the user is asked to authorize the Avaya Presence/IM communication address, but is not otherwise prompted to authorize watchers. The third-party device has no visibility about watchers.
  - <sup>5</sup> The Avaya Aura client allows the watcher to select the presentity device to which an instant message (IM) should be delivered. The watcher can send an IM either to the Avaya Aura device of presentity or the third-party device.
  - <sup>6</sup> The presence status in the search results depends on the effective ACL setting of Presence Services for the watcher-presentity pair, and the capabilities of the watcher client device. If the effective ACL setting is Allow on Presence Services, and the watcher client supports the ability to display presence status while searching for contacts, then a watcher can see the presence status of the presentity in the search results. If the effective ACL setting is Confirm or Block, then the watcher cannot see the presentity presence status in the search results.
  - <sup>7</sup> Category 2 watchers are not capable of directly adding an external presentity/contact. Therefore, these watchers do not support PC1 presentities.
  - <sup>8</sup> The Presence server is primarily responsible for controlling whether to allow or block presence to the watcher. If the system ACL policy is Confirm or Block, then by default Category 2 watchers cannot watch Category 2 presentities. To override this setting, the user-default-policy-domain.sh script must be run on System Manager. For more information, see user-default-policy-domain.sh ACL script. If the effective ACL setting on the third-party server/device is Confirm, then the first time the PC2 user logs on to the third-party device, the user is asked to authorize the Avaya Presence/IM communication address, but is not otherwise prompted to authorize watchers. The third-party device has no visibility about the watchers.
  - <sup>9</sup> The watcher Avaya Aura client might provide the option to initiate an IM to one of following addresses: the presentity Avaya Presence/IM communication address, or the presentity Microsoft SIP or Other XMPP communication address. To direct IMs to the presentity third-party device, the watcher should select the Microsoft SIP or Other XMPP communication address.

---

## user-default-policy-domain.sh ACL script

Category 2 watchers can watch the following types of presentities:

- Category 2 (PC2): A presentity with a device that is hosted by a federated server, but is configured in System Manager for Category 2 watchers.
- Category 3 (PC3): A presentity with a device that is hosted by a federated server, another device that his hosted by Aura, and the user is configured in System Manager.

When a Category 2 watcher attempts to watch a Category 3 presentity, the Presence server is primarily responsible for controlling whether to allow or block presence to the watcher, and the user manages watchers through the Aura device.

When a Category 2 watcher attempts to watch a Category 2 presentity, the Presence server is primarily responsible for controlling whether to allow or block presence to the watcher, but the user does not have an Aura device with which the user manages watchers. The watcher management is performed with an ACL script.

In a WC2-PC2 scenario, if the effective ACL policy for this watcher-presentity pair is Block or Confirm, then by default the watcher cannot watch the presentity. To override this setting with an Allow policy, run the `user-default-policy-domain.sh ACL` script. For more information, see *Running the user-default-policy-domain.sh ACL script*. Once this has been done, the Presence server allows any Category 2 watcher to watch any Category 2 presentity that has an Other XMPP or Microsoft SIP communication address in the *domain* specified in the script.

For more information, see *user-default-policy-domain.sh ACL script*.

### Related Links

[User default policy domain ACL script](#) on page 270

## Running the user-default-policy-domain.sh ACL script

### Procedure

1. Log in to Presence Services as a root user.
2. Navigate to the `/opt/Avaya/Presence/presence/bin` directory.
3. Copy the `user-default-policy-domain.sh` script to a temporary directory on the System Manager server.  
For example, `/tmp/directory`.
4. Log in to System Manager server as a root user.
5. Navigate to the temporary directory.
6. Run the `chmod +x ./user-default-policy-domain.sh` command to change the current mode to the executable mode.
7. Run the `./user-default-policy-domain.sh -c ALLOW extdomain.com` command, where *extdomain.com* is the federated domain.

---

## Aura or federated watcher and PC3 presentity

For any watcher of a PC3 presentity, Presence Services provides aggregated presence of both of the PC3 user devices. For example, consider the following watchers and presentity:

- Watcher User A has a Lync client hosted by a Microsoft server. User is not configured in System Manager.
- Watcher User B has an open source third-party client hosted by an Openfire server. The user is not configured in System Manager.
- Watcher User C has a Avaya one-X<sup>®</sup> Communicator SIP client hosted by Aura. The user is configured in System Manager with an Avaya SIP communication address and an Avaya Presence/IM communication address.
- Presentity User D has an Avaya one-X<sup>®</sup> Communicator SIP client hosted by Aura, and a third-party client hosted by a third-party server, for example, Lync client hosted by a Microsoft server. The user is configured in System Manager with an Avaya SIP communication address, an Avaya Presence/IM communication address, and a Microsoft SIP communication address. User D is a PC3 presentity user.

Watchers User A, User B, and User C add User D as a contact. The watchers add UserD through the Avaya Presence/IM communication address of User D. The presence state that the watchers can observe is an aggregation of both One-X device and Microsoft Lync device of User D.

For example:

- User D makes a phone call on the Avaya one-X<sup>®</sup> Communicator device. All watchers see User D as Busy.
- While this call is ongoing, User D manually sets presence state to Do Not Disturb on the Microsoft Lync device. All watchers see User D as Do Not Disturb. Presence Services generally prioritizes the manual presence states higher than automatic presence states.
- User D resets the Microsoft Lync device to automatic mode. Therefore, the presence state of the Microsoft Lync device is Available, but all watchers see User D as Busy. Presence Services aggregates the presence state of both of the devices of User D , and prioritizes automatic Busy on the Avaya one-X<sup>®</sup> Communicator device higher than automatic Available on the Microsoft Lync device.
- User D ends the phone call on the Avaya one-X<sup>®</sup> Communicator device. All watchers see User D as Available.

---

## Federated user and Avaya Aura<sup>®</sup> presentity

A federated watcher can add an Avaya Aura<sup>®</sup> presentity as a contact or buddy by using the Avaya Presence/IM communication address of the Avaya Aura<sup>®</sup> user. For the presentity, the experience is the same whether the watcher is federated or non-federated. ACL is managed by the Presence server, and if the effective ACL setting for this watcher-presentity pair is Confirm, then the presentity device handles this request in the same way as a request from an Avaya Aura<sup>®</sup> watcher. For

example, Avaya one-X<sup>®</sup> Communicator presents the user with an authorization dialog, while some hard clients might be configured to automatically authorize watch requests. A federated user is capable of directly sending IMs to the Avaya device of the Avaya Aura<sup>®</sup> user, provided the device supports IM.

---

## XMPP federation

---

### Overview – XMPP federation

Avaya Aura<sup>®</sup> Presence Services provides presence and IM services to Avaya Aura<sup>®</sup> users that are hosted by a single Presence server or a clustered Presence server.

XMPP federation is used for federation with Openfire or federation with another Presence Services instance or cluster.

 **Note:**

Presence Services does not support XMPP federation when Inter-Tenant Communication Control is enabled on System Manager.

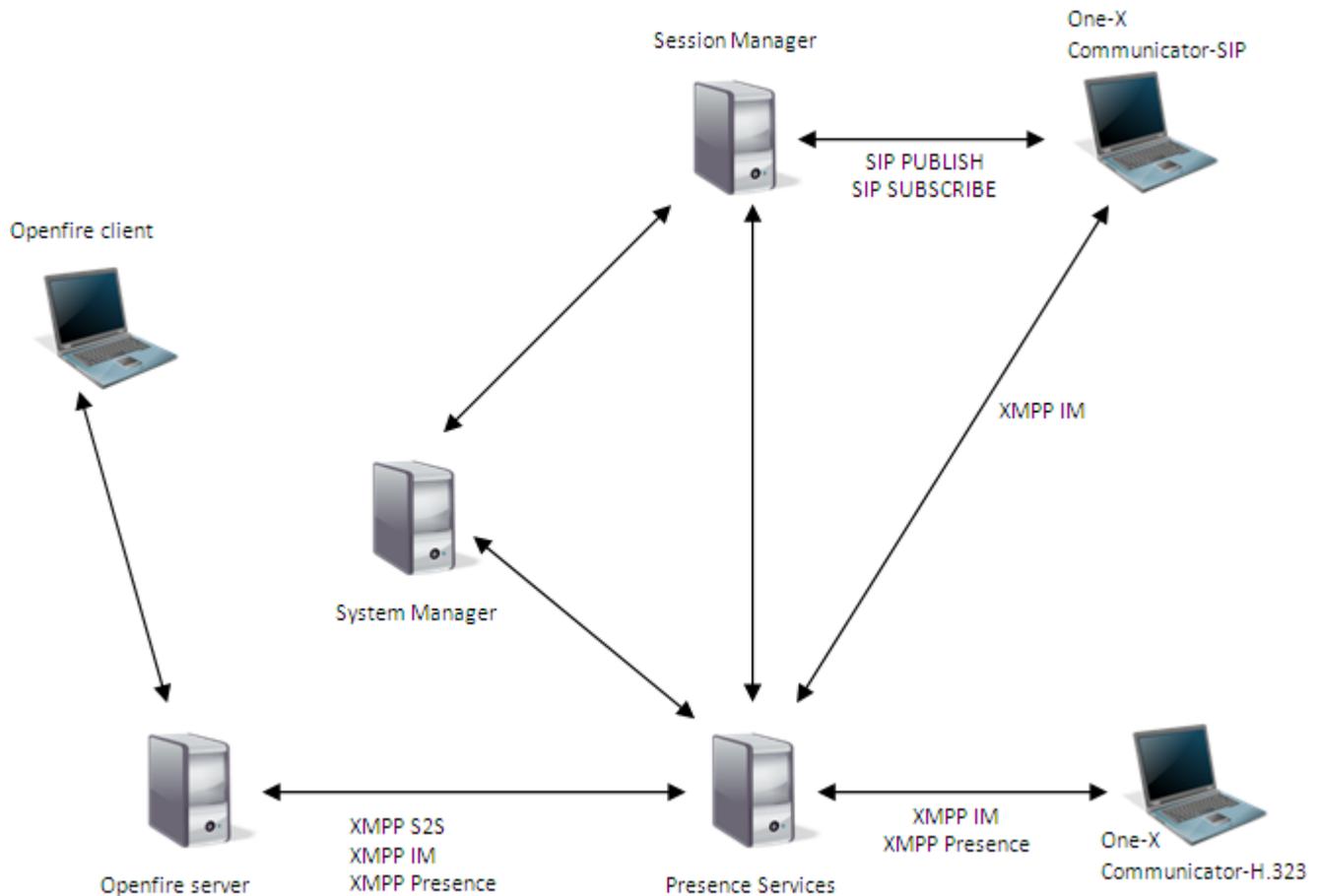
#### Related Links

[The Presence server and XMPP federation architecture](#) on page 141

### The Presence server and XMPP federation architecture

The deployment of Presence Services with Openfire or another Presence Services instance includes the following components:

- Avaya Aura<sup>®</sup> Presence Services.
- XMPP S2S. Server to Server connection.
- Optional. Avaya Aura<sup>®</sup> Session Manager.
- Avaya Aura<sup>®</sup> System Manager.
- Avaya clients. Avaya one-X<sup>®</sup> Communicator SIP and H.323.
- Third-party server. An example of a third-party server is Openfire.
- Openfire clients.



XMPP and Presence server architecture shows the network view of Presence Services and Openfire. Presence Services and Openfire use the XMPP S2S connection to exchange the IM and presence information. The Avaya one-X<sup>®</sup> Communicator H.323 clients establish an XMPP connection with Presence Services for exchanging the IM and presence information. The Avaya one-X<sup>®</sup> Communicator SIP clients establish an XMPP connection with Presence Services for exchanging IMs and use the SIP messages to subscribe or publish the presence information using Session Manager.

When an Avaya Aura<sup>®</sup> user, a watcher, adds a federated user, a presentity, as a contact, and the federated user publishes presence information, Presence Services converts the basic XMPP presence information received from the Openfire or the Presence Services server into a rich PIDF and sends presence information to the Avaya Aura<sup>®</sup> user. Conversely, when a federated user, who is a watcher, adds an Avaya Aura<sup>®</sup> user, a presentity, as a contact and the Avaya Aura<sup>®</sup> user publishes presence information, Presence Services converts the rich PIDF into basic XMPP presence information and sends presence information to the Openfire or the Presence Services server.

To configure the Avaya Aura<sup>®</sup> network, use System Manager.

### Related Links

[Overview – XMPP federation](#) on page 141

## XMPP Federation Configuration

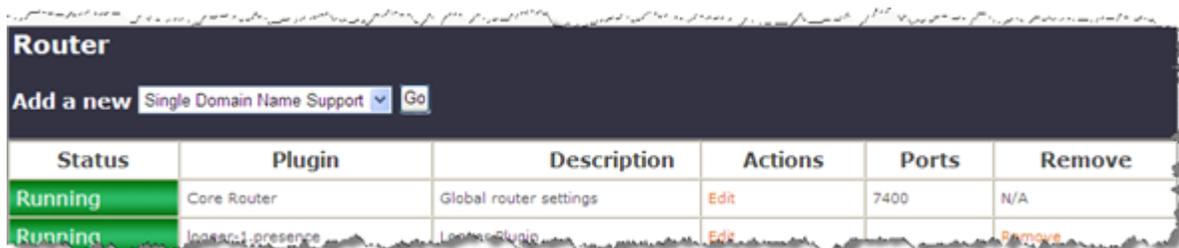
### Checklist for configuring XMPP federation

No.	Task	Link	✓
Presence Services server configuration			
1	Configure federated domains.	<a href="#">Configuring federated domains</a> on page 143	
2	Add a Server-to-Server Connection Manager component.	<a href="#">Adding a Server-to-Server Connection Manager component</a> on page 144	
3	Add an OpenPort component.	<a href="#">Adding an OpenPort component</a> on page 147	
Openfire server configuration (Optional)			
4	Configure Openfire server. This step is required only if federating between Presence Services and an Openfire server.	<a href="#">Configuring the Openfire XMPP server</a> on page 149	
DNS server configuration			
5	Configure DNS server.	<a href="#">Configuring the DNS server</a> on page 151	
Verifying the domains are resolvable			
6	Verify the domains are resolvable.	<a href="#">Verifying domains are resolvable</a> on page 156	

## Configuring federated domains

### Procedure

1. Log in to the Presence Services XCP Controller Web console (<https://<IP Address>:7300/admin>).
2. On the Presence Services home page, select the **Advanced** configuration view. Under the **Router** area, in the Core Router (Global router settings) section, click **Edit**.



The system displays the Global Settings Configuration page.

3. On the Global Settings Configuration page, select the **Federation Domains** check box.
4. In the **Federation Domain(s)** field, enter the federated domain(s).

If the federated server only supports a single domain, then enter only one domain. If the federated server supports multiple domains, for instance if federating with another Presence Services server which supports multiple presence domains, then list the domains by adding each one on a separate line.

5. To save the changes, click **Submit**.

## Adding a Server-to-Server Connection Manager component

### Procedure

1. Log in to the Presence Services XCP Controller Web console.
2. In the Components section, from **Add a new** drop-down list, select **Connection Manager**, and then click **Go**.

The system displays the Connection Manager Configuration page. By default, the system displays a basic configuration view, select the advanced configuration view.

**\* Note:**

On the Connection Manager Configuration page, in the Connection Manager section, you can rename the **Description** field to XMPP S2S Fed, for more clarity.

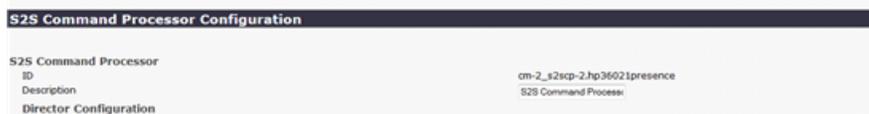
The screenshot shows the 'Connection Manager Configuration' page. The title bar is 'Connection Manager Configuration'. The page is divided into two columns. The left column contains labels for various settings, and the right column contains the corresponding input fields. The settings include: ID (cm-2.hp36021presence), Description (XMPP S2S Fed), Runlevel (50), Timeout for shutdown (60), Component Properties (checked), Number of packets buffered when component is down (512), Bounce error packets to stderr (Yes), Router Outbound Connection Information (unchecked), Component IP (10.136.1.21), Port (7301), Password (masked with asterisks), Confirm Password (masked with asterisks), Buffer size in bytes for outgoing data (65535), Buffer size in bytes for incoming data (65535), Send keepalives (No), Log the delivery of packets to this component (Yes), Execute an External Command (checked), Maximum interval in seconds to wait before restarting component (30), Maximum number of times to restart component (-1), Interval in seconds at which to reset this value to 1 second (empty), and Command line to run (empty).

3. Scroll down to the Add a New Command Processor section.
4. In the Add a New Command Processor section, from the **Add a new** drop-down list, select **S2S Command Processor** and click **Go**.



The system displays the S2S Command Processor Configuration page.

Note the S2S Command Processor ID that is automatically created. For example, **cm-2\_s2scp-2.hp36021presence**. This value id required when creating an OpenPort component.



5. In the Director Configuration section, verify the following setting for an outgoing server director:



- a. Click **Details** next to **XMPP Outgoing Server Director**.

The system displays the XMPP Outgoing Server Director Configuration page.

- b. In the **Timeout for idle connections (in seconds)** field, verify that the value is 0.  
If the value is other than 0, set the value to 0.

- c. Click **Submit** to save the changes, or **Cancel** otherwise

The system returns to the S2S Command Processor Configuration page.

6. Deny outgoing messages from all domains except the local Presence Services domains:
  - a. On the S2S Command Processor Configuration page, scroll down to the **Authorized Outgoing 'From' Addresses** section.
  - b. In the **Default behavior** field, click **deny**.
  - c. In the **Host Filters** field, enter the local Presence Services domain name(s).

If the local Presence Services server only supports a single presence domain, then enter one domain. If the local Presence Services server supports multiple presence domains, then list the domains by adding each one on a separate line.

- d. To save the changes, click **Submit**.

## Presence Services federation with third-party servers

**S2SCP Configuration**  
You must also configure an Open Port for this command processor.

**Router Connection Information**

Connection type: connect

Component IP: 10.136.1.21

Port: 7400

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Dialback secret: secret

Local IP address used for outgoing connections

**Authorized Outgoing 'From' Addresses**

Default behavior: deny

Hosts and IPs are exceptions to this behavior.

**Host Filters**

Host(s): avaya.com

The system displays the Connection Manager Configuration page.

- At the bottom of the Connection Manager Configuration page, click **Submit**.

The system displays the main Presence Services XCP Controller Web console, and at the bottom of the screen the system displays the new Server-to-Server Connection Manager component. The status of the component may be **Stopped**, and the status may automatically transition to **Running** with a message recommending that you select the **Apply** option. At this point, it is unnecessary to apply the change or restart the system, as a system restart is performed after creating an OpenPort component.

**Components**  
Add a new Connection Manager

Status	Component	Description	Actions	Ports	Remove
Running	server-1-hj36021presence	SIP Presence Server	Edit, Stop	8061 (2004)	N/A
Running	server-proxy-1-hj36021presence	SIP Proxy	Edit, Stop	8061 (2004), 8061 (2004), 25061	N/A
Running	server-subscriber-1-hj36021presence	SIP Sub Subscriber Server	Edit, Stop	25061	N/A
Running	cm-1-hj36021presence	Connection Manager	Edit, Stop	5222 (2029), 7400	N/A
Running	presence-container-1-hj36021presence	Presence Server	Edit, Stop		N/A
Running	presence_transformer-1-hj36021presence	Presence Transformer Component	Edit, Stop		N/A
Running	rlm-1-hj36021presence	Resource List Management Service	Edit, Stop		N/A
Running	server-open-port	Generic Open Port	Edit, Stop		N/A
Running	server-single-domain-name-support	Single Domain Name Support	Edit, Stop		N/A
Running	sipmanager-1-hj36021presence	SIPManager Component	Edit, Stop		N/A
Running	authmanager-1-hj36021presence	Auth Component	Edit, Stop		N/A
Running	status-optimizer-1-hj36021presence	Status Optimizer Component (SOP-030)	Edit, Stop		N/A
Stopped	cm-2-hj36021presence*	S2SCP S2S Fed	Edit, Start	5229 (7400)	Remove

\* Indicates that a configuration of a component has been modified. To apply changes please restart the modified components or restart the whole system. [Restart the system](#)

**Components**  
Add a new Connection Manager

Status	Component	Description	Actions	Ports	Remove
Running	server-1-hj36021presence	SIP Presence Server	Edit, Stop	8061 (2004)	N/A
Running	server-proxy-1-hj36021presence	SIP Proxy	Edit, Stop	8061 (2004), 8061 (2004)	N/A
Running	server-subscriber-1-hj36021presence	SIP Sub Subscriber Server	Edit, Stop	25061	N/A
Running	cm-1-hj36021presence	Connection Manager	Edit, Stop	5222 (2029), 7400	N/A
Running	presence-container-1-hj36021presence	Presence Server	Edit, Stop		N/A
Running	presence_transformer-1-hj36021presence	Presence Transformer Component	Edit, Stop		N/A
Running	rlm-1-hj36021presence	Resource List Management Service	Edit, Stop		N/A
Running	server-open-port	Generic Open Port	Edit, Stop		N/A
Running	server-single-domain-name-support	Single Domain Name Support	Edit, Stop		N/A
Running	sipmanager-1-hj36021presence	SIPManager Component	Edit, Stop		N/A
Running	authmanager-1-hj36021presence	Auth Component	Edit, Stop		N/A
Running	status-optimizer-1-hj36021presence	Status Optimizer Component (SOP-030)	Edit, Stop		N/A
Running	cm-2-hj36021presence*	S2SCP S2S Fed	Edit, Stop, Start	5229 (7400)	N/A

\* Indicates that a configuration of a component has been modified. To apply changes please restart the modified components or restart the whole system. [Restart the system](#)

### \* Note:

During creation of the Server-to-Server Connection Manager component, three Outgoing Connection Attempt Rules are automatically created. The first rule is required to successfully establish Presence Services federation with another server. To view the rule, from the Presence Services XCP Controller Web console, scroll down to the newly-created Server-to-Server Connection Manager component, and click **Edit**. The system displays the Connection Manager Configuration page. Scroll down to the S2S Command Processor and click **Details**.

Connection Manager Configuration

Maximum number of sockets: 1000

Maximum size of the threadpool: 3

User to run the CM as:

Add a New Command Processor

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new: JSM Command Processor [Go]

Name	Actions	Description	Remove
cm-2_s2scp-1.hp36021presence	Detail	S2S Command Processor	Remove

The system displays the S2S Command Processor Configuration page. Scroll down to the **Outgoing Connection Attempt Rules** section, and click **Detail** to the left of the first rule.

**Outgoing Connection Attempt Rules**

All rules (including initial defaults) must have their Director IDs match one of the directors above.

Add new items by clicking 'GO'.

Add a new Rule [Go]

Id	Actions	Description	Remove
1	Detail	cm-2_s2scp-1_xmppsoout-1	Remove
2	Detail	cm-2_s2scp-1_xmppsoout-1	Remove
3	Detail	cm-2_s2scp-1_xmppsoout-1	Remove

The system displays the Rule Configuration page.

**Rule Configuration**

Rule

Director ID: cm-2\_s2scp-1\_xmppsoout

Must match one of the loaded directors.

DNS SRV lookup to use: \_xmpp-server\_tcp

Port to use instead of DNS SRV lookup:

Do not delete or edit this rule, as this rule is required for successful DNS lookups by the Presence Services server when routing outgoing XMPP messages to a federated server. Click **Cancel** three times to return to the Presence Services XCP Controller Web console.

## Adding an OpenPort component

### Before you begin

When creating an OpenPort component, the system prompts for an ID. Perform the following steps to get the ID:

1. Log on to the Presence Services XCP Controller web console.
2. Scroll down to the Server-to-Server Connection Manager component created for XMPP federation, and click **Edit**.

The system displays the Connection Manager Configuration page.

3. Scroll down to S2S Command Processor, and in the **Name** column, the system displays an identifier .

In the following screen shot, the identifier is `cm-2_s2scp-1.hp36021presence`. In this example, note that `hp36021presence`. This identifier is Router Realm configured when the Presence Services server was installed.

## Presence Services federation with third-party servers

Connection Manager Configuration

Maximum number of sockets: 1000

Maximum size of the threadpool: 3

User to run the CM as: [text box]

Add a New Command Processor

Add new items by selecting from the drop-down and clicking 'GO'.

Add a new: JSM Command Processor [Go]

Name	Actions	Description
cm-2_s2scp-1.hp36021presence	<a href="#">Details</a>	S2S Command Processor

Component Logging (Jlog)

The ID consists of all characters to the left of the "." character in the identifier.

Remove Router Realm from the identifier. , In the previous example, the ID is `cm-2_s2scp-1`.

When creating an OpenPort component, the system prompts for the federated domains. If federating with an Openfire server, perform the following steps to get the federated domain:

1. Log on to the Openfire Admin web console.
2. Click **Server > System Properties**.
3. In **System Properties**, locate Property Value of **xmpp.domain** Property Name.

In the following screen shot, the value is `of.avaya.com`.

openfire

Server | Users/Groups | Sessions | Group Chat | Plugins

Server Manager | Server Settings | Media Services

System Properties

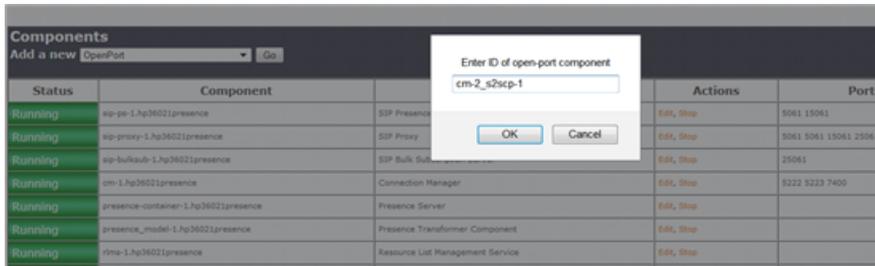
Below is a list of the system properties. Values for password sensitive fields are hidden. Long property names and values are clipped. Hold name and value, click the edit icon next to the property.

Property Name	Property Value
passwordKey	hidden
provider.admin.className	org.jivesoftware.openfire.admin.DefaultAdminProvider
provider.auth.className	org.jivesoftware.openfire.auth.DefaultAuthProvider
provider.group.className	org.jivesoftware.openfire.group.DefaultGroupProvider
provider.lockout.className	org.jivesoftware.openfire.lockout.DefaultLockOutProv...
provider.securityAudit.className	org.jivesoftware.openfire.security.DefaultSecurityAud...
provider.user.className	org.jivesoftware.openfire.user.DefaultUserProvider
provider.vcard.className	org.jivesoftware.openfire.vcard.DefaultVCardProvider
update.lastCheck	1395853026532
xmpp.auth.anonymous	true
xmpp.domain	of.avaya.com

### Procedure

1. Log on to the Presence Services XCP Controller web console.
2. In the Components section, in the **Add a new** field, click **OpenPort**, and then click **Go**.  
The system prompts for the ID.
3. In the **Enter ID of open-port component** dialog box, type the ID obtained earlier, and click **OK**.

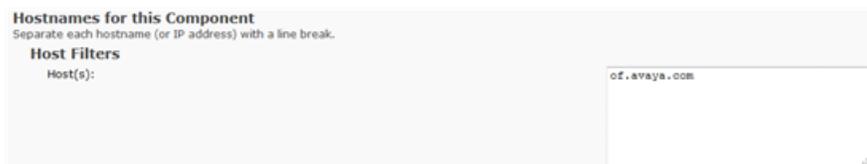
The system displays the OpenPort Configuration page.



4. Ensure that the configuration view is set to **Advanced**.
5. In the **Description** field, type a name.  
For example, XMPP OpenPort.
6. In the Hostnames for this Component section, in the **Host(s)** field, type the federated domains.

If federating with an Openfire server, use Property Value of **xmpp.domain** Property Name.

If the federated server supports multiple domains, add each one on a separate line.



7. Click **Submit**.

The system returns to the Presence Services XCP Controller web console and displays the newly-created OpenPort component.

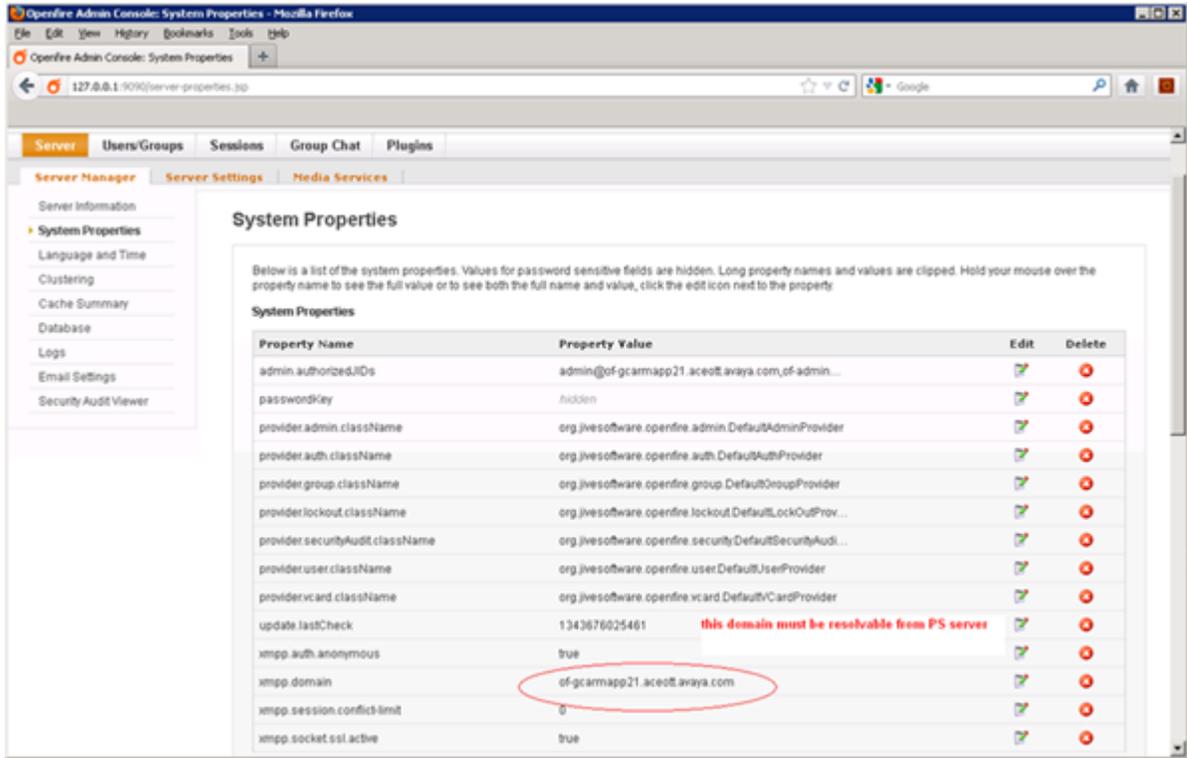
8. Click **Restart the system**.

## Configuring the Openfire XMPP server

By default, the Openfire server enables the Server-to-Server Connection Manager component that is required for the basic federation between a Presence server and an XMPP server.

### Procedure

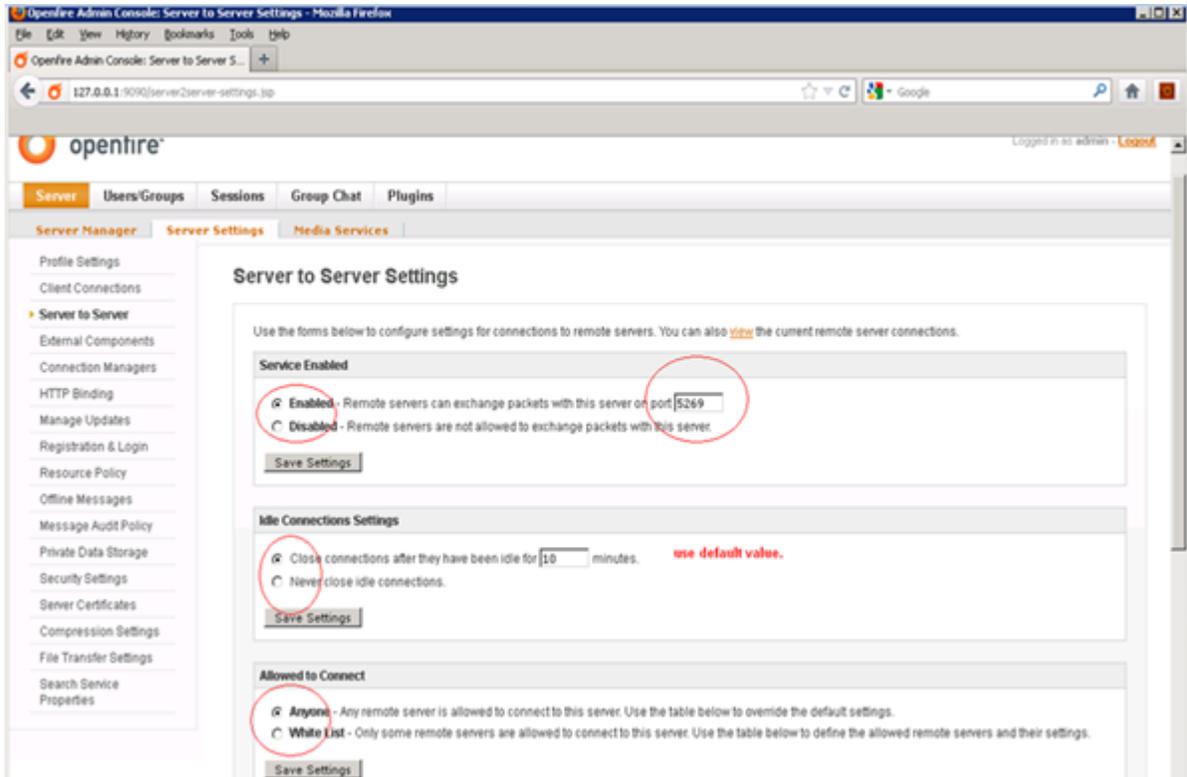
1. Log on to the Openfire Admin web console.
2. Click **Server > Server Manager > System Properties**.
3. In System Properties, check the property value of the XMPP domain.



4. Click **Server > Server Settings > Server to Server**.

The system displays the Server to Server Settings page.

5. In the Service Enabled field, select the **Enabled – Remote servers can exchange packets with this server port** option, and type 5269.
6. In the Idle Connections Settings field, select the **Close connections after they have been idle for \_\_ minutes** option, and accept the default value.
7. In the Allowed to Connect field, select the **Anyone – Any remote server is allowed to connect to this server**. Use the table below to override the default settings option.



## Configuring the DNS server

### Before you begin

If you are federating the Presence Services server with an Openfire server, you must obtain the following:

1. The Server-to-Server port from an Openfire server. For more information, see *Obtaining the Server-to-Server Port from an Openfire server*.
2. The local presence domains from an Openfire server. For more information, see *Obtaining the local presence domain(s) from an Openfire server*.
3. The IP address or the host name of the Openfire server.

If you are federating the Presence Services server with another Presence Services server, you must obtain the following:

1. The Server-to-Server port from a Presence Services server. For more information, see *Obtaining the Server-to-Server Port from a Presence Services server*.
2. The local presence domains from a Presence Services server. For more information, see *Obtaining the local presence domains from a Presence Services server*.
3. The IP address or the host name of the federated Presence Services server.

### About this task

Use this procedure to create DNS SRV records for each server that you are federating. For an Openfire server, you require one DNS SRV record. For a Presence Services server, you require one DNS SRV record for each presence domain.

For example,

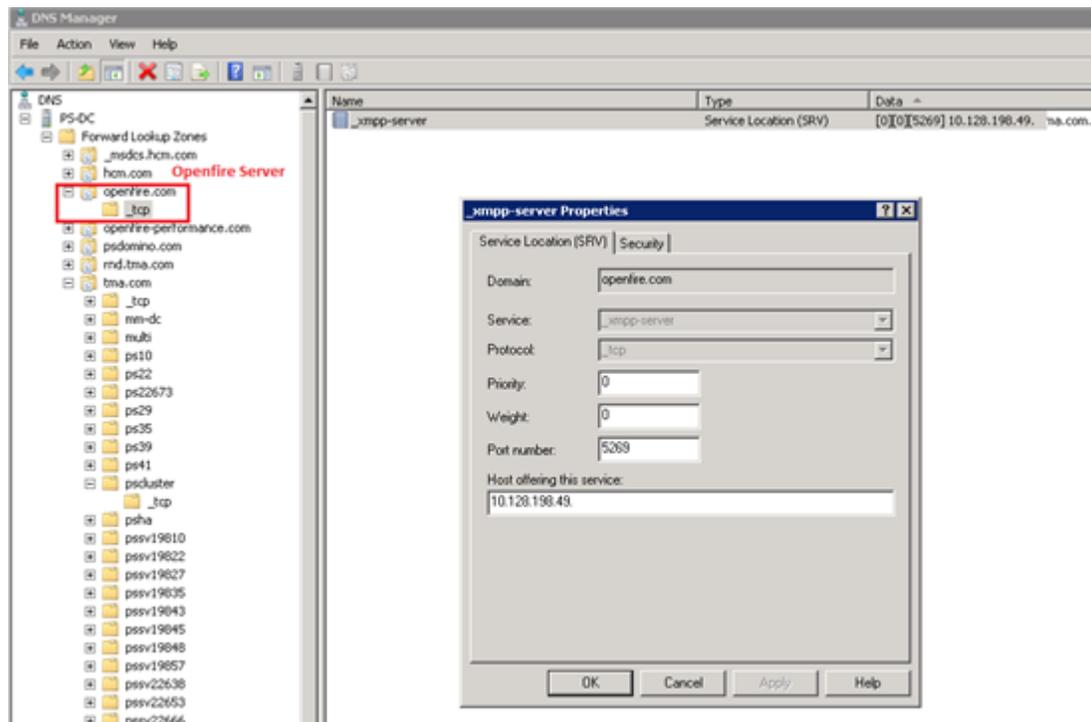
- If a Presence Services server supports a single presence domain and is federating with an Openfire server, you require two DNS SRV records.
- If a Presence Services server supports three presence domains and is federating with an Openfire server, you require four DNS SRV records.
- If a Presence Services server supports three presence domains and is federating with another Presence Services server that supports five presence domains, you require eight DNS SRV records.
- For a Presence Services cluster federation, see *XMPP Federation with Presence Services Cluster*.

## Procedure

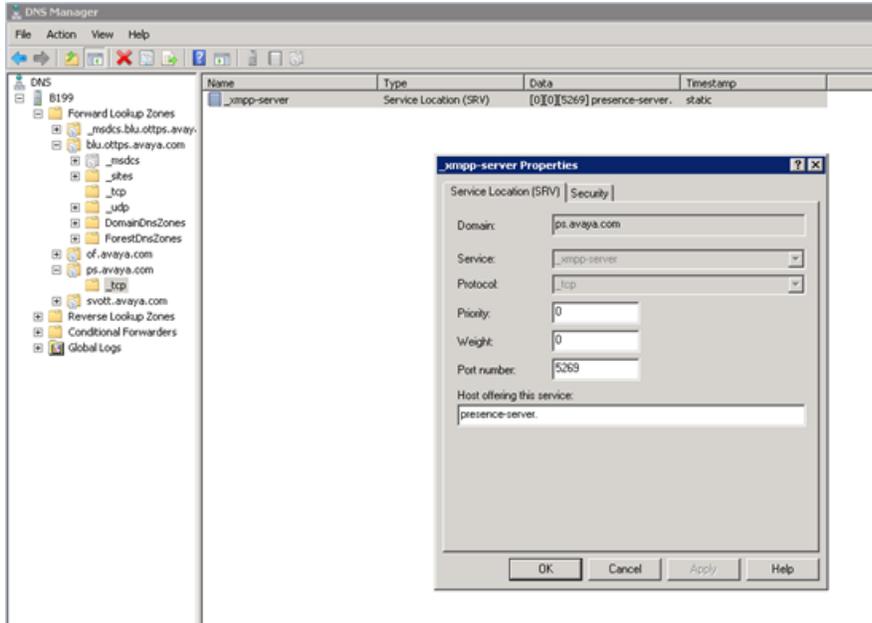
On the DNS server, create each DNS SRV record with the following values:

- **Domain:** local presence domain
- **Service:** `_xmpp-server`
- **Protocol:** `_tcp`
- **Port Number:** *Server-to-Server Port*
- **Host offering this service:** *Server IP address, or Server Host Name*

For example, the following is a DNS SRV record for an Openfire server:



For example, the following is a DNS SRV record for a Presence Services server that supports a single presence domain:



## Obtaining the Server-to-Server port from a Presence Services server Procedure

1. Log on to the Presence Services XCP Controller web console.
2. Scroll down to the Server-to-Server Connection Manager component created for the XMPP federation, and click **Edit**.

The system displays the Connection Manager Configuration page.

3. Scroll down to S2S Command Processor, and in the **Actions** column, click **Details**.

The system displays the S2S Command Processor Configuration page.

4. In the Director Configuration section, click **Details** next to XMPP Incoming Server Director.

The system displays the XMPP Incoming Server Director Configuration page.

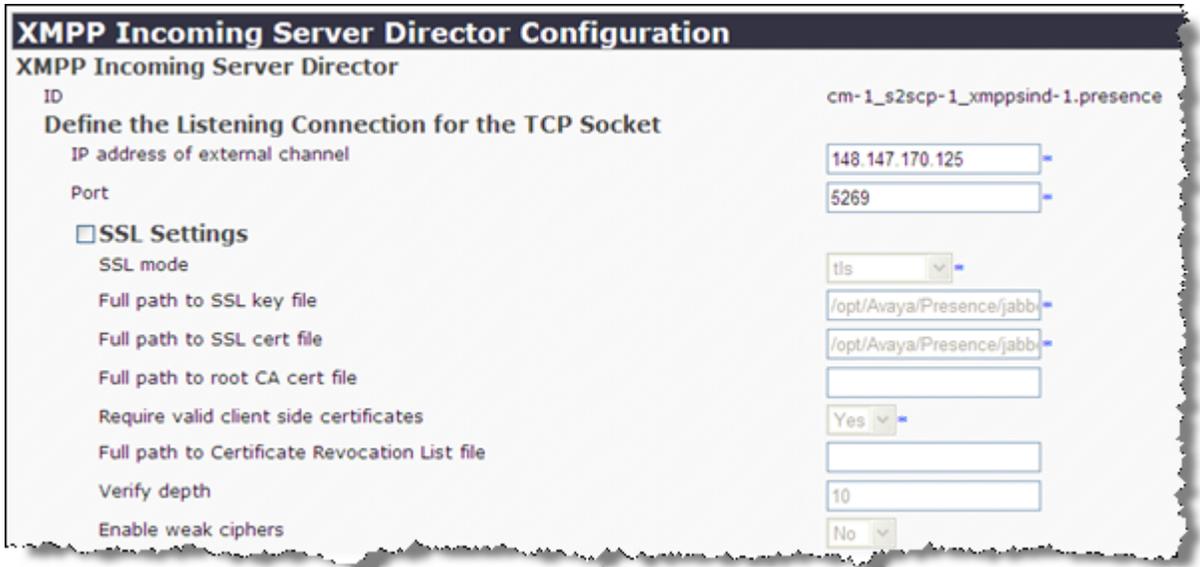
**Director Configuration**  
*Add new items by selecting from the drop-down and clicking 'GO'.*

Add a new XMPP Incoming Server Director

Name	Actions	Description	Remove
cm-2_s2scp-1_xmppscind-1.hp36021presence	<a href="#">Details</a>	XMPP Outgoing Server Director	<a href="#">Remove</a>
cm-2_s2scp-1_xmppscind-1.hp36021presence	<a href="#">Details</a>	XMPP Incoming Server Director	<a href="#">Remove</a>

5. In the **XMPP Incoming Server Director** section, note the value of the **Port** field.

By default, the value is **5269**.

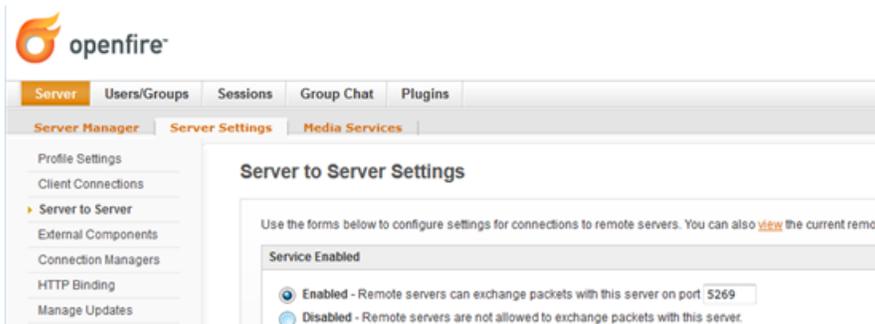


## Obtaining the Server-to-Server Port from an Openfire server

### Procedure

1. Log in to the Openfire Web console.
2. Click **Server > Server Settings > Server to Server**.
3. In the **Service Enabled** section, the **Enabled** check box should be checked, and the port value is contained in the box to the right of **Remote servers can exchange packets with this server on port**.

By default the value is **5269**, and it is recommended that this default value be maintained.



## Obtaining the local presence domain(s) from an Openfire server

### Procedure

1. Log in to the Openfire web console.
2. Click **Server > System Properties**.

- In **System Properties**, note the **Property Value** for the Property Name named **xmpp.domain**.

Below is a list of the system properties. Values for password sensitive fields are hidden. Long property names and values are clipped. Hold your mouse over a property name and value, click the edit icon next to the property.

Property Name	Property Value
passwordKey	hidden
provider.admin.className	org.jivesoftware.openfire.admin.DefaultAdminProvider
provider.auth.className	org.jivesoftware.openfire.auth.DefaultAuthProvider
provider.group.className	org.jivesoftware.openfire.group.DefaultGroupProvider
provider.lockout.className	org.jivesoftware.openfire.lockout.DefaultLockOutProv...
provider.security.audit.className	org.jivesoftware.openfire.security.DefaultSecurityAud...
provider.user.className	org.jivesoftware.openfire.user.DefaultUserProvider
provider.vcard.className	org.jivesoftware.openfire.vcard.DefaultVCardProvider
update.lastCheck	1395853026532
xmpp.auth.anonymous	true
xmpp.domain	of.avaya.com

## Obtaining the local presence domain(s) from a Presence Services server

### About this task

Presence Services supports one or more presence domains. Use the following procedure to determine the presence domains.

### Procedure

- Log in to the System Manager web console.
- Navigate to **Elements > Routing > Domains**.
- If there is only one routing domain with **sip** type, then Presence Services supports zero or one presence domain.

The local presence domain is displayed in the **Name** field.

Domain Management

New Edit Delete Duplicate More Actions

Name	Type
avaya.com	sip

- If there is more than one routing domain with **sip** type, then Presence Services may support more than one presence domains. To determine which routing domains support presence, search for all users with an Avaya Presence/IM communication address and check the value of the **Domain** field.

To obtain the value of Avaya Presence/IM communication address, navigate to **Users > User Management > Manage Users > Communication Profile > Communication Address >**

**Type = Avaya Presence/IM** on the System Manager dashboard. For more information, see *User configuration in System Manager*.

## Verifying domains are resolvable

### About this task

On each server, verify that the federated presence domain(s) is resolvable. In the following example, an Openfire server with local presence domain **openfire.com** and host name **openfire.host** is federating with a Presence Services server with local presence domains **aura.presence.1** and **aura.presence.2**, and hostname **ps.host**. As such, three DNS SRV records have been created.

### Procedure

1. Verify that Openfire domain is resolvable from Presence Services server:
  - a. Log in to the Presence Services server Command Line Interface (CLI).
  - b. At the command prompt, run the following command: `nslookup -querytype=SRV _xmpp-server._tcp.<Openfire domain>`.  
For example, `nslookup -querytype=SRV _xmpp-server._tcp.openfire.com`  
If successful, the system displays either the Openfire server IP address or hostname.
  - c. If the system displays the Openfire server IP address, proceed to step 1.e.
  - d. If the system displays the Openfire server hostname, at the command prompt, run the following command: `nslookup -querytype=A <Openfire hostname>`.  
For example, `nslookup -querytype=A openfire.host`  
If successful, the system displays the Openfire server IP address.
  - e. From the Presence Services server CLI, verify network connectivity to the Openfire server by pinging the Openfire server IP address.
2. Verify that Presence Services domains are resolvable from Openfire server:
  - a. Log in to the Openfire server Command Line Interface (CLI).
  - b. At the command prompt, run the command: `nslookup -querytype=SRV _xmpp-server._tcp.<Presence Services domain>`.  
For example, `nslookup -querytype=SRV _xmpp-server._tcp.aura.presence.1`  
For example, `nslookup -querytype=SRV _xmpp-server._tcp.aura.presence.2`  
If successful, the system displays either the Presence Services server IP address or hostname.
  - c. If the system displays the Presence Services server IP address, proceed to step 2.e.
  - d. If the system displays the Presence Services server hostname, at the command prompt, run the command: `nslookup -querytype=A <Presence Services hostname>`.

For example, `nslookup -querytype=A ps.host`

If successful, the system displays the Presence Services server IP address.

- e. From the Openfire server CLI, verify network connectivity to the Presence Services server by pinging the Presence Services server IP address.

## Troubleshooting

### Enabling optional logging from the XCP Controller Web console

#### Procedure

1. Log in to the Presence Services XCP Controller Web console and switch to the **Advanced/Intermediate** configuration view.
2. On the Connection Manager Configuration page, under the Connection Manager Configuration section, click the **Component Logging (Jlog)** check box.
3. Click **Logger** and then click **Filtered Syslog Logger**.

**Component Logging (Jlog)**

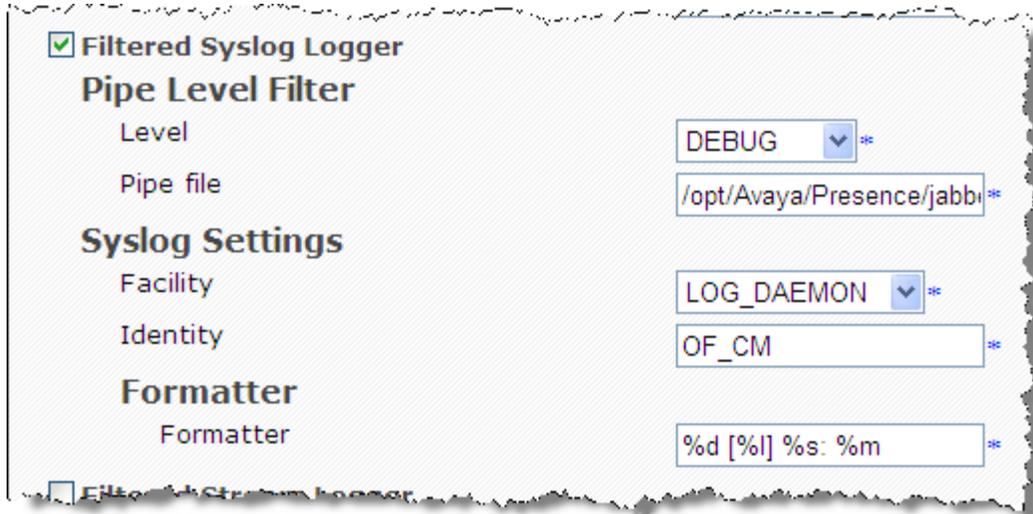
- Logger**
  - Filtered File Logger**
  - Filtered Syslog Logger**

**Pipe Level Filter**

Level: WA...  
 Pipe file:   
**File Settings**  
 Name and location:   
 Memory buffer size (in bytes):   
 Size of file (in megabytes) after which the log rotates:   
 Number of hours after which the log rotates:   
 Number of log files to keep after the log rotates:   
**Formatter**  
 Formatter:

4. Under Pipe Level Filter, from the **Level** drop-down list, select **DEBUG**.

5. In the **Pipe file** field, type `/opt/Avaya/Presence/jabber/xcp/var/log/of-cm.pipe`.
6. Under Syslog Settings, from the **Facility** drop-down list, select **LOG\_DAEMON**.
7. In the **Identity** field, type `OF_CM`.



The screenshot shows a configuration window for a "Filtered Syslog Logger". It includes several sections: "Pipe Level Filter" with a "Level" dropdown set to "DEBUG"; "Pipe file" with a text field containing "/opt/Avaya/Presence/jabber/xcp/var/log/of-cm.pipe"; "Syslog Settings" with a "Facility" dropdown set to "LOG\_DAEMON" and an "Identity" text field containing "OF\_CM"; and "Formatter" with a "Formatter" text field containing "%d [%l] %s: %m". There are also checkboxes for "Filtered Syslog Logger" (checked) and "Filtered Stream Logger" (unchecked).

8. To save the changes, click **Submit**.

## Enabling optional logging using CLI

### Procedure

1. Log in to the Presence Services server.
2. At the command prompt, type the `su root` command to log in as the root user.
3. To check the current log level, type `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh OF_CM -c`.
4. To increase the logging level, type the following command till you reach the **DEBUG** level, `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh OF_CM -i`.

The default logging level is **WARNING**.

5. In the `/etc/rsyslog.conf` file, check the filtering level of the rsyslog logger.
6. Type `Service rsyslog restart` to restart service logging.

---

## XMPP Federation with Presence Services Cluster

---

### Checklist for configuring XMPP federation for a Presence Services cluster

No.	Task	Link	✓
1	Configure DNS to add SRV records.	<a href="#">Configuring DNS</a> on page 159	
2	Add the R2R component to every Presence Services instance in the cluster.	<a href="#">Adding Router-to-Router connection</a> on page 161	
3	Configure the federation domain on every Presence Services instance in the cluster.	<a href="#">Configuring the federation domain</a> on page 163	
4	Add the S2S component to a Presence Services instance in the cluster.	<a href="#">Adding the S2S component</a> on page 163	
5	Add the OpenPort component to a Presence Services instance in the cluster.	<a href="#">Adding the OpenPort component</a> on page 164	

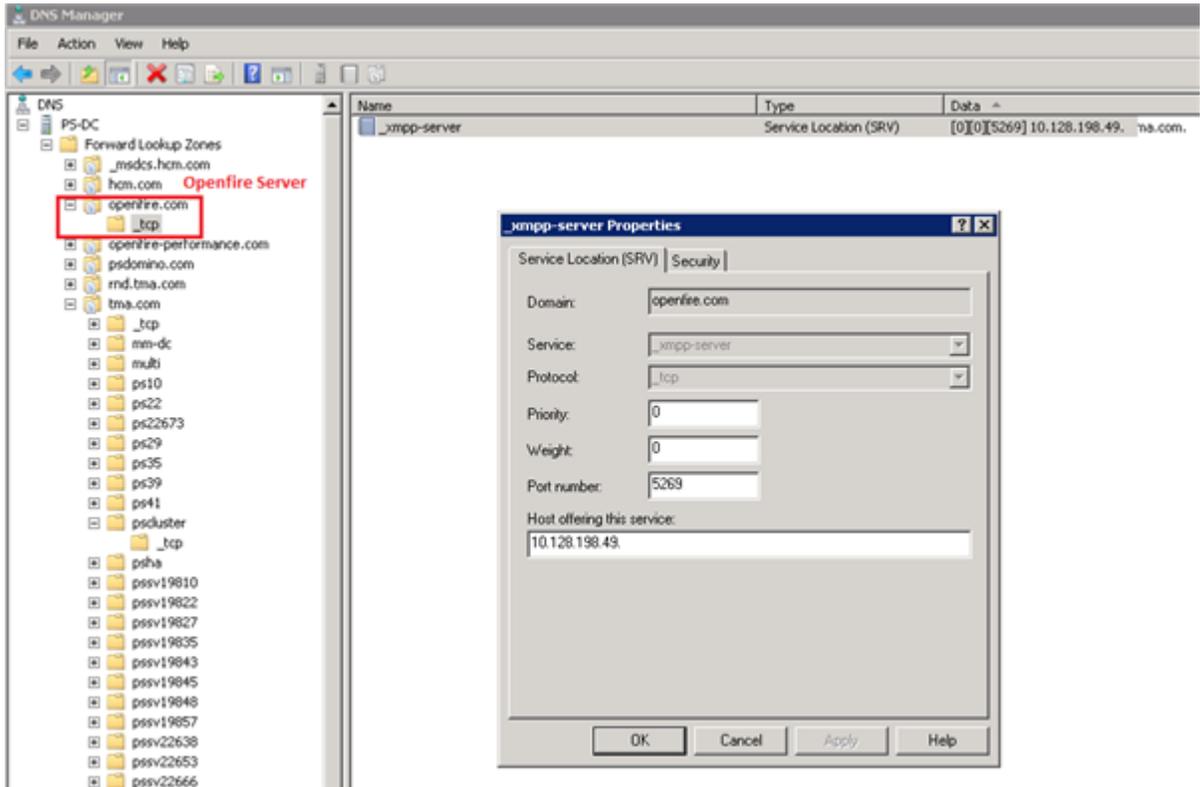
---

## Configuring DNS

### Procedure

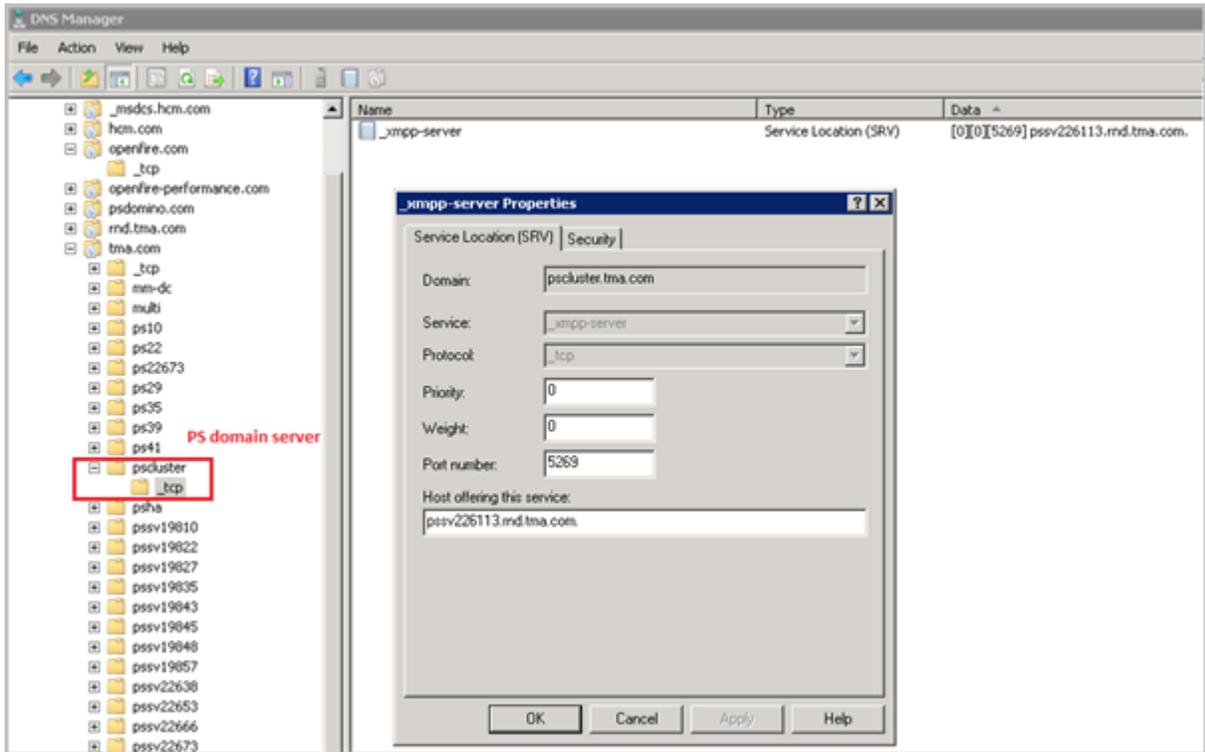
1. Ensure that the Openfire server can resolve the Presence Services domain and the Presence Services server can resolve the Openfire domain.

2. Ensure that the service record matches the following rule defined on the XCP controller:  
**\_xmpp-server.\_tcp**.



3. Configure one of the Presence Services servers in the cluster as the Presence Services gateway.

4. Configure SRV of the Presence Services gateway host with the Presence Services cluster domain.



5. Test the DNS and SRV setup.
6. Run the following commands on the Openfire system:
  - a. `nslookup -querytype=SRV _xmpp-server._tcp.<PS domain>.`
  - b. `nslookup -querytype=A <PS domain>.`
  - c. Ensure that the system returns the correct IP address.
7. Run the following commands on the Presence Services gateway:
  - a. `nslookup -querytype=SRV _xmpp-server._tcp.<Openfire domain>.`
  - b. `nslookup -querytype=A <Openfire domain>.`
  - c. Ensure that the system returns the correct IP address.

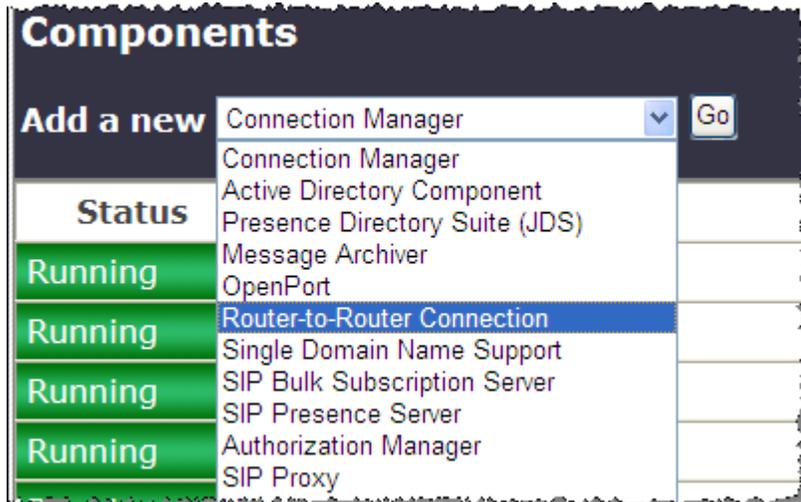
## Adding Router-to-Router connection

### About this task

Perform the following procedure to add a Router-to-Router connection between every member of cluster.

## Procedure

1. Log in to the Presence Services XCP Controller web interface.
2. Select the **Advanced configuration** view.
3. In the **Components** area section, from the **Add a new** drop-down list, select **Router-to-Router Connection**, and click **Go**.



The system displays the Router-to-Router Connection Configuration page.

4. In the **Router-to-Router Connection** section, set the **Runlevel** field to 10.
5. In the **Router Outbound Connection Information** section, perform the following:
  - a. In the **Component IP** field, enter the IP address of the remote peer node.
  - b. In the **Password** field, enter the password.
  - c. Confirm the password.

- d. Ensure that the **Connection weight** field is set to 1.

**Router Outbound Connection Information (i.e., Router connects to another component)**

Component IP: 148.147.1

Port: 7400

Password: .....

Confirm Password: .....

Connection weight: 1

Buffer size in bytes for outgoing data: 65535

Buffer size in bytes for incoming data: 65535

Log the delivery of packets to this component  
(Disable this option for logging components such as the Message Archiver.): Yes

Submit Reset Cancel

6. Click **Submit** to save the changes.

---

## Configuring the federation domain

### About this task

Perform the following procedure to configure the federation domain on every member of cluster.

### Procedure

1. Log in to the XCP controller.
2. On the Presence Services XCP Controller home page, select the **Advanced configuration** view.
3. In the **Router** section, click **Edit** in the **Actions** column next to Global router settings of Core Router.

The system displays the Global Settings Configuration page.

4. Select the **Federation Domains** check box.
5. In the **Federation Domain(s)** field, specify the domains that you want the system to federate with.
6. Click **Submit**.

---

## Adding the S2S component

### About this task

S2S is responsible for handling inter-domain federation.

Perform the following procedure to add an S2S component on a Presence Services instance of the cluster. You must add this component to only one Presence Services instance.

### Procedure

1. Log in to the XCP controller.
2. On the Presence Services XCP Controller home page, select the **Advanced configuration** view.
3. In the **Component** section, in the **Add a new** field, select **Connection Manager**.  
The system displays the Connection Manager Configuration page.
4. In the **Add a New Command Processor** section, in the **Add a new** field, select **S2S command processor**, and click **Go**.  
The system displays the S2S Command Processor Configuration page.  
Note the ID that the system generates for later use.
5. Remove the last two entries in the **Outgoing Connection Attempt Rules** section.  
These entries are unnecessary and add complexity to the logs.
6. Click **Submit**.
7. On the Connection Manager Configuration page, select the **Component Logging (Jlog)** check box.
8. Select the **Logger** check box.
9. Select the **Filtered Syslog Logger** check box.
10. In the **Pipe Level Filter** section:
  - a. Set the value of the **Level** field to **DEBUG**.
  - b. Set the value of the **Pipe file** field to `/opt/Avaya/Presence/jabber/xcp/var/log/of-cm.pipe`
11. Click **Submit**.

---

## Adding the OpenPort component

### About this task

Perform the following procedure to add an OpenPort component on a Presence Services instance of the cluster. You must add this component to only one Presence Services instance.

### Procedure

1. Log in to the XCP controller.
2. In the **Component** section, in the **Add a new** field, select **OpenPort**.
3. Click **Go**.

The system displays the prompts to enter the ID of the component.

4. In the **Enter ID of open-port component** field, enter the ID of the S2S component that you had noted earlier, and click **OK**.

The system displays the OpenPort Configuration page.

5. In the **Configuration view** field select **Advanced**.
6. In the **Hostnames for this Component** section, in the **Host(s)** field, add the Openfire domain.

Ensure that the Presence server can resolve this domain name.

7. Click **Submit**.
8. Restart the system.

---

## OCS Gateway

---

### Introduction

#### Overview - OCS/Lync integration

Avaya Aura® Presence Services is a multiprotocol, multifunctional server providing presence and IM services to Avaya Aura® users. Presence Services collects and distributes the communication status of an Avaya Aura® user from the various communication endpoints connected on an enterprise network. Presence Services provides aggregation and composition services in its Event State Compositor (ESC) to create a composite presence document for an Avaya Aura® user. This composite presence document is available to any authorized subscribing enterprise user. A Presence server aggregates the presence for an Avaya Aura® user and obtains the presence of a user from the following sources:

- PIDF presence published by Avaya Aura® clients using both SIP and XMPP.
- Collected presence from an integrated enterprise system, for example, telephony presence through AES collection.
- Third-party presence integration such as Microsoft OCS/Lync collects presence.

Additionally, Presence Services provides IM capabilities to Avaya Aura® users. This capability is achieved using the XMPP protocol support within an Avaya Aura® client. Thus, all Avaya Aura® clients, which are enabled for IM use XMPP for managing their IM conversations. Avaya Aura® users can engage in IM conversations with each other through their Avaya Aura® clients. After enabling the OCS Gateway the scope of this interaction is extended. Thus, an Avaya Aura® user can engage in an IM conversation with another enterprise user, who is using Microsoft Office Communicator (MOC)/Lync clients for their IM communications. Thus, enabling the OSC Gateway within the installation of Presence Services installation supports:

- Avaya Aura® users, using their Avaya Aura® clients, can IM the other enterprise user colleagues who are using Microsoft Office Communicator (MOC)/Lync clients.

- Enterprise users, using MOC/Lync clients, can initiate an IM conversation with their enterprise colleagues who are using Avaya Aura<sup>®</sup> clients.

Additionally, an Enterprise user can obtain the overall presence availability of their Aura colleagues by adding the presence handle of an Avaya Aura<sup>®</sup> user to their buddy list. The MOC/Lync client displays the presence against the contact address of an Avaya Aura<sup>®</sup> user.

**\* Note:**

You can enable OCS Gateway during the Presence Services installation. But if you decide to enable OCS Gateway after you have installed Presence Services, see *Integrating OCS Gateway*.

The main purpose of integrating an OCS Gateway with Presence Services is to provide an IM interoperability and presence distribution from Presence Services to the OCS/Lync users. In the latter scenario, an Avaya Aura<sup>®</sup> user is added to buddy list of an MOC/Lync user, so that you can obtain an overall availability of an Avaya Aura<sup>®</sup> user. As a result, you have two buddies in your buddy list. This requires that a Presence server is configured as a federated IM provider in the deployment of an OCS/Lync Edge server. This federated interworking model requires the management of trust configuration between the two systems, and the setup of network configuration in the form of DNS records (SRV and Host A records).

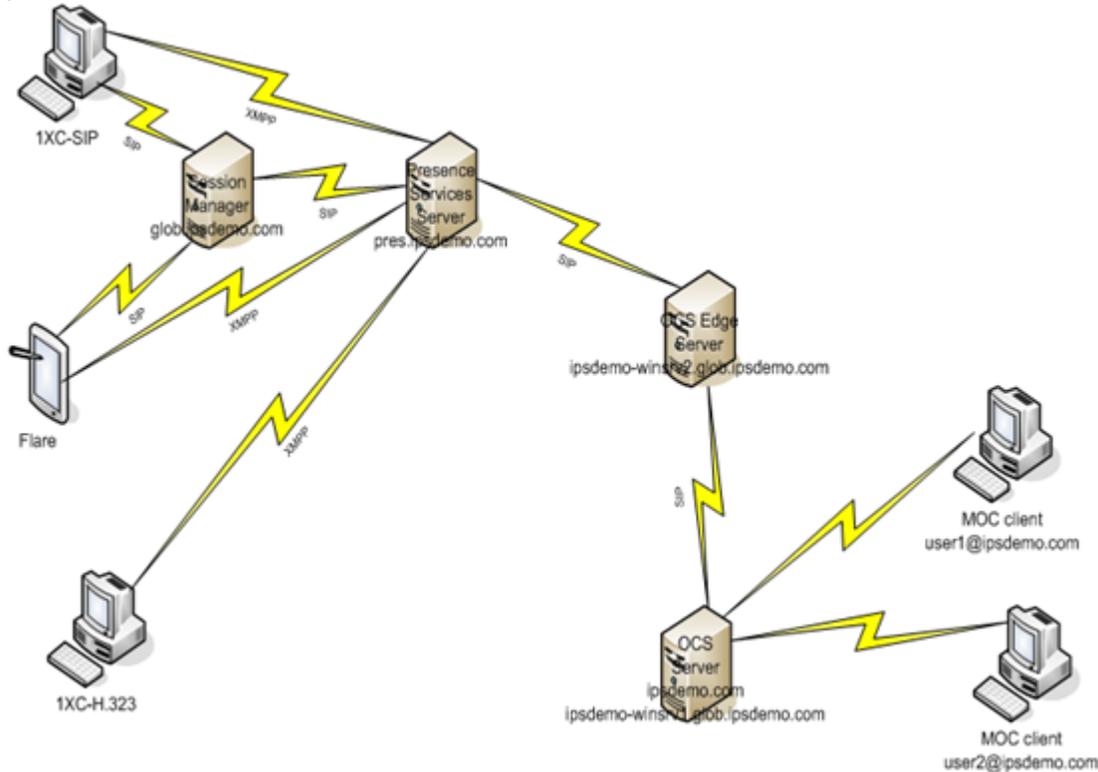
**\* Note:**

Presence Services does not support OCS/Lync federation when Inter-Tenant Communication Control is enabled on System Manager.

When you enable and deploy an OCS Gateway in a Presence Services installation, an enterprise user using an MOC/Lync client can engage in IM conversations with a colleague who is using an Avaya Aura<sup>®</sup> client. Additionally, the enterprise user using the MOC/Lync client can see an overall availability of an Avaya Aura<sup>®</sup> user, by adding the presence handle of an Aura user to their buddy list.

## The Presence server and OCS/Lync integration architecture

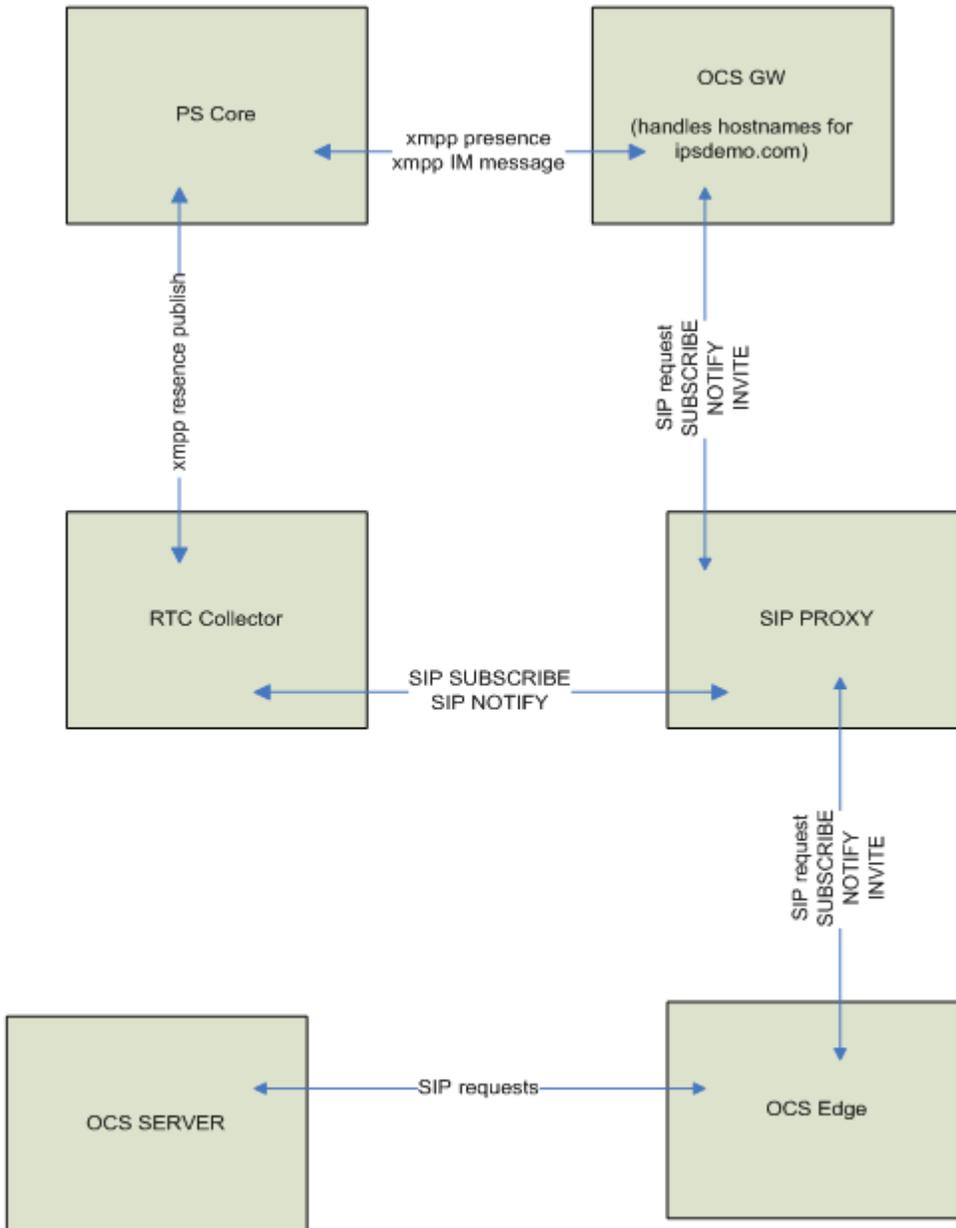
In the deployment of Presence Services, the OCS Gateway integrated with OCS/Lync for the IM and presence information



In the figure that shows a sample deployment, the OCS server resides on the `ipsdemo.com` domain, Presence Services resides on the `pres.ipsdemo.com` domain, while the Avaya Aura® domain resides on `glob.ipsdemo.com`. Therefore, users provisioned in System Manager have Presence Services handles with domain as **pres.ipsdemo.com** and have SIP handles with domain as **glob.ipsdemo.com**. The FQDN for Presence Services is `ipsdemo-ips1.ipsdemo.com`, the external FQDN for the OCS server is `ipsdemo-winsrv1.glob.ipsdemo.com`, and the FQDN for the OCS Edge server is `ipsdemo-winsrv2.glob.ipsdemo.com`. This sample deployment is used as an example in this guide to show the configuration input.

Within the Presence server, a number of server components provide OCS Gateway services.

## Presence Services federation with third-party servers



The figure that illustrates the component view shows the Presence Services OCS Gateway component communicating with an OCS Edge server. The SIP requests from OCS Gateway to the OCS Edge server are routed through the SIP Proxy of Presence Services and then through an OCS Edge server.

The Presence Services integration with OCS/Lync is based on a federated interworking deployment between the two systems. You can administer Presence Services as a federated provider on the OCS/Lync environment that enables the exchange of IM and presence between the two systems. The main components from the Avaya Aura<sup>®</sup> perspective are:

- Avaya Aura<sup>®</sup> clients.
- The OCS Gateway component.

- The SIP Proxy component.

The main components involved from an OCS/Lync perspective are:

- OCS/Lync Edge.
- OCS/Lync server.
- MOC/Lync clients.
- DNS server.
- Active Directory.

---

## Presence Services multi-domain support with Lync federation

The following are the requirements of Presence Services multi-domain support with Lync federation:

- A DNS SRV record is required for the Lync federation for each Presence Services domain.
- The multiple Presence Services domains must have a common prefix or suffix in order to use the domain wildcard on Lync server. For example, the wildcard can be `presence.*` or `*.avaya.com`.

You need to add the domain wildcard in the provider section of SIP Federated Providers. Click the **Federation and External Access – SIP Federated Providers** link on the Lync server control panel to access SIP Federated Providers.

- The Lync configuration change requires some time to take effect. It is recommended to restart both Presence Services and Lync servers, and wait 30 minutes after the configuration change.

### **Note:**

Multiple domains with distinct domain name are not supported with Lync federation.

---

## Integrating OCS Gateway

### Overview - OCS Gateway

The main purpose of integrating an OCS Gateway with Presence Services is to provide an IM interoperability and presence distribution from Presence Services to the OCS/Lync users. In the latter scenario, an Avaya Aura® user is added to buddy list of an MOC/Lync user, so that the MOC/Lync user can obtain an overall availability of an Avaya Aura® user. This requires that a Presence server is configured as a federated IM provider in the deployment of an OCS/Lync Edge server. This federated interworking model requires the management of trust configuration between the two systems, and the setup of network configuration in the form of DNS records (SRV and Host A records).

When you enable and deploy an OCS Gateway in a Presence Services installation, an enterprise user using an MOC/Lync client can engage in IM conversations with a colleague who is using an Avaya Aura® client. Additionally, the enterprise user can also see an overall availability of an Avaya Aura® user, by adding an Aura presence handle to their buddy list.

**\* Note:**

You cannot add an OCS/Lync contact directly to the contact list on an Aura client. In order to subscribe for the presence of an OCS/Lync user you must first add an OCS/Lync contact handle to the communication profile of an Aura user in System Manager. Then you add the Aura user as the contact.

Also, please note that Presence Services does not support ACL=Confirm for Lync.

**Related Links**

[Inbound requests](#) on page 170

[Outbound requests](#) on page 170

**Inbound requests**

The inbound requests originate from the OCS/Lync and route through the OCS/Lync Edge server and the Presence Services SIP Proxy. The Presence Services SIP Proxy is instrumental in directing SIP requests from the OCS/Lync system to the OCS Gateway. You can achieve this through the routing rules defined in SIP Proxy. Inbound SIP requests are subject to routing rules, which are defined on the To and From header fields of a SIP request. The inbound routing rules directs certain SIP requests originating from an OCS/Lync system to the OCS Gateway.

**Related Links**

[Overview - OCS Gateway](#) on page 169

**Outbound requests**

The outbound requests are the SIP requests that the system initiates as a result of Avaya Aura<sup>®</sup> client initiated requests destined for an OCS/Lync enterprise user. These requests are processed by Presence Services and are routed internally through the OCS Gateway. In the current Presence Services implementation, these requests are XMPP requests that originates from an Aura client.

For example, an Avaya Aura<sup>®</sup> enterprise user logged on a 1XC-H.323 or 1XC-SIP client can click on a user in their contact list and initiate an IM with that peer enterprise user. The 1XC clients then indicates that the target user has two IM addresses: an Avaya Aura<sup>®</sup> XMPP handle and an OCS/Lync handle. If the initiating user selects the OCS/Lync handle, then the Avaya Aura<sup>®</sup> client sends an XMPP IM message to Presence Services and then Presence Services routes this IM message internally through the OCS Gateway. This is because the system configures the OCS Gateway to handle communications with the OCS/Lync domain and the address used in the request contains the OCS/Lync domain.

Outbound SIP requests route through a SIP Proxy of Presence Services, then to the OCS/Lync Edge, and then into the OCS/Lync server. The SIP communication is based on a federated deployment of Presence Services with OCS/Lync. The configuration on OCS/Lync Edge is for federated inter-working. Therefore, you must configure Presence Services for federation as an IM provider on the OCS/Lync Edge server.

Additionally, to establish TLS communications and achieve server authentication, it is necessary that the CA TLS/SSL certificate of the Certificate Authority, which signed the TLS/SSL certificates of Presence Services and OCS/Lync Edge, are imported into each of the trust stores on Presence Services and the OCS/Lync Edge respectively. With the appropriate Presence Server Host records

and SRV records configured in the DNS service associated with the OCS/Lync Edge and the OCS/Lync server, you establish this trust relationship.

Use the following domains as an illustration:

- The PS domain is pres.ipsdemo.com
- The OCS/Lync domain is ipsdemo.com
- The PS server FQDN is ipsdemo-ips1.ipsdemo.com
- The OCS/Lync Edge server external FQDN is ipsdemo-winsrv2.glob.ipsdemo.com
- The OCS/Lync server is ipsdemo-winsrv1.glob.ipsdemo.com

If you are enabling the OCS Gateway during installation, then you must know the appropriate values for the following parameters on the Presence server:

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com
- OCS/Lync SIP domain: The OCS/Lync domain, for example, ipsdemo.com
- OCS/Lync SIP Port: 65061

These parameters set up the OCS Gateway configuration together with the default settings for non-solicited parameters. You can also use these parameters to configure the OCS Gateway routing rules in the SIP Proxy.

The SIP Proxy plays an integral part in the processing of a SIP request that the system sends to the OCS/Lync server and in handling the SIP requests received from the OCS/Lync server to Presence Services. You must define routing rules in the SIP Proxy, which routes SIP requests to their appropriate destination servers. Two rules govern the flow of SIP requests to and from OCS/Lync:

- The outbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests from Presence Services to OCS/Lync have a rule which specifies that if the To header is set to the OCS/Lync domain and if the From header is from the Presence Services domain, then you must apply the default SIP routing rule.
- The inbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests have a rule which specifies that if the To header contains the Presence Services domain and the From header contains the OCS/Lync domain, then the request is to be routed to the OCS Gateway.
- The default SIP routing rules determine the destination IPS address of the target domain. This requires the configuring of a Host mapping in the Proxy. This Host mapping maps an OCS/Lync domain to the external FQDN of the OCS/Lync Edge server. The external FQDN of the OCS/Lync edge server must be resolvable and requires an entry in the /etc/hosts file.

## Related Links

[Overview - OCS Gateway](#) on page 169

## OCS Gateway deployment checklist

This checklist outlines the set of tasks that you must execute to deploy an OCS Gateway and provides cross references to sections of this guide, which provide details of the tasks.

Presence Services federation with third-party servers

#	Server	Task	✓
	Presence server	Enable, deploy, and configure OCS Gateway in the Presence server	
	Presence server	Check that the PS SIP Proxy routing rules and Host mapping configuration has been set for integration with OCS/Lync.	
	OCS/Lync CA and OCS/Lync Edge	Generate an SSL certificate for use on the OCS/Lync Edge. This requires server authentication and client authentication properties to be set.	
	OCS/Lync Edge	Download the CA which signed the external certificate of the Edge server.	
	Presence server	Copy the OCS/Lync Edge server CA certificate to Presence server.	
	OCS/Lync Edge and Presence server	Add the CA for the Edge server to the Presence Services to the Presence Services trust store.	
	Presence server	Verify that the downloaded CA certificate exists in the trust store, execute prescert list command.	
	Presence server	Restart Presence Services to pick up the new trust store and configurations.	
	OCS/Lync Active Directory	Enable OCS/Lync users for federated inter-working.	
	OCS/Lync Edge server	Upload the Presence Services CA certificate to the OCS/Lync Edge server and add the Presence Services CA certificate to the trust store of the OCS/Lync Edge server. By default, the Presence Services CA certificate is usually the System Manager CA certificate. Use the Presence Services CA certificate to sign the	

#	Server	Task	✓
		Presence Services TLS certificate.	
	OCS/Lync Edge and Presence server	Verify the configuration status for both Presence Services and OCS/Lync servers, check trust stores, and DNS configuration on OCS/Lync Edge server.	
	OCS/Lync Edge server	Restart external services to apply the changes.	
	System Manager	Add OCS/Lync handles for users on System Manager.	

## OCS Gateway configuration worksheet

The OCS Gateway configuration worksheet identifies the set of configuration parameters that are when you enable an OCS Gateway. It is important that you know the values for the following parameters before starting the configuration process.

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
OCS Domain		
PS SIP Domain <sup>10</sup>		The service router name configured during installation, for example, pres.ipsdemo.com.
Transport		tls
Port <sup>11</sup>		
Expires		86400
Subscription Failure retry		3600
Server Failure retry		3600
PS IP address		
SIP Proxy Port <sup>12</sup>		
PS server FQDN		
SIP SUBSCRIBE Contact Port <sup>13</sup>		
TLS keystore full file path <sup>14</sup>		

<sup>10</sup> The Service Router Name solicited during the installation process is the Presence Services presence domain.

<sup>11</sup> The system provides a default port, 5061. You must change this port to a free port, typically to 65061. The convention for backend SIP servers is to use 5061 with an integer value from the set 1,2,3,4,5,6 prepended to create the port. Note that any value greater than 6 pushes the port value beyond the acceptable range of TCP ports.

<sup>12</sup> The SIP Proxy port is 5061.

<sup>13</sup> The contact port should be that of the SIP Proxy, that is 5061.

<sup>14</sup> Currently, TLS keystore full file path is `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
TLS trust store full file path <sup>15</sup>		

## Enabling OCS Gateway

You can enable an OCS Gateway in the following scenarios:

- During Presence Services installation
- After Presence Services installation

### Related Links

[Enabling OCS Gateway during installation](#) on page 174

[Enabling OCS Gateway post installation](#) on page 174

### Enabling OCS Gateway during installation

When you select and enable an OCS Gateway at the time of installation, as a part of the installation process, the system requests the following configuration parameters:

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com.
- OCS/Lync SIP Domain: The OCS/Lync domain.
- OCS/Lync SIP Port: The TLS port used by the SIP stack.

The system presents a default 65061 port number for the OCS/Lync SIP port. You can accept this value almost invariably. The installer enables the OCS Gateway and sets up its configuration. Additionally, the system configures SIP Proxy with routing route and host mappings for interacting with OCS/Lync.

### Related Links

[Enabling OCS Gateway](#) on page 174

### Enabling OCS Gateway post installation

#### About this task

The OCS Gateway provides IM and presence interoperability between a Presence Services installation and an OCS/Lync installation. You can achieve this by setting up a federated deployment between OCS/Lync and Presence Services. For this interoperability between the two systems, you must configure Presence Services as an IM provider on the OCS/Lync Edge server on OCS/Lync, and also ensure that the relevant DNS network configuration and trust management is in place.

You can enable an OCS Gateway post installation through the XCP Controller Web interface.

#### Procedure

1. Log in to the Presence Services XCP Controller Web interface.

<sup>15</sup> Currently, TLS trust store full file path is `/opt/Avaya/Presnce/jabber/xcp/certs/generic.trusts`

- In the **Components** area, select **Connection Manager** from the **Add a new** drop-down list, and click **Go**. The system displays the Connection Manager Configuration page. By default, the system displays a basic configuration view, but you must switch to the advanced configuration view.

**+ Tip:**

- On the Connection Manager Configuration page, under the Connection Manager section, you can rename the **Description** field to `OCS Connection Manager` for more clarity.
- Under the Command line to run section, change the text in the **Command line to run** text box to, `exec /opt/Avaya/Presence/jabber/xcp/bin/sip_gw -h %i -m %m -n %n -p %p -P /opt/Avaya/Presence/jabber/xcp/var/run/jabberd/%n.pid`. The OCS Gateway does not start, unless you make these changes.
  - From the **Add a New Command Processor** drop-down box, select **S2S Command Processor**.
  - Click **GO**. The system displays the S2S Command Processor Configuration page. The initial configuration settings on this page are the default settings for an XMPP S2S Gateway. You must remove parts of the default configuration and replace with SIP/Simple Gateway configuration.
  - In the Director Configuration section, the system presents two default XMPP directors. Click **Remove** next to each default XMPP directors.
  - To confirm the removal of the XMPP directors, on the **Click 'OK' to confirm removal from the configuration** dialog box, click **OK** for each of the XMPP directors.
  - On the S2S Command Processor Configuration page, under the Director Configuration section, from the **Add a new** drop-down box, select **SIP/SIMPLE Gateway** and then click **Go**.

The system displays the SIP/Simple Gateway Configuration page. The system requires a number of configuration parameters for the SIP/Simple Gateway, which includes Remote Host Configuration, SIP Stack Configuration, and Outbound Proxy configuration.

### Next steps

Configure OCS Gateway.

### Related Links

[Enabling OCS Gateway](#) on page 174

## Configuring OCS Gateway

### Overview - Configuring OCS

The SIP/Simple gateway requires the configuration setting of a number of parameters under various categories, which includes SIP Host Configuration and SIP Stack Configuration. To add a SIP Host configuration, perform the following:

- Configure a SIP TLS transport under the SIP Stack Configuration category

- Set the Outbound Proxy
- Modify a number of SIP request timeout parameters

## Configuring the SIP Remote Host Configuration parameters

### Procedure

1. In the SIP/Simple Gateway Configuration page, scroll to the Remote Host Configuration section and select **Local Configuration**.
2. Click **GO** to add a new SIP Host. The system displays the SIP Host Configuration page. This configuration defines a mapping between the OCS/Lync domain and the OCS/Lync Edge server. For the mapping, you need the following three parameters:
  - Remote server hostname
  - Server Type
  - Hostname mapping
3. In the **Remote server hostname** field, enter the external FQDN of the OCS/Lync Edge server.
4. From the **Server Type** drop-down box, select **ocs**.
5. On the Hostname Mappings section, in the **Hostname(s)** field, enter the OCS/Lync domain. For example, ipsdemo.com.
6. To save the configuration, click **Submit**. The system returns to the SIP/Simple Gateway Configuration page.

## Configuring the SIP Stack Configuration parameters for the OCS Gateway

### Procedure

1. In the SIP Stack Configuration Parameters section, create and configure TLS transport.
2. From the **Add a new SIP Transport** drop-down box, select **TLS** and click **GO**.

The system displays the TLS transport Configuration page. This page provides network and TLS configuration parameters for the selected TLS transport.

 **Note:**

Ensure that the domain that you use for TLS certificate is the FQDN of Presence Services. The full path to the certificate file must be `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber` and the full path to the CA certificate file should be `/opt/Avaya/Presence/jabber/xcp/certs/generic.trusts`.

3. Accept the default values for the following configuration parameters:
  - **Unique identifier for this transport**
  - **Hostname of external interface**
  - **IP address**

**\* Note:**

The hostname for external interface is the PS domain name.

4. In the **Port** field, change the value of the port from 5061 to 65061.  
This is the port configured for the OCS Gateway.
5. In the **Use this transport by default for TLS requests** field, use the default value **Yes**.
6. In the **Domain used for TLS certificate** field, enter the FQDN of Presence Services.
7. Use the following values:
  - The Full path to the certificate file: `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`
  - Full path to the CA certificate: `/opt/Avaya/Presence/jabber/xcp/certs/generic.trusts`
8. In the Define an optional external contact for SIP servers to use to contact this transport section, enter the following two configuration parameters:
  - **External hostname that SIP servers will use to contact:** Enter the FQDN of Presence Services.
  - **External port that SIP servers will use for contact:** Enter the SIP Proxy port 5061.

**\* Note:**

Use these parameters are to set the Contact header of the outbound SIP requests.

9. To save the configuration settings click **Submit** .  
The system displays the SIP/Simple Gateway page again.
10. Configure Outbound Proxy. This forces outbound SIP requests through a next hop processing node. In this case, the next hop processing node is the Presence Services SIP Proxy, where you need to apply the outbound OCS/Lync routing rules.
11. Select the **Outbound Proxy** check box and enter the following parameters:
  - **Proxy IP address:** Presence Services IP address.
  - **Proxy Port:** 5061.
  - **Proxy Transport:** TLS
12. In the list of configuration parameters, set **Send/Receive Buffer Size (bytes)** to 8192 and set the **TLS connection strict checking of hostname and TLS connection strict certificate usage** parameters value to `NO`. Use the default values for the remaining parameters.  
  
The SIP/Simple Gateway Configuration provides parameters that define how TLS certificates are handled, for example, whether strict host name checking is applied or not.
13. To save the SIP/Simple Gateway Configuration, click **Submit** .  
The system displays the S2S Command Processor Configuration page. On the S2S Command Processor Configuration page, the system displays an entry for

`cm-2_s2scp-1_sip_sd-1.presence` SIP/Simple Gateway component in the director configuration table.

14. On the S2S Command Processor Configuration page, on the Outgoing Connection Attempt Rules page, the system displays three rules. These rules are applicable to the XMPP S2S directors and are not relevant for the OCS Gateway configuration. Therefore, you must remove the rules.
15. In the table, for each of the existing rules, click **Remove** next to each rule to delete the rule.
16. Create a new dummy rule, Outgoing Connection Attempt Rule. These dummy rules are a form of local SRV DNS lookup and are associated with built-in default rules within OCS Gateway.
17. Prior to creating the dummy rule, take note of the SIP/Simple Gateway identifier. Typically, this is `cm-2_s2scp-1_sip_sd-1`, and you can obtain the value from the director table at the top of this configuration page.
18. To create a dummy rule, click **GO**.  
The system displays the Rule Configuration page.
19. For example, enter the following:
  - **Director ID:** `cm-2_s2scp-1_sip_sd-1`. This is the SIP/Simple Gateway component identifier.
  - **DNS SRV lookup to use:** `abcdef`.
  - **Port to use instead of DNS SRV lookup:** Leave this field blank.
20. To save this rule configuration, click **Submit**.  
The system returns to the S2S Command Processor Configuration page.
21. On the S2S Command Processor Configuration page, click **Submit** to save all configuration inputs.  
The system displays the Connection Manager Configuration page.
22. On the Connection Manager Configuration page, the system displays a command process `cm-2_s2scp-1.presence` in the command processor table. As a final part of the configuration, enable logging.
23. To enable logging, scroll to Component Logging, and select the **Component Logging** check box.
24. Select the **Logger** check box and then select the **Filtered Syslog Logger** check box.
25. Under the Pipe Level Filter section, accept the default Level at WARNING, and in the **Pipe file** text box, enter the path `/opt/Avaya/Presence/jabber/xcp/var/log/ocs-cm.pipe`.  
This file is used to dynamically adjust the logging level of the OCS Gateway through the `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh` script.
26. Under the File Settings section, in the **Name and location** field, enter the name and location, for example, `/var/log/presence/ocsgateway.log`.

27. Under the Syslog Settings section, in the **Identity** text box, enter `OCS-CM`.
28. Click **Submit**. The system creates a Connection Manager component containing the OCS Gateway.

The system now displays the XCP Controller main page. The system adds an additional connection manager component to the component list.

### Next steps

To complete the OCS Gateway setup and integration with OCS/Lync, it is necessary to complete the trust management and DNS administration procedures. For more information, see the *Trust management and DNS Administration* section.

## Configuring the OCS Gateway Hostname Filter: Open Port component configuration

### About this task

You must configure the OCS Gateway in such a way that any presence packets or IM messages destined for the OCS/Lync domain can be routed internally within the Presence Services through the OCS Gateway. For this, you must create an Open Port component that specifies that the OCS Gateway handles packets and message requests destined for the OCS/Lync domain.

### Procedure

1. Log in to the XCP Controller Web interface.
2. On the XCP Controller Configuration page, from the **Component** drop-down box, select **Open Port**.
3. Click **GO**. The system displays a pop-up menu, where the system asks you to enter the user input for the name of a component associated with the Open Port component that you want to create.
4. In the enter ID of open port component field, enter the name of the S2SCP which was created while enabling the OCS Gateway. For example, if the name of the Connection Manager was `cm-2` and the S2SCP is `cm-2_s2scp-1`, then enter `cm-2_s2scp-1` as the component ID for the Open Port component.

#### **Note:**

Ensure that you use the same S2SCP component name, created during the configuration for the OCS Gateway, for the Open Port component name. Also, you must not include “.presence” in the Open port component name.

5. Click **OK**. The system displays the OpenPort Configuration page.
6. On the Hostname for this Component section, in the **Host Filter Host(s)** field, enter the OCS/Lync domain, for example, `ipsdemo.com`.
7. To save the configuration, click **Submit**. This configuration is the only configuration required for the Open Port.

The main objective of OpenPort configuration is to associate the OCS/Lync domain with the OCS Gateway. This allows any presence packets or IM messages to route internally within

Presence Services to the OCS Gateway. The OCS Gateway then converts any presence packets or IM messages to SIP requests. The OCS Gateway then sends these SIP requests to the OCS/Lync server through the SIP Proxy and OCS/Lync Edge server.

## Configuring SIP Proxy routing rules for OCS Gateway

You must add the SIP Proxy routing rules manually only after enabling the OCS SIP Gateway. Configure the following rules:

- Outbound SIP requests to OCS
- Inbound SIP requests from OCS

### \* Note:

The addition of routing rules is linear, that is, a new rule is added directly after the last rule is defined. You must take note of the last rule currently defined, which should be a default routing rule or catch all, which routes all remaining SIP requests, not covered by the preceding rules, to the SIP Presence server or SIP PS component. Once you record this rule, remove this rule.

If there is a rule defined to route the SIP method "NOTIFY" to the default SIP routing (for example, the second last rule), then you have to take note to record the rule as well. Otherwise you do not need to record it. Once record the rule for the "NOTIFY" method, remove the rule as well. You will have to restore it later.

Add the two new routing rules for the OCS Gateway, and then add the recorded routing rules.

### Before you begin

Check that the following configuration parameters are set to the values indicated:

- The Add Record-Route header field is set to `No`.
- The Enable LCS Routing compatibility field is set to `Yes`.

### \* Note:

To check the Add Record-Route header field and Enable LCS Routing compatibility field, see the SIP Proxy settings.

### Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP proxy component.
3. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section. Review the last routing rule by clicking details of the last routing rule table entry, and record the details of this rule. The system displays the Routing Rule Configuration page. This rule specifies the default or catch all rule routing SIP requests to the SIP Presence server component. If not, then there is a potential error in your proxy configuration. The default routing rule reads as follows: In the Destination Routes section, a use a specific destination for this rule configuration will be set with a routing tag sip-ps-1. If the system deploys more than one SIP Presence server component, then each of these SIP Presence Services is also listed.

4. Click **Cancel** and **OK** to return to the main configuration page for the SIP Proxy.
5. To remove the last routing rule, click **Remove**.

## OCS Gateway routing rule

The rules to govern the outbound SIP requests (SUBSCRIBE, INVITE, ACK, NOTIFY) and the inbound SIP requests (SUBSCRIBE, INVITE, ACK, NOTIFY) are based on the domains in the To and From headers. The outbound SIP requests are destined to a user at the OCS domain and come from a user in the Presence Services domain. For the inbound requests, the system originates these requests from a user in the OCS domain and routes to a user in the Presence Services domain.

### Related Links

- [Inbound SIP requests routing rule](#) on page 181
- [Outbound SIP requests routing rule](#) on page 182
- [Adding a new Remote Host](#) on page 182
- [Adding a new routing label for the OCS Gateway](#) on page 183

## Inbound SIP requests routing rule

### About this task

The inbound SIP requests rule is based on the To and From header field. The From header rule pattern specifies the domain as the OCS/Lync domain, for example, ipsdemo.com. The To header rule pattern specifies the Presence Services domain, for example, pres.ipsdemo.com.

### Procedure

1. On the SIP Proxy Configuration page, scroll down to the SIP Proxy Routing Rules section. Click **GO** to add a new SIP PROXY Routing Rule. The system displays a SIP Proxy Routing Rule Configuration page.
2. Select the **From Hosts** check box.
3. Enter the OCS/Lync domain, for example, ipsdemo.com.
4. On the SIP Proxy Routing Rule Configuration page, select **Use a specific destination for this rule**.
5. Enter the following:
  - rule-destination: ocs-gw

#### **Note:**

The ocs-gw is a routing tag. Define this tag in the TLS transport configuration under the SIP Stack Configuration Parameters on the main SIP Proxy configuration page. Additionally, if you enable the OCS Gateway during installation, then the system selects the routing tag as cm2-s2scp-1. This label serves the same purpose as the ocs-gw label. The ocs-gw label is an internal routing label which identifies the network configuration parameters used by the OCS Gateway process, that is, the OCS Gateway IP address and port.

- Select destination based on to or from user: to

6. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

## Related Links

[OCS Gateway routing rule](#) on page 181

## Outbound SIP requests routing rule

### About this task

The outbound SIP requests rule is based on the **To** and **From** header field. The From header rule pattern specifies the domain as the Presence Services domain, for example, pres.ipsdemo.com. The To header rule pattern specifies the OCS/Lync domain, for example, ipsdemo.com.

### Procedure

1. On the SIP Proxy Routing Rule Configuration page, select the **To Hosts** check box.
2. Enter the OCS/Lync domain, for example, `ipsdemo.com`.
3. In the Destination Routes section, select **use sip default routing rules**.
4. On the SIP Proxy Routing Rule Configuration page, click **Submit** to save the changes.

### Next steps

You must recreate the routing rules that you removed in the previous sections. If you have recorded the routing rule for the SIP method NOTIFY in the previous section, then you have to restore the rule first by adding a new SIP proxy routing rule with the recorded value. In all cases, you have to recreate the default routing rule. For example, perform the following:

1. On the SIP Proxy Configuration page, under the SIP Proxy Configuration section, click **Go** next to **Add a new SIP Proxy Routing Rule**.
2. On the SIP Proxy Routing Rule Configuration page, under the Destination Routes section, select **Use a specific destination for this rule**.
3. In the **IDs of Specific Destinations** text box, enter the same default value removed in the previous sections. By default, it is `sip-ps-1`.
4. From the Choose destination based on to or from user drop-down box, select the same default value removed in the previous sections. By default, the value is **to**.
5. To save the routing rule, click **Submit**.

### \* Note:

If a Presence Services installation enables multiple sip Presence Services components, then the original default routing rule will have multiple sip Presence Services entries. Therefore, in recreating the default routing rule, enter the sip PS component id for each sip PS into the **IDs of Specific Destinations** text box.

## Related Links

[OCS Gateway routing rule](#) on page 181

## Adding a new Remote Host

### Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.

2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.  
The system displays the SIP Proxy Configuration page.
3. Under the Remote Host Configuration section, select **Local Configuration** and then click **Go** next to **Add a new SIP Host**.  
The system displays the SIP Host Configuration page.
4. Under SIP Host, in the **Remote server hostname** text box, enter the external FQDN of the OCS/Lync Edge server. For example, `edger2svext.eu.ocs2adsv.com`.
5. From the **Server Type** drop-down box, select **ocs**.
6. In the **Hostname Mapping** text box, enter the OCS/Lync domain name. For example, `ocsr2adsv.com`.
7. To save the changes, click **Submit**.  
The system take you to the SIP Proxy Configuration page. On the Remote Host Configuration section, under Local Configuration, the system displays the SIP Host entry that you recently created.

#### Related Links

[OCS Gateway routing rule](#) on page 181

#### Adding a new routing label for the OCS Gateway Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the Actions column next to the SIP Proxy component.  
The system displays the SIP Proxy Configuration page.
3. Under the SIP Stack Configuration Parameters section, click **Details** next to the already added TLS transport.  
The system displays the TLS transport Configuration page.
4. Under the Routes for this Transport section, click **Go**.  
The system displays the Route Configuration page.
5. Enter the details for the following fields:
  - ID, enter the ID. For example, `ocs-gw`.
  - IP address, enter the IP address. For example, `135.60.22.51`.
  - Port, enter the port, `65061`.
6. To save the changes, click **Submit**.

**\* Note:**

The OCS Gateway routing label that you just added here must correspond with inbound routing rule for SIP Proxy, as specified perviously.

The system takes you to the TLS transport Configuration page.

7. On the TLS transport Configuration page, under Routes for this Transport, ensure that the new routes are present.
8. To save all the newly added SIP Proxy configuration, click **Submit**.

### Next steps

Enable trust management and DNS administration to setup a trust relationship between Presence Services and the OCS Gateway. For more information on trust management and DNS administration, see the *Trust Management and DNS Administration* chapter.

### Related Links

[OCS Gateway routing rule](#) on page 181

---

## Trust Management and DNS Administration

### Overview - Presence Services and OCS Gateway connection

By default, the Edge server external interface uses a server certificate. To enable communication with the OCS Gateway, you must generate a server SSL certificate to act as both the Client certificate and the Server certificate. To verify the certificate in use by the OCS/Lync Edge server external interface, use the OCS/Lync Edge server properties. For more information on verification, see the *OCS 2007 R2 Edge Server Deployment Guide* at: <http://www.microsoft.com/download/en/details.aspx?id=24402>.

To verify the certificate in use by the Lync Edge server external interface, use the Lync Edge server properties. For more information on verification, see the *Microsoft Lync Server 2010 Edge server Guide* at: <http://www.microsoft.com/en-us/download/details.aspx?id=11379>.

### Checking the certificate used by external interface on server

#### About this task

By default, the Edge server external interface uses a server certificate. To enable communication with the OCS Gateway, you must configure this server certificate to act as both a Client certificate and Server certificate.

#### Procedure

To verify the certificate in use by the Edge server external interface, use the Edge server properties. For more information on verification, refer the *OCS 2007 R2 Edge Server Deployment Guide* at: <http://www.microsoft.com/download/en/details.aspx?id=24402>.

## Generating and importing certificate for OCS

### Generating a certificate with server and client authentication

#### About this task

The certificate that the Edge server external interface uses must have server and client authentication. If not, generate a certificate with server and client authentication and assign the certificate to the Edge server external interface.

To create a certificate for external interface using Microsoft Certificate Authority (CA) in a Windows 2003 Enterprise Edition Server running a standalone Microsoft Enterprise CA:

#### \* **Note:**

The procedure may vary depending on the configuration and setup of your Microsoft CA.

#### Procedure

1. Log on to the Web enrollment page of Certificate Authority at: `http://<CA_Machine>/certsrv/`.
2. On the Web enrollment page, click **Certificate > Advanced Certificate Request**.
3. On the **Advanced Certificate Request** dialog box, enter the following details:
  - a. Select **Other** from the drop-down menu.
  - b. In the **OID** text field, enter `1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2`.  
Separate the two OIDs by a comma but do not add a space.
  - c. Click the **Store certificate in the local computer certificate store** check box.  
Leave all other details as is.
  - d. Click **Submit**.
4. On the Certificate server perform the following:
  - a. To open the mmc of the CertificateAuthority, type `mmc` in the **Run** dialog box, and click **Ok**.
  - b. Right-click **Pending Requests**.  
The system displays the certificate request from the Edge server.
  - c. Right-click on the certificate request based on request ID, and click **All Tasks > Issues**.
5. On the client computer, perform the following:
  - a. To open the Web enrollment page, click **Certificate > Advanced Certificate Request**.
  - b. Click **View the status of a pending certificate request**.
  - c. Click the certificate and save the certificate to use as the Certificate for the External Interface on the Edge server.

## Importing the System Manager default CA certificate into the OCS Edge Trust Store Procedure

1. Log in to System Manager Web Console.
2. Click **Security > Certificates > Authority**.
3. Click **Download pem file**. Save the pem file with an appropriate name, for example, `default-cacert.pem` and upload to the OCS Edge server.
4. Copy the System Manager CA certificate to the OCS Edge server.
5. On the OCS Edge, run the management console, click **Start > Run**.
6. In the **Run** dialog box, enter `mmc` , and click **OK**.
7. On **MMC Console**, select **File > Add/Remove Snap-in** to launch the Add/Remove Snap-in wizard.
8. In the **Add/Remove Snap-in** dialog box, click **Add**.
9. On the **Standalone** tab, click **Add**.
10. In the **Add Standalone Snap-in** dialog box, select **Certificates** and then click **Add**.
11. In the **Certificates Snap-in** dialog box, select **Computer Account** and click **Next**.
12. In the **Select Computer** dialog box, select the default setting **Local Computer** and click **Finish**.
13. In the **Add Standalone Snap-in** dialog box, click **Close**. And then in the **Add/Remove Snap-in** dialog box, click **OK**.

The system takes you to the MMC Console.

14. Click **Console Root**, select **Certificates > Trusted Root Certification Authorities**.
15. Select **Trusted Root Certification Authorities**, right-click **Certificates** and select **All Tasks > Import**.

The system launches the Certificate Import Wizard. Follow the steps of the wizard and browse for the `default-cacert.pem` file.

16. On the Certificate Import Wizard screen, click **Next**.
17. In the **Open** dialog box, click **Browse** to locate the file and then click **Next**.
18. Retain the default settings and then click **Next**.
19. Click **Finish** to complete the Certificates Import Wizard.
20. Verify the Certificate is in the `Certificates/Trusted Root Certification Authorities/ Certificates` list.
  - a. Right-click **Certificates** and select **Refresh** to update the certificates list.

The system might display the certificate as the default setting.

- b. Verify that the serial number and the expiry date of the System Manager certificate match the serial number and the expiratory date of the new default certificate that appears in the certificate list on the Edge server.
- c. To determine the serial number and expiry date of the System Manager certificate, enter the following command on the Presence server: `openssl x509 -in $PRES_HOME/jabber/xcp/certs/default-cacert.pem -noout -text`.  
The details of this certificate must match the default certificate added to Edge server.
- d. To determine if the certificate was added, double-click the certificate in the list of certificates.

If the system does not display a default certificate, then the Presence Services CA Certificate has not been added to the OCS Edge server's Trusted Root Certificates.

**\* Note:**

The default-cacert.pem is the name given to the System Manager CA certificate when the system downloads the from the System Manager security management page.

## Generating and importing certificate for Lync

### Generating a Web server certificate with server and client authentication

#### About this task

The certificate that the Edge server external interface uses must have server and client authentication. If not, generate a certificate with server and client authentication and assign the certificate to the Edge server external interface.

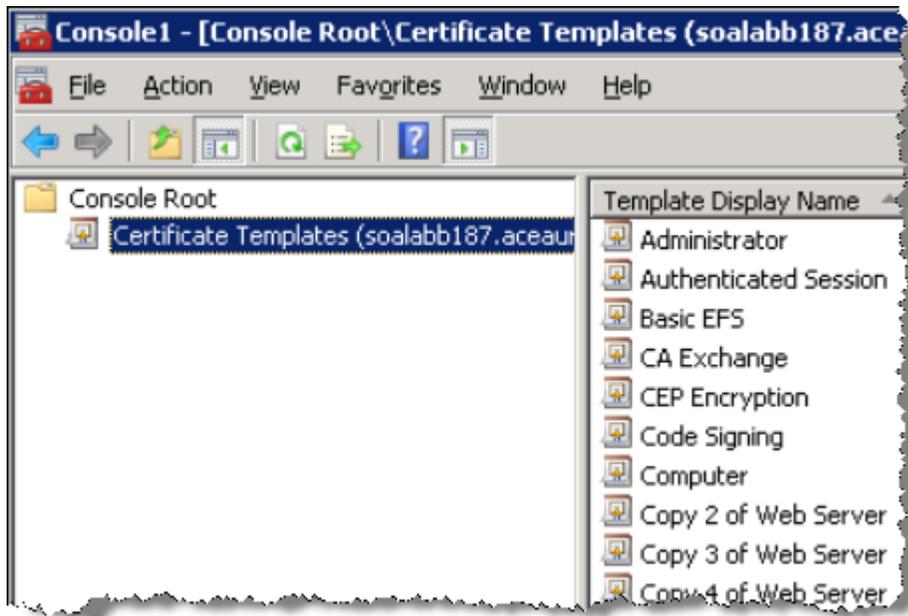
To create a certificate for external interface using Microsoft Certificate Authority (CA) in a Windows 2008 Enterprise Edition Server running a standalone Microsoft Enterprise CA:

**\* Note:**

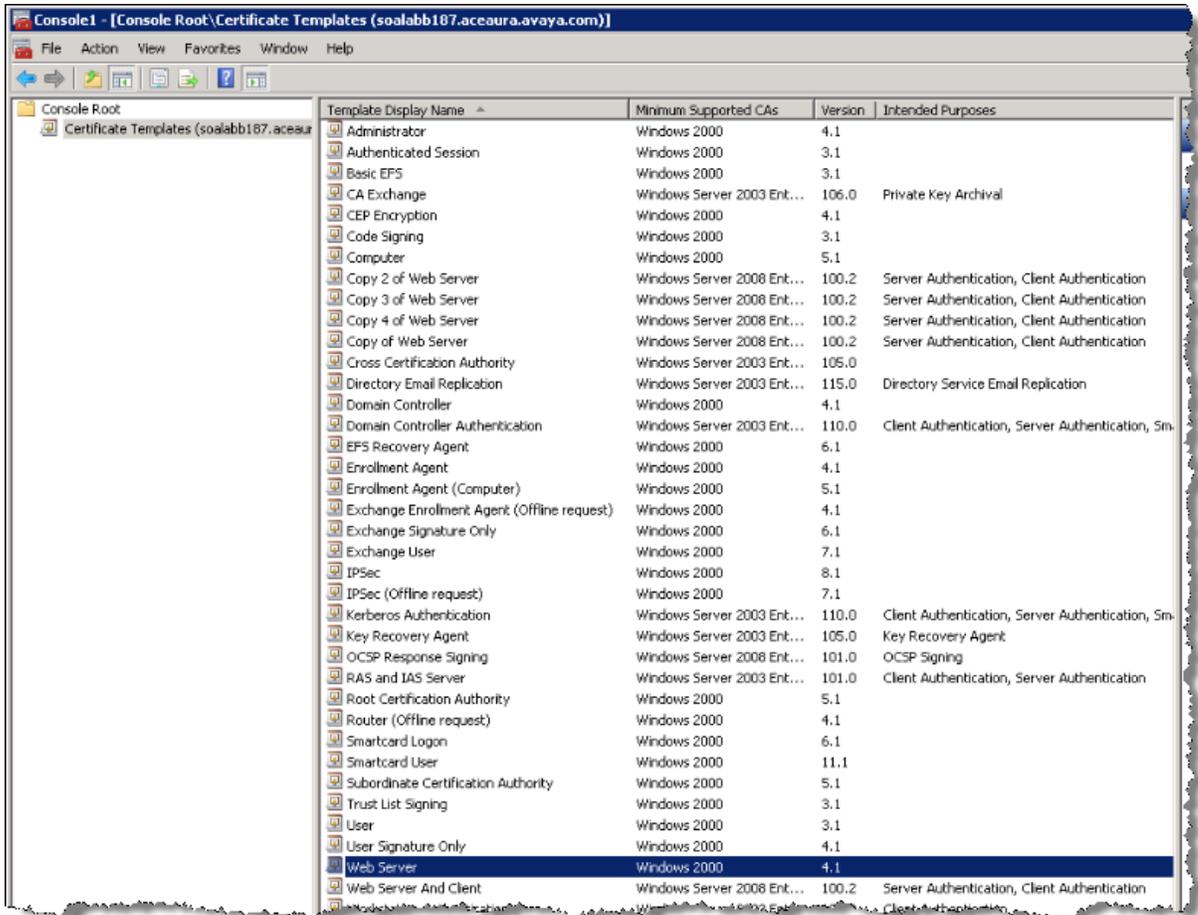
The procedure may vary depending on the configuration and setup of your Microsoft CA.

## Procedure

1. Expand **Console Root** and click **Certificate Templates**. The system displays a list of template display names.



2. From the Template Display Name list, right-click **Web Server** and then click **Duplicate Template**.



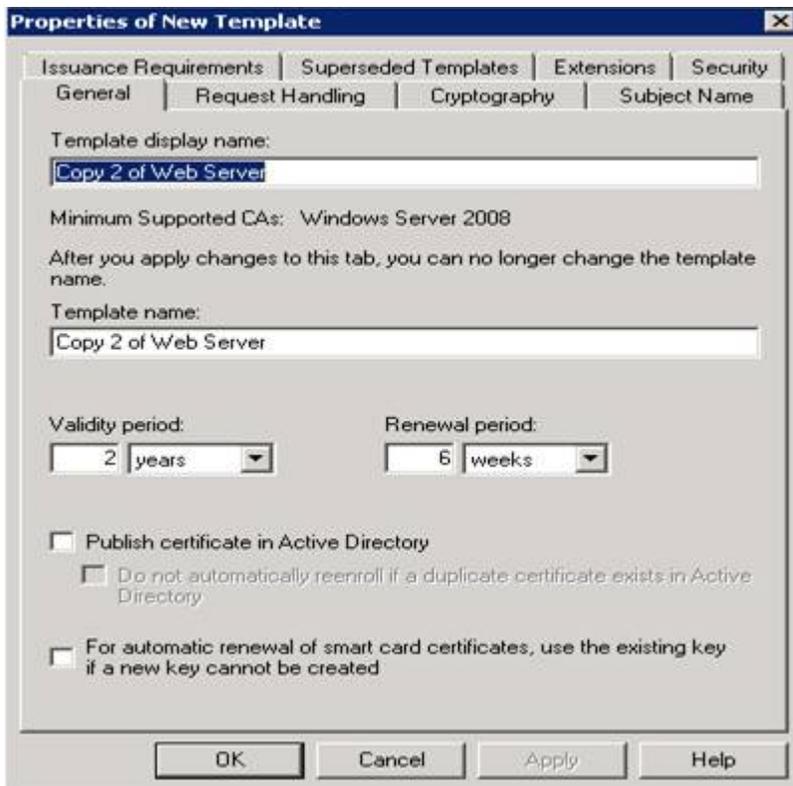
The system displays the Duplicate Template dialog box.

- On the Duplicate Template dialog box, select the **Windows Server 2008, Enterprise Edition** option.



The system displays the Properties of New Template dialog box.

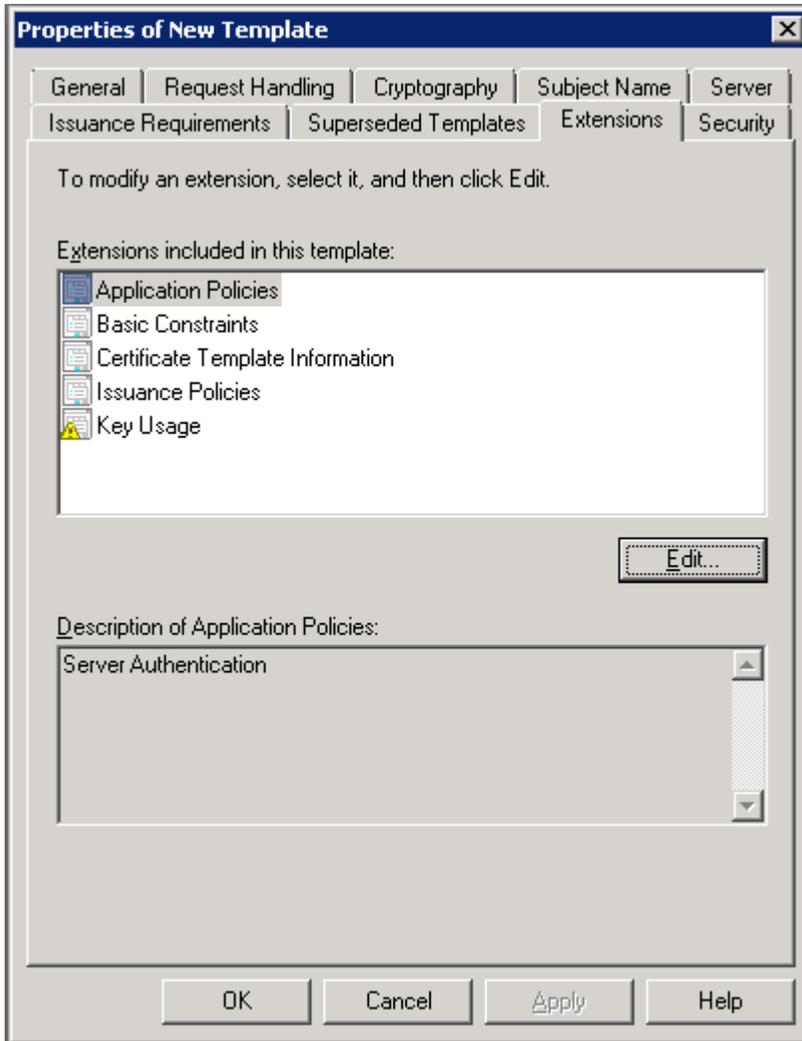
- In the Properties of New Template dialog box, on the **General** tab, in the **Template display name** and **Template name** field, enter a display name for the template.



**\* Note:**

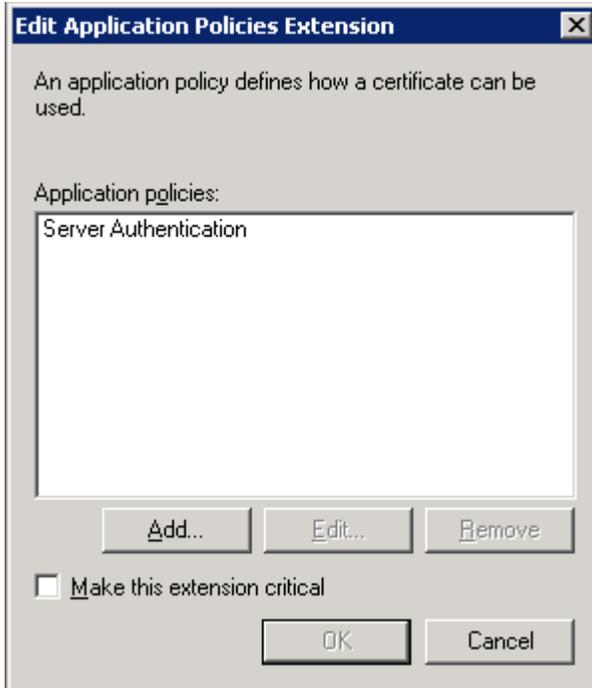
You must use the default entry for the Template name field.

5. On the **Extensions** tab, under the **Extensions included in this template** list, select **Application Policies**, and then click **Edit**.



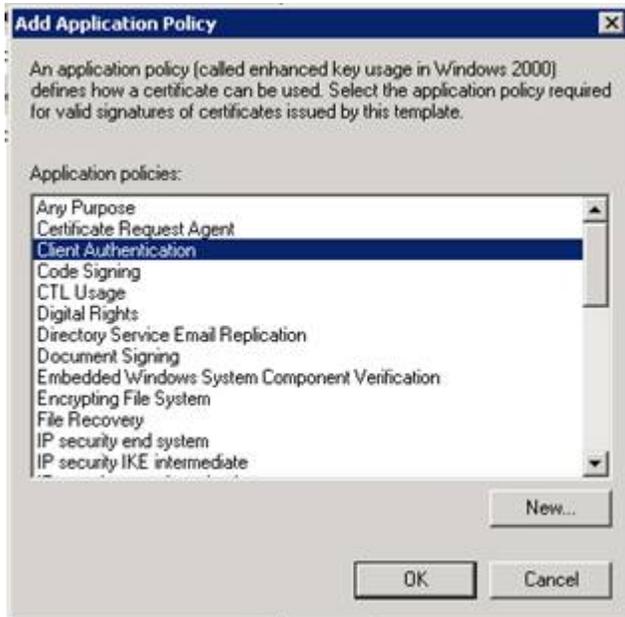
The system displays the Edit Application Policies Extension dialog box.

6. On the Edit Application Policies Extension dialog box, click **Add**.



The system displays the Add Application Policy dialog box.

7. On the Add Application Policy dialog box, from the Application policies list, select **Client Authentication**, and then click **OK**.



8. Click **Apply**, and then click **OK**.

### Next steps

1. Verify the newly added duplicate Web server certificate in the Certificate Templates list.

Template Display Name	Minimum Supported OSs	Version	Intended Purposes
Administrator	Windows 2000	4.1	
Authenticated Session	Windows 2000	3.1	
Basic EFS	Windows 2000	3.1	
CA Exchange	Windows Server 2003, En...	106.0	Private Key Archival
CEP Encryption	Windows 2000	4.1	
Code Signing	Windows 2000	3.1	
Computer	Windows 2000	5.1	
<b>Copy of Web Server</b>	Windows Server 2000	<b>100.3</b>	<b>Client Authentication, Server Authentication</b>
Cross Certification Authority	Windows Server 2003, En...	105.0	
Directory Email Replication	Windows Server 2003, En...	115.0	Directory Service Email Replication
Domain Controller	Windows 2000	4.1	
Domain Controller Authentication	Windows Server 2003, En...	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	Windows 2000	6.1	
Enrollment Agent	Windows 2000	4.1	
Enrollment Agent (Computer)	Windows 2000	5.1	
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	
Exchange Signature Only	Windows 2000	6.1	
Exchange User	Windows 2000	7.1	
IPSec	Windows 2000	8.1	
IPSec (Offline request)	Windows 2000	7.1	
Kerberos Authentication	Windows Server 2003, En...	110.0	Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication
Key Recovery Agent	Windows Server 2003, En...	105.0	Key Recovery Agent
OCSIP Response Signing	Windows Server 2000	101.0	OCSIP Signing
RAS and IAS Server	Windows Server 2003, En...	101.0	Client Authentication, Server Authentication

## Importing the System Manager default CA certificate into the Lync Edge Trust Store Procedure

1. Log in to System Manager Web Console.
2. Click **Security > Certificates > Authority**.
3. Click **Download pem file**. Save the pem file with an appropriate name, for example, `default-cacert.pem` and upload to the Lync Edge server.
4. Copy the System Manager CA certificate to the Lync Edge server.
5. On the Lync Edge, run the management console, click **Start > Run**.
6. In the **Run** dialog box, enter `mmc`, and click **OK**.
7. On **MMC Console**, select **File > Add/Remove Snap-in** to launch the Add/Remove Snap-in wizard.
8. In the **Add/Remove Snap-in** dialog box, click **Add**.
9. On the **Standalone** tab, click **Add**.
10. In the **Add Standalone Snap-in** dialog box, select **Certificates** and then click **Add**.
11. In the **Certificates Snap-in** dialog box, select **Computer Account** and click **Next**.
12. In the **Select Computer** dialog box, select the default setting **Local Computer** and click **Finish**.
13. In the **Add Standalone Snap-in** dialog box, click **Close**. And then in the **Add/Remove Snap-in** dialog box, click **OK**.

The system takes you to the MMC Console.

14. Click **Console Root**, select **Certificates > Trusted Root Certification Authorities**.
15. Select **Trusted Root Certification Authorities**, right-click **Certificates** and select **All Tasks > Import**.

The system opens the Certificate Import Wizard. Follow the steps of the wizard and browse for the `default-cacert.pem` file.

16. On the Certificate Import Wizard screen, click **Next**.
17. In the **Open** dialog box, click **Browse** to locate the file and then click **Next**.
18. Retain the default settings and then click **Next**.
19. Click **Finish** to complete the Certificates Import Wizard.
20. Verify the Certificate is in the `Certificates/Trusted Root Certification Authorities/ Certificates` list.

- a. Right-click **Certificates** and select **Refresh** to update the certificates list.

The system might display the certificate as the default setting.

- b. Verify that the serial number and the expiry date of the System Manager certificate match the serial number and the expiratory date of the new default certificate that appears in the certificate list on the Edge server.
- c. To determine the serial number and expiry date of the System Manager certificate, enter the following command on the Presence server: `openssl x509 -in $PRES_HOME/jabber/xcp/certs/default-cacert.pem -noout -text`.

The details of this certificate must match the default certificate added to Edge server.

- d. To determine if the certificate was added, double-click the certificate in the list of certificates.

If the system does not display a default certificate, then the Presence Services CA Certificate has not been added to the Lync Edge server's Trusted Root Certificates.

**\* Note:**

The `default-cacert.pem` is the name given to the System Manager CA certificate when the system downloads the from the System Manager security management page.

## DNS Administration

### Adding a DNS SRV record for the OCS Gateway

On the DNS for the Microsoft domain, which is the DNS server that Edge server uses, the FQDN of the Presence Services specified in the network address in the IM provider section must be resolvable. You must also add a DNS SRV record for the Presence server (OCS Gateway).

You must create the DNS records that meet the following criteria:

1. When Presence Services contacts Edge server, Presence Services provides a certificate that contains the Presence Services FQDN. Ensure that this FQDN is resolvable in the DNS of the OCS.
2. The Edge server performs a DNS lookup on the Presence Services FQDN. The Edge server rejects the TLS connection request with Presence Services if the DNS server does not return the same FQDN as in the certificate.

3. The Edge server performs a reverse DNS lookup on the IP address of Presence Services. The Edge server rejects TLS connection request with Presence Services if the DNS server does not return the same IP address as in the certificate.
4. The OCS Edge server performs a SRV DNS lookup for the SRV record `_sipfederationtls._tcp.<PS domain>`. The PS domain is also referred to as the Router Service Name. PS domain is the domain part of the SIP URI in a SIP request originating from the Presence server. It gets the SIP domain from the name of the Presence Services user requesting the subscription. In this case, the SIP domain is the Presence ID domain of the Presence server.

**\* Note:**

If the firewall on Microsoft Edge server is on, update the firewall so that the Presence server can gain access to port 5061 on the Edge server.

## Adding New Host (A)

### Procedure

1. On the OCS DNS server, right-click the domain that you just created and select **New Host (A)**.
2. In the New Host dialog box, enter the Presence server name and IP address. For example, `ipsdemo-ips1.ipsdemo.com`.
3. Click **Add Host > Done**.

**\* Note:**

When you add New Host (A) in DNS, check the associated pointer. This associated pointer may eliminate the need to add the machine name to the Reverse Lookup Zone if that zone already exists.

## Related Links

[Reconfiguring OCS](#) on page 256

## Adding a new reverse pointer

### Procedure

1. On the OCS DNS server, in the left navigation pane, select **Reverse Lookup Zones > New Zone**.
2. To add a new zone, on the **Action** menu, click **New Zone > Next**.
3. Select **Primary zone** and **Store the zone in Active Directory**.
4. Click **Next**.
5. Select **To all DNS servers in the Active Directory domain ...**.
6. Click **Next**.
7. Enter the `Network ID` corresponding to the Presence server, and click **Next**.
8. Select **Allow both non-secure and secure dynamic updates**, and click **Next**.

9. Click **Finish**.
10. Right-click on the new zone you just created and select **New Pointer (PTR)...**
11. In the **Host IP number** field, enter the Host IP number of the Presence server.
12. In the **Host Name** field, enter the Host Name of the Presence server.
13. Click **OK**.

### **Adding OCS Gateway as an IM service provider for Microsoft OCS Procedure**

1. Click **Start > All Programs > Administrative Tools > Computer Management**.  
The system displays the Computer Management window.
2. In the left navigation pane, expand **Services and Applications** and then select **Microsoft Office Communications 2007**.
3. Right-click **Microsoft Office Communications 2007 > Properties**.
4. On the **IM Provider** tab, click **Add**.

Enter details in the following fields:

- **IM service provider name:** This name must match the Presence ID domain name used by the Presence server. For example, `ipsdemo.com`
- **Network address of the IM service provider Access Edge:** This address must match the hostname of the Presence server. For example, `ipsdemo-ips1.ipsdemo.com`.
- **This is a public IM service provider:** Do not clear this field.
- **Allow all communications from this provider:** Select this option for filtering incoming communication.

5. Click **OK**.

### **Adding OCS Gateway as an IM service provider for Lync Procedure**

1. On the Lync Front End Server, click **Start > All Programs > Microsoft Lync Server 2010 > Microsoft Lync Server Control Panel**.

**\* Note:**

Log in as a user from Active Directory, who is a member of the CSAdministrator group. (The user account cannot be the local administrator of the server running Lync Server 2010, Standard Edition) You may need to add a user to the CSAdministrator group, and if that user is currently logged on, log them off and on again to register the group membership update.

2. Under External User Access, click **Provider**.
3. Click **New > Public Provider**.
4. Ensure that you select the **Enable communications with this provider** check box.

5. Specify the JID domain name that the Presence server uses for Provider and the Presence server FQDN for the Access Edge (FQDN).
6. Click **External User Access** and then click the **External Access Policy** tab.
7. Select the global policy and click **Edit**.  
The system displays the Edit External Access Policy screen.
8. Ensure that you select the following:
  - **Enable communications with federated users**
  - **Enable communications with remote users**
  - **Enable communications with public users**
9. To save the changes, click **Commit**.
10. Click the **Access Edge Configuration** tab and then click **Edit**.  
The system displays the Edit Access Edge Configuration screen.
11. Ensure that you select the following:
  - **Enable federation**
  - **Enable partner domain discovery**
  - **Enable remote user access**
  - **Enable anonymous user access to conferences**
12. To save the changes, click **Commit**.

### **Enabling an OCS user for remote access and federation Procedure**

1. Click **Start > All Programs > Administrative Tools > Microsoft Office Communications Server 2007 R2**.
2. Right-click **Forest** and select **Properties > Global Properties**.  
The system displays the **Office Communications Server Global Properties** dialog box.
3. On the **Federation** tab, select **Enable Federation and Public IM connectivity**.
4. In the **FQDN** field, enter the external FQDN of the OCS Edge server.
5. In the **Port** field, enter 5061.
6. Click **Start > All Programs > Administrative Tools > Active Directory Users and Computer**.
7. In the left navigation pane, click **Users**.
8. Double-click an enterprise user.  
The system displays the **Properties** dialog box of the selected user.
9. In the **Properties** dialog box of the user, click the **Communications** tab, and then click **Configure...** next to Other settings.

10. In the **Other Options** dialog box:
  - a. Select **Enable federation**
  - b. Select **Enable remote user access**
  - c. Select **Enable public IM connectivity**
  - d. Click **OK**
  - e. Click **OK**
11. Repeat the steps for all other OCS users.

## Enabling a Lync user for remote access and federation

### Procedure

1. On the Lync Front End Server, click **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Control Panel** and gain access as a CSAdministrator group user.
2. In the left navigation pane, click **Users**.
3. In the **Provided Search Filter** field, enter all or part of the name of an Active Directory user that you want to enable for Lync.
4. In the search results displayed, select a user you want to enable and click **Edit**.
5. Ensure that you select **Enable for Lync Server** check box, and in the **SIP address** field, enter the login handle for the user, selecting the enterprise SIP domain from the drop-down.
6. Ensure that system defaults the Registrar pool field to the Lync Front End pool.
7. For Telephony, select **PC-to-PC only**.
8. For External Access Policy, select from the following choices:
  - Global: Ensure this policy is correctly set to allow federation as described in an earlier section.
  - Custom policy: Ensure that you enable Federation, Public, and Outside Access.
9. For all other policy fields, select **Automatic**.
10. Repeat the steps for all other users you want to enable for Lync remote access and federation.

## Restarting the Edge server service after completing changes to DNS

### About this task

The Edge server hold a cache of DNS information. Restart Edge server if you have entered an incorrect DNS entry. You must recreate the entry to prevent Edge server from storing the incorrect DNS records.

### Procedure

1. On the Microsoft Edge Server, click **Start > Administrative Tools > Services**.
2. Locate the Office Communications Server Access Edge service.
3. Right-click **Office Communications Server Access Edge** service and select **Start > Start all stopped Services**.

## Presence Services Trust Management for OCS integration

### Downloading the CA that signed the certificate for the External Interface of the Edge server

#### About this task

You must add the CA, which signed the certificate that the External Interface of the Edge server uses, to the Presence Services list of trusted CAs. Download the CA from a standalone Microsoft Enterprise Certificate Authority and convert the CA to a format that you can use on Presence Services.

#### Procedure

1. From a Microsoft server, enter `http://<CA_Machine>/certsrv/` in the address bar.  
The system displays the Web enrollment page of the Certificate Authority.
2. On the Web enrollment page, click **Download a CA certificate, certificate chain, or CRL > Download CA certificate chain > Save**.
3. In Windows Explorer, double-click the `filename.p7b` file.  
The system displays a Certificates window.
4. In the left pane of the Certificates window, click the file name.
5. Click the **Certificates** folder.  
The system displays a list of certificates.
6. Select a certificate to convert to the PEM format.
7. Right-click the certificate, then select **All Tasks > Export** to display the Certificate Export wizard.
8. On the Certificate Export wizard, click **Next**.
9. Select the **Base-64 encoded X.509 (.CER)** option.
10. Click **Next**.  
Base-64 encoded is the PEM format.
11. In the **File name** field, enter a name for the converted digital certificate.
12. Click **Next**.
13. Copy the Microsoft root CA to any location on Presence Services. For example, `/opt/Avaya/Presence/jabber/xcp/certs` or `$JABBER_HOME/certs`.
14. Run `dos2unix <msroot>.cer`.
15. Run `$PRES_HOME/presence/bin/prescert addTrusted pem<msroot>.cer alias <optional name>`.

## Adding Federation Domain to the Presence Services Global Router Configuration

### About this task

When the Presence server receives presence subscriptions from the OCS domain, the subscriptions are subject to authorization rules, and the Presence server applies the ACL controls to the subscription. As the subscribing user is effectively an external user that is external to Avaya Aura® and external to Presence Services, by default, the system treats the authorization as a CONFIRM ACL. To apply this CONFIRM policy, Presence server must recognize the OCS domain. Therefore, you must add the OCS domain to the Federation Domain list in the Presence Services global router configuration.

### Procedure

1. Log in to the XCP Controller Web interface.
2. On the home page, scroll to the Core Router and click the **Edit** link. The system displays the Global Settings Configuration page.
3. In the Federation Domains section, select the **Federation Domain(s)** check box, if not already selected, and add the OCS domain to the Federation Domain.

## Stopping the Presence server

Avaya recommends that you use a script instead of the Presence Services Web GUI to stop the entire Presence Services system.

### Before you begin

Before you stop Presence Services, you must have an instance of Presence Services running on your server.

### About this task

The purpose of this task is to terminate the activity of Presence Services.

### Procedure

To stop Presence Services, run `/opt/Avaya/Presence/presence/bin/stop.sh`

### Note:

You can use this script to stop jadderd.

## Starting the Presence server

Avaya recommends that you use a script instead of the Presence Services Web GUI to start the entire Presence Services system.

### Before you begin

Before you start Presence Services, you must have an instance of Presence Services on your server that is not currently running.

### About this task

The purpose of this task is to start or restart the activity of Presence Services.

## Procedure

To start Presence Services, run `/opt/Avaya/Presence/presence/bin/start.sh`

### \* Note:

You can use this script to start jadderd.

## Verifying the trust configuration

### Procedure

1. Log in to the OCS Edge server.
2. On the prompt, type `nslookup <FQDN of Presence Services>`. The system returns the IP address of the Presence server.
3. Type, `nslookup <IP Address of Presence Services>`.  
The system returns the FQDN of the Presence Services machine and port 5061.
4. Log in to the Presence server and use the `presstatus` tool, which is located in the `/opt/Avaya/Presence/presence/bin` directory, to see the status of the Microsoft Office Communications Server Integration component.
5. Use the `/opt/Avaya/Presence/presence/bin/prescert list` command and ensure that the OCS CA certificate is in the trust store.

## Adding Microsoft OCS/Lync SIP user handles to System Manager

### Procedure

1. Log on to System Manager web Console as an administrator.
2. On System Manager Dashboard, click **User Management > Manage Users**.
3. On the User Management page, select the relevant user and click **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. On the Communication Profile page, click **New** in the Communication Address section.
6. From the **Type** drop-down list box, select **Microsoft OCS SIP**.
7. In the **Fully Qualified Address:** field, enter the handle and domain details.

For example, in the **Handle** field, enter `sip:handle` and in the **Domain** field, enter `ocsdomain.com`.

8. Click **Add**.

## Changing the Cipher Suite Order

An issue was identified in Windows Server 2008 while establishing a communication between the Lync Edge and an external provider through Public Internet Cloud (PIC). The initial SSL dialog established between the Presence server and Lync Edge needs to use a different cipher suite in place of the default cipher suite in Windows Server 2008. This requires modifying the Cipher Suite

Ordering on the Windows Server on which you deploy the Lync Edge. You must use the `TLS_RSA_WITH_RC4_128_MD5` cipher suite.

## Procedure

1. On the Windows Server 2008 (x64) Edge server, click **Start > Run > gpedit.msc > OK**.
2. In the Group Policy Object Editor, click **Computer Configuration > Administrative Templates > Network**.
3. Under Network, click **SSL Configuration**, and then double-click **SSL Cipher Suite Order** (by default, the SSL Cipher Suite Order is set to **Not Configured**)
4. Select the **Enable** radio button.
5. From the SSL Cipher Suites text box, copy the entire text from the SSL Cipher Suites text box to a Notepad. It should look like the following:

```
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA
```

You must move the `TLS_RSA_WITH_RC4_128_MD5` value to the beginning of the list.

6. In your Notepad, where you have copied the text from the SSL Cipher Suites text box, search for the `TLS_RSA_WITH_RC4_128_MD5` value and move it to the beginning of the list. It should look like the following:

```
TLS_RSA_WITH_RC4_128_MD5,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA
```

7. Copy the recently formatted list back into the SSL Cipher Suites text field, click **OK**.
8. For the changes to take effect, restart the Windows Server 2008 (x64) Edge server.

## Troubleshooting

### Enabling logging for OCS Gateway

#### Procedure

1. Log in to the Presence server.
2. Once logged in, type the following command to log in as the root user: **su root**
3. Check the current log level, type `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh cm-2 -c`.

**\* Note:**

OCS Gateway logging is typically set at the WARN level. To diagnose any issue, you must increase the logging level to DEBUG.

4. To increase the logging level, type the following command until you reach the DEBUG level, `/opt/Avaya/Presence/jabber/xcp/bin/updateLogLevel.sh cm-2 -i`.
5. Check the filtering level of the rsyslog logger in the `/etc/rsyslog.conf` file.
6. Restart the logging service, type `Service rsyslog restart` to restart service logging.

**\* Note:**

Service rsyslog sends the OCS Gateway logging to the `/var/log/messages` file. You can recognize the OCS Gateway records by the logging tag `OCS_GW` in each of the associated log output entries from the OCS Gateway. The system sends the debug level logging messages from the OCS Gateway to `/var/log/messages` and extracts these messages to assist in diagnosing any problems that you might encounter.

### Changing the default logging level

#### Procedure

1. Log in to the Presence server.
2. Make changes to the `/opt/Avaya/Presence/presence/lib/path/log4j.xml` file.
3. Enable the relevant section and change the level as required.

```
<logger name="events.operational">
  <level
value="WARN#com.avaya.common.logging.client.LogLevel"/
>
  </logger>
to, for example,
<logger name="events.operational">
  <level
value="INFO#com.avaya.common.logging.client.LogLevel"/
```

```
>  
</logger>
```

**\* Note:**

The system generates more log records if you set a level lower. Do not set a low level for a long period of time. If you do, you will have to navigate through unwieldy log files. Set a lower log level for individual components as opposed to changing the default for the whole Presence server.

If the log level of a component is increased to the DEBUG level then you must change it back to the ERROR level as soon as the required debug logs are collected for debugging.

## OCS server side logging

### Starting SIP logging on OCS Edge

#### Procedure

1. Click **Start > Control Panel > Administrative Tools**.
2. Double-click **Computer Management**. The system displays the Computer Management page.
3. Click **Services and Applications** and then select **Microsoft Office Communications Server**.
4. Right-click **Microsoft Office Communications Server** and select **Logging Tool > New Debug**. The system displays the Microsoft Office Communications Server 2007 Logging Tool page.
5. From the Components list, select **SIPStack**.
6. Click **Start Logging**.

### Starting SIP logging on OCS Server

#### Procedure

1. Click **Start > Control Panel > Administrative Tools**.
2. Double-click **Microsoft Office Communications Server 2007**. The system displays the Microsoft Office Communications Server 2007 page.
3. Click **Enterprise pools**.
4. Right-click **Pools > New Debug Session**.
5. From the **Components** list, select **SIPStack**.
6. Click **Start Logging**.

### Enabling logging on the OCS server

#### Procedure

1. On the Microsoft Office Communications Server 2007 Logging Tool page, click **Stop Logging**.

2. Click **Analyze Log Files** or **View Log Files**.

**\* Note:**

- When you click **View Log Files**, the system displays the trace in the text mode.
- When you click **Analyze Log Files**, the system displays the trace in the GUI mode.

3. In the Snooper GUI, check all the SIP trace messages.

## Lync server side logging

### Starting SIP trace on Lync Edge

#### Procedure

1. Click **Start > Microsoft Lync Server 2010 > Lync Server Logging Tool**.

The system displays the logging properties page, where you can select components and flags for the logging sessions.

2. From the Components list, select **SIPStack**.
3. Click **Start Logging**.

### Starting SIP trace on Lync server

#### Procedure

1. Click **Start > Microsoft Lync Server 2010 > Lync Server Logging Tool**.

The system displays the logging properties page, where you can select components and flags for the logging sessions.

2. From the Components list, select **SIPStack**.
3. Click **Start Logging**.

### Checking the SIP trace

#### Procedure

1. On the Microsoft Office Communications Server 2007 Logging Tool page, click **Stop Logging**.
2. Click **Analyze Log Files** or **View Log Files**.

**\* Note:**

- When you click **View Log Files**, the system displays the trace in the text mode.
- When you click **Analyze Log Files**, the system displays the trace in the GUI mode.

3. In the Snooper GUI, check all the SIP trace messages.

## Lync federation with Presence Services cluster using Session Manager as edge server

### Checklist for configuring Presence Services cluster federation with Lync through Session Manager

No.	Task	Link	✓
DNS Administration			
1	Add a DNS SRV record for the Lync/OCS Gateway.	<a href="#">Adding a DNS SRV record for the Lync/OCS Gateway</a> on page 207	
2	Add New Host (A).	<a href="#">Adding New Host (A)</a> on page 208	
3	Add a new reverse pointer.	<a href="#">Adding a new reverse pointer</a> on page 208	
Lync server			
4	Generate and import certificate for Lync.	<a href="#">Generating a Web server certificate with server and client authentication</a> on page 187	
5	Import the System Manager CA root certificate into the Lync Edge Trust store.	<a href="#">Importing the System Manager default CA certificate into the Lync Edge Trust Store</a> on page 193	
6	Add Presence Services as an IM service provider for Lync.	<a href="#">Adding OCS Gateway as an IM service provider for Lync</a> on page 209	
7	Enable a Lync user for remote access and federation.	<a href="#">Enabling a Lync user for remote access and federation</a> on page 210	
8	Restart the Edge server service after completing changes to DNS.	<a href="#">Restarting the Edge server service after completing changes to DNS</a> on page 198	
9	Download the root certificate of the CA that has signed the certificate used on the External Interface of the Edge server.	<a href="#">Downloading the CA that signed the certificate for the External Interface of the Edge server</a> on page 210	
10	Verify the trust configuration.	<a href="#">Verifying the trust configuration</a> on page 211	
Presence Services configuration			
11	Enable OCS Gateway.	<a href="#">Enabling OCS Gateway</a> on page 211	
12	Add Lync domain to the Presence Services Global Router configuration.	<a href="#">Adding Federation Domain to the Presence Services Global Router Configuration</a> on page 200	
13	Configure the SIP Remote Host Configuration parameters.	<a href="#">Configuring the SIP Remote Host Configuration parameters</a> on page 213	

No.	Task	Link	✓
14	Configure the SIP Stack Configuration parameters for the OCS Gateway.	<a href="#">Configuring the SIP Stack Configuration parameters for the OCS Gateway</a> on page 176	
15	Configure the OCS Gateway Hostname filter.	<a href="#">Configuring the OCS Gateway Hostname Filter: Open Port component configuration</a> on page 179	
16	Configure SIP Proxy routing rules for OCS Gateway.	<a href="#">Configuring SIP Proxy routing rules for OCS Gateway</a> on page 180	
17	Add a new Remote Host.	<a href="#">Adding a new Remote Host</a> on page 214	
18	Add a new routing label for the OCS Gateway.	<a href="#">Adding a new routing label for the OCS Gateway</a> on page 183	
Session Manager configuration			
19	Update the Session Manager TLS certificate.	<a href="#">Updating the Session Manager TLS certificate</a> on page 214	
20	Verify the updated Session Manager TLS certificate.	<a href="#">Verifying the updated Session Manager TLS certificate</a> on page 215	
21	Add the host information on Session Manager.	<a href="#">Adding host information on Session Manager</a> on page 215	
22	Add the SIP entities and the entity link representing Lync edge server.	<a href="#">Adding SIP entities and the entity link representing Lync edge server</a> on page 216	
23	Add the routing regular expressions.	<a href="#">Adding the routing regular expressions</a> on page 218	
24	Add the routing policies.	<a href="#">Adding the routing policies</a> on page 219	
25	Add or update the existing Communication Manager application.	<a href="#">Adding or updating the existing Communication Manager application</a> on page 220	
26	Update the Avaya Aura® user configuration.	<a href="#">Updating the Avaya Aura user configuration</a> on page 222	

## Adding a DNS SRV record for the Lync/OCS Gateway

1. On the DNS for the Microsoft domain, which is the DNS server that Edge server uses, the FQDN of the Session Manager SIP asset must be resolvable.
2. You must add a DNS SRV record: `_sipfederationtls._tcp` for the Presence Services pointing to the Session Manager server FQDN so that Lync will send the SIP messages to Session Manager.

**\* Note:**

If the firewall on Microsoft Edge server is on, update the firewall so that the Session Manager server can gain access to default port 5061 on the Edge server.

## Adding New Host (A)

### Procedure

1. Log in to the OCS DNS server as an administrator.
2. In the **Forward Lookup Zones** section, create a domain for Session Manager, if not created.  
  
For example, `ca.avaya.com`.
3. Right-click the domain that you created, and select **New Host (A)**.
4. In the New Host dialog box, type the Session Manager SIP server name and IP address.  
  
For example, `sm-sip-pslab.ca.avaya.com` and `47.11.48.165`.
5. Click **Add Host > Done**.

 **Note:**

When you add New Host (A) in DNS, you can select the **Create associated pointer (PTR) record** check box. This pointer might eliminate the need to add the machine name to Reverse Lookup Zone if the zone already exists.

## Adding a new reverse pointer

### Procedure

1. On the Lync/OCS DNS server, in the navigation pane, click **Reverse Lookup Zones > New Zone**.
2. On the **Action** menu, click **New Zone > Next** to add a new zone.
3. Select **Primary zone** and **Store the zone in Active Directory**.
4. Click **Next**.
5. Click **To all DNS servers in the Active Directory domain ...**
6. Click **Next**.
7. Type the `Network ID` corresponding to the Session Manager server, and click **Next**.
8. Select **Allow both non-secure and secure dynamic updates**, and click **Next**.
9. Click **Finish**.
10. Right-click the zone you created, and select **New Pointer (PTR)...**
11. In the **Host IP number** field, type the SIP IP address of the Session Manager server.
12. In the **Host Name** field, type the SIP FQDN of the Session Manager server.
13. Click **OK**.

## Adding OCS Gateway as an IM service provider for Lync

### Procedure

1. On the Lync Front End Server, click **Start > All Programs > Microsoft Lync Server 2013 > Microsoft Lync Server Control Panel**.

**\* Note:**

Log in as a user from Active Directory, who is a member of the CSAdministrator group. The user account cannot be the local administrator of the server running Lync Server 2010, Standard Edition. You may need to add a user to the CSAdministrator group, and if that user is currently logged on, log them off and on again to register the group membership update.

2. Under Federation and External User Access, click **SIP Federation Providers**.
3. Click **New > Public Provider**.
4. Ensure that you select the **Enable communications with this provider** check box.
5. In **Provider name**, specify the domain name that the Presence server uses as a presence/IM service provider.
6. In **Access Edge service (FQDN)**, specify the Session Manager Server FQDN.
7. Ensure that you select the Allow users to communicate with everyone using this provider for the Default verification level.
8. To save the changes, click **Commit**.
9. Click **External Access Policy**.
10. Select the global policy and click **Edit > Show details**.

The system displays the Edit External Access Policy screen.

11. Ensure that you select the following:
  - **Enable communications with federated users**
  - **Enable communications with remote users**
  - **Enable communications with public users**

12. To save the changes, click **Commit**.
13. Click **Access Edge Configuration**.
14. Click **Edit > Show details**.

The system displays the Edit Access Edge Configuration screen.

15. Ensure that you select the following:
  - **Enable federation**
  - **Enable partner domain discovery**
  - **Enable remote user access**
  - **Enable anonymous user access to conferences**

16. To save the changes, click **Commit**.

## Enabling a Lync user for remote access and federation

### Procedure

1. On the Lync Front End server, click **Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel** and gain access as a CSAdministrator group user.
2. In the navigation pane, click **Users**.
3. Click **Enable Users > Add**.
4. In the **Select from Active Directory** window, enter all or part of the name of an Active Directory user that you want to enable for Lync.
5. In the search results displayed, select a user you want to enable, and click **OK**.
6. Ensure that you select the proper edge server pool for the user from the **Assign users to a pool** drop down list.
7. Click **generate user's SIP URI** and ensure that you have created a SIP URI for the user.
8. For Telephony, select **PC-to-PC only**.
9. For all other policy fields, select **Automatic**.
10. Click **Enable** to enable the user for federation.
11. Repeat the steps for all other users you want to enable for federation.

## Downloading the CA that signed the certificate for the External Interface of the Edge server

### About this task

You must add the CA that signed the certificate that the External Interface of the Edge server uses to the Session Manager list of trusted CAs. Download the CA root certificate from a standalone Microsoft Enterprise Certificate Authority and convert the certificate to a format that you can use on Session Manager.

### Procedure

1. From a Microsoft server, enter `http://<CA_Machine>/certsrv/` in the address bar.  
The system displays the Web enrollment page of the Certificate Authority.
2. On the Web enrollment page, click **Download a CA certificate, certificate chain, or CRL > Download CA certificate chain > Save**.
3. In Windows Explorer, double-click the `filename.p7b` file.  
The system displays a Certificates window.
4. In the left pane of the Certificates window, click the file name.
5. Click the **Certificates** folder.  
The system displays a list of certificates.

6. Select a certificate to convert to the PEM format.
7. Right-click the certificate, then select **All Tasks** > **Export** to display the Certificate Export wizard.
8. On the Certificate Export wizard, click **Next**.
9. Select the **Base-64 encoded X.509 (.CER)** option.
10. Click **Next**.  
Base-64 encoded is the PEM format.
11. In the **File name** field, enter a name for the converted digital certificate.
12. Click **Next**.
13. On the System Manager web console, click **Inventory** > **Manage Elements**, and select the Session Manager server used for the Lync federation.
14. Click **More Actions** > **Configure Trusted Certificates** > **Add**.
15. In the **Add trusted Certificate** window, select **SECURITY\_MODULE\_SIP** from the **Select Store Type to add trusted certificate** drop down list.
16. Select **Import from file**, and click **Browse...** to select the file.
17. Click on **Retrieve Certificate** to check the certificate to be loaded.
18. Click **Commit** to save the changes.

## Verifying the trust configuration

### Procedure

1. Log in to the OCS Edge server.
2. On the prompt, type `nslookup <FQDN of Session Manager>`, and press **Enter**.  
The system returns the IP address of the Session Manager server.
3. Type `nslookup <IP Address of Presence Services>`, and press **Enter**.  
The system returns the FQDN of the Session Manager machine and port 5061.
4. Log in to the Presence server and use the `presstatus` tool, which is located in the `/opt/Avaya/Presence/presence/bin` directory, to see the status of the Microsoft Office Communications Server Integration component.

## Enabling OCS Gateway

You can enable an OCS Gateway in the following scenarios:

- During Presence Services installation
- After Presence Services installation

### Related Links

[Enabling OCS Gateway during installation](#) on page 212

[Enabling OCS Gateway post installation](#) on page 212

## Enabling OCS Gateway during installation

When you select and enable an OCS Gateway at the time of installation, as a part of the installation process, the system requests the following configuration parameters:

- OCS/Lync Edge: The FQDN of the Session Manager server. For example, `sm-sip-pslab.ca.avaya.com`.
- OCS/Lync SIP Domain: The OCS/Lync domain. For example, `lync2013.ca.avaya.com`.
- OCS/Lync SIP Port: The TLS port used by the SIP stack.

The system presents a default 65061 port number for the OCS/Lync SIP port. You can accept this value invariably. The installer enables the OCS Gateway and sets up the configuration. Additionally, the system configures SIP Proxy with routing route and host mappings for interacting with OCS/Lync.

### Related Links

[Enabling OCS Gateway](#) on page 211

## Enabling OCS Gateway post installation

### About this task

The OCS Gateway provides IM and presence interoperability between a Presence Services installation and an OCS/Lync installation. You can achieve this by setting up a federated deployment between OCS/Lync and Presence Services. For this interoperability between the two systems, you must configure the Session Manager or the Presence Services server as an IM provider on the OCS/Lync Edge server on OCS/Lync, and also ensure that the relevant DNS network configuration and trust management is in place.

You can enable an OCS Gateway post installation through the XCP Controller Web interface.

### Procedure

1. Log in to the Presence Services XCP Controller Web interface.
2. In the **Components** area, select **Connection Manager** from the **Add a new** drop-down list, and click **Go**. The system displays the Connection Manager Configuration page. By default, the system displays a basic configuration view, but you must switch to the advanced configuration view.

#### **Tip:**

On the Connection Manager Configuration page, under the Connection Manager section, you can rename the **Description** field to `OCS Connection Manager` for more clarity.

3. Under the Command line to run section, change the text in the **Command line to run text box** to, `exec /opt/Avaya/Presence/jabber/xcp/bin/sip_gw -h %i -m %m -n %n -p %p -P /opt/Avaya/Presence/jabber/xcp/var/run/jabberd/%n.pid`. The OCS Gateway does not start, unless you make these changes.

4. From the **Add a New Command Processor** drop-down box, select **S2S Command Processor**.
5. Click **GO**. The system displays the S2S Command Processor Configuration page. The initial configuration settings on this page are the default settings for an XMPP S2S Gateway. You must remove parts of the default configuration and replace with SIP/Simple Gateway configuration.
6. In the Director Configuration section, the system presents two default XMPP directors. Click **Remove** next to each default XMPP directors.
7. To confirm the removal of the XMPP directors, on the **Click 'OK' to confirm removal from the configuration** dialog box, click **OK** for each of the XMPP directors.
8. On the S2S Command Processor Configuration page, under the Director Configuration section, from the **Add a new** drop-down box, select **SIP/SIMPLE Gateway** and then click **Go**.

The system displays the SIP/Simple Gateway Configuration page. The system requires a number of configuration parameters for the SIP/Simple Gateway, which includes Remote Host Configuration, SIP Stack Configuration, and Outbound Proxy configuration.

#### Related Links

[Enabling OCS Gateway](#) on page 211

## Configuring the SIP Remote Host Configuration parameters

### Procedure

1. On the SIP/Simple Gateway Configuration page, in the **Remote Host Configuration** section and click **Local Configuration**.
2. Click **GO** to add a new SIP Host.

The system displays the SIP Host Configuration page. This configuration defines a mapping between the OCS/Lync domain and the OCS/Lync Edge server. For the mapping, you need the following parameters:

- Remote server hostname
  - Server Type
  - Hostname mapping
3. In the **Remote server hostname** field, type the FQDN of the Session Manager server.
  4. From the **Server Type** drop down box, select **ocs**.
  5. In the Hostname Mappings section, in the **Hostname(s)** field, type the OCS/Lync domain.  
For example, `lync2013.ca.avaya.com`.
  6. To save the configuration, click **Submit**.

The system returns to the SIP/Simple Gateway Configuration page.

## Adding a new Remote Host

### Procedure

1. On the Presence Services XCP Controller home page, select the **Advanced** configuration view.
2. In the Components area, click **Edit** in the **Actions** column next to the SIP Proxy component.  
The system displays the SIP Proxy Configuration page.
3. In the **Remote Host Configuration** section, select **Local Configuration**, and click **Go** next to **Add a new SIP Host**.  
The system displays the SIP Host Configuration page.
4. In SIP Host, in the **Remote server hostname** field, type the FQDN of the Session Manager server.  
For example, `sm-sip-pslab.ca.avaya.com`.
5. From the **Server Type** drop-down box, select **ocs**.
6. In the **Hostname Mapping** field, type the OCS/Lync domain name.  
For example, `lync2013.ca.avaya.com`.
7. To save the changes, click **Submit**.  
The system returns to the SIP Proxy Configuration page. In the **Remote Host Configuration** section, the system displays the SIP Host entry that you created.

## Updating the Session Manager TLS certificate

### About this task

When Lync server connects to Session Manager using TLS connection, the **Common Name (CN)** field of TLS certificate must have the FQDN of the Session Manager SIP interface. By default, Session Manager does not use FQDN in the certificate. Thus, you must update the certificate through System Manager.

### Procedure

1. Log in to the System Manager web console.
2. Click **Inventory > Manage Elements**.
3. Select the Session Manager server used for the federation with the Lync server.
4. Click **More Actions > configure Identity Certificates**.
5. Select **Security Module SIP**, then click **Replace**.
6. Select **Replace this Certificate with Internal CA Signed Certificate**, and set the values of the following fields:
  - **Common Name (CN)**: Enter the Session Manager SIP FQDN. For example, `sm-sip-pslab.ca.avaya.com`.
  - **Key Algorithm**: Select the default value from the drop down list.

- **Key Size:** select the default value from the drop down list.

**\* Note:**

You can use a third party certificate. The certificate must have the Session Manager FQDN in the **Common Name (CN)** field. You must select the **Import third party certificate** option.

7. Click **Commit** to save the changes.
8. Click **Done** to go back to home page.
9. Reboot the Session Manager server to make sure the CA certificate change takes effect.

## Verifying the updated Session Manager TLS certificate

### Procedure

1. Log in to the System Manager web console.
2. Click **Elements > Session Manager > System Status > Security Module Status**.
3. The value in the **Certificate Used** column must be **customer CA**.

## Adding host information on Session Manager

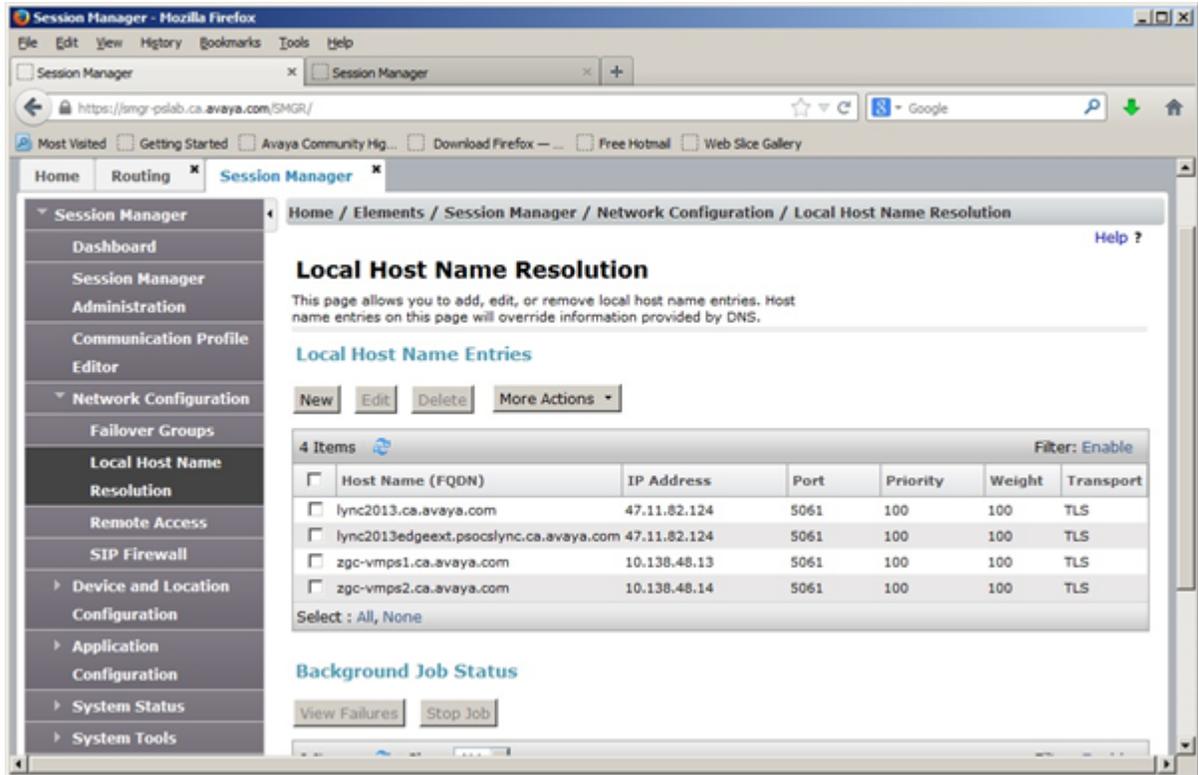
### Procedure

1. Log in to the System Manager web console.
2. Click **Session Manager > Network Configuration > Local Host name Resolution**.
3. Add the entries for Lync domain.

For example, **lync2013.ca.avaya.com** and the Lync edge external FQDN with the same edge external IP address. Use the 5061 port for TLS transport.

4. Add the entries for each Presence Services server FQDN.

Use the 5061 port for TLS transport.



5. Click **Commit** to save the changes.

## Adding SIP entities and the entity link representing Lync edge server Procedure

1. Log in to the System Manager web console.
2. Click **Routing** > **SIP Entities** > **New**.
3. Add a new entity entry for the Lync edge server with the following values:
  - **Name:** Enter a name for the Lync edge server.
  - **FQDN or IP Address:** Enter the Lync edge server external interface FQDN.
  - **Type:** Select **Other**.
  - **SIP Link Monitoring:** Select **Link Monitoring Disabled**.

Use default values for the other fields.

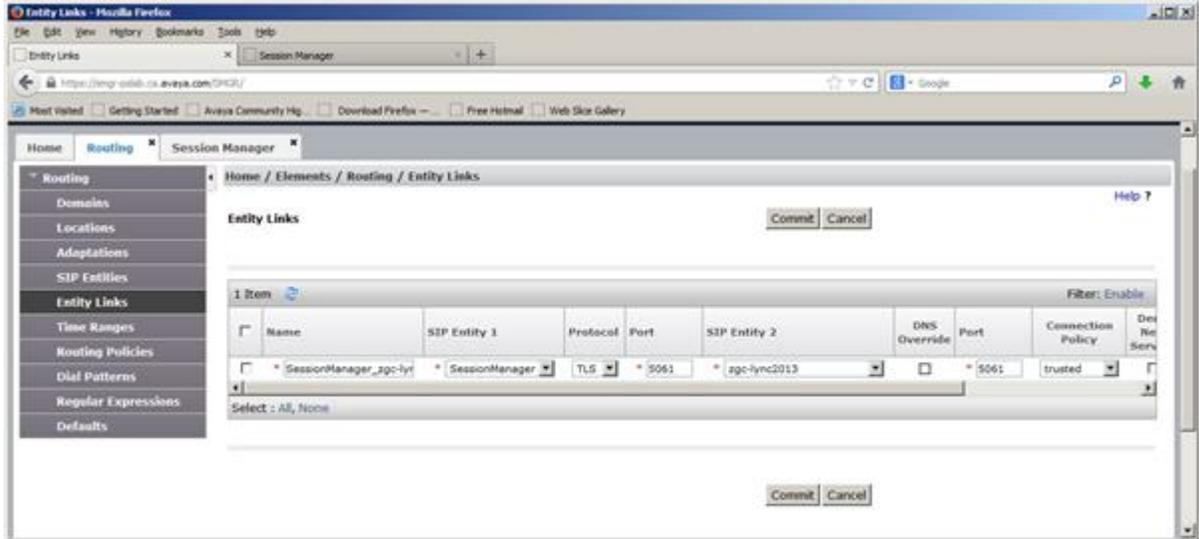
The screenshot shows the Avaya Aura System Manager 6.3 web interface. The browser window title is "SIP Entity Details - Mozilla Firefox". The address bar shows "https://smgr-pslab.ca.avaya.com/SMGR/". The page header includes the Avaya logo and "Aura System Manager 6.3". The breadcrumb trail is "Home / Elements / Routing / SIP Entities". The main content area is titled "SIP Entity Details" and has "Commit" and "Cancel" buttons. The "General" section contains the following fields:

- Name: zgc-lync2
- FQDN or IP Address: lync2013edgeext.psocslync.ca.av
- Type: Other
- Notes: (empty)
- Adaptation: (empty)
- Location: Lab1
- Time Zone: America/Fortaleza
- SIP Timer B/F (in seconds): 4
- Credential name: (empty)
- Call Detail Recording: none
- CommProfile Type Preference: (empty)

The "Loop Detection" section has "Loop Detection Mode" set to "Off". The "SIP Link Monitoring" section has "SIP Link Monitoring" set to "Link Monitoring Disabled". At the bottom, there are checkboxes for "Supports Call Admission Control" and "Channel Bandwidth Manager", both of which are unchecked.

4. Add an entity link between Session Manager and the Lync edge server using protocol TLS and the default port 5061.

The connection policy must be set to **trusted**.

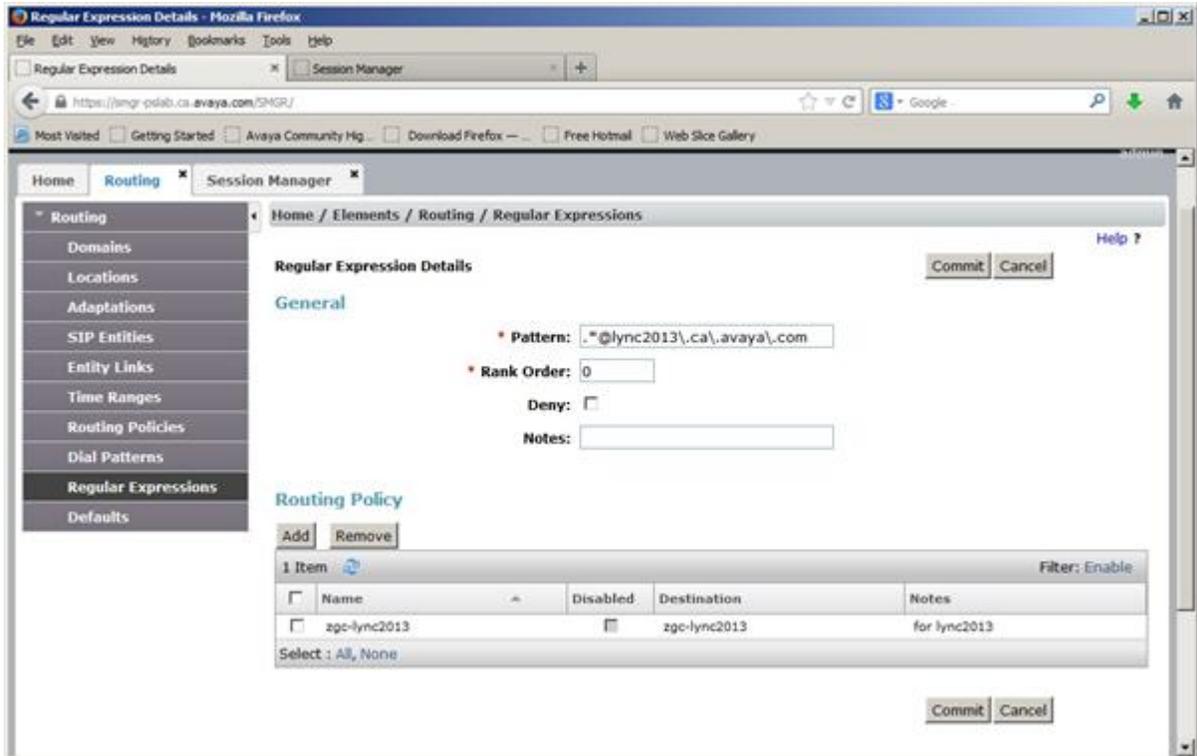


5. Click **Commit** to save the changes.

## Adding the routing regular expressions

### Procedure

1. Log in to the System Manager web console.
2. Click **Routing > Regular Expressions > New**.
3. On the **Regular Expression Details** page, enter the following values:
  - **Pattern:** Add a pattern for the Lync domain. For example, `.*@lync\.com`
  - **Rank Order:** Enter the proper rank value. For example, `0`.



4. Click **Commit** to save the change.
5. Use the above steps to create the pattern for each Presence Services node FQDN.

## Adding the routing policies

### About this task

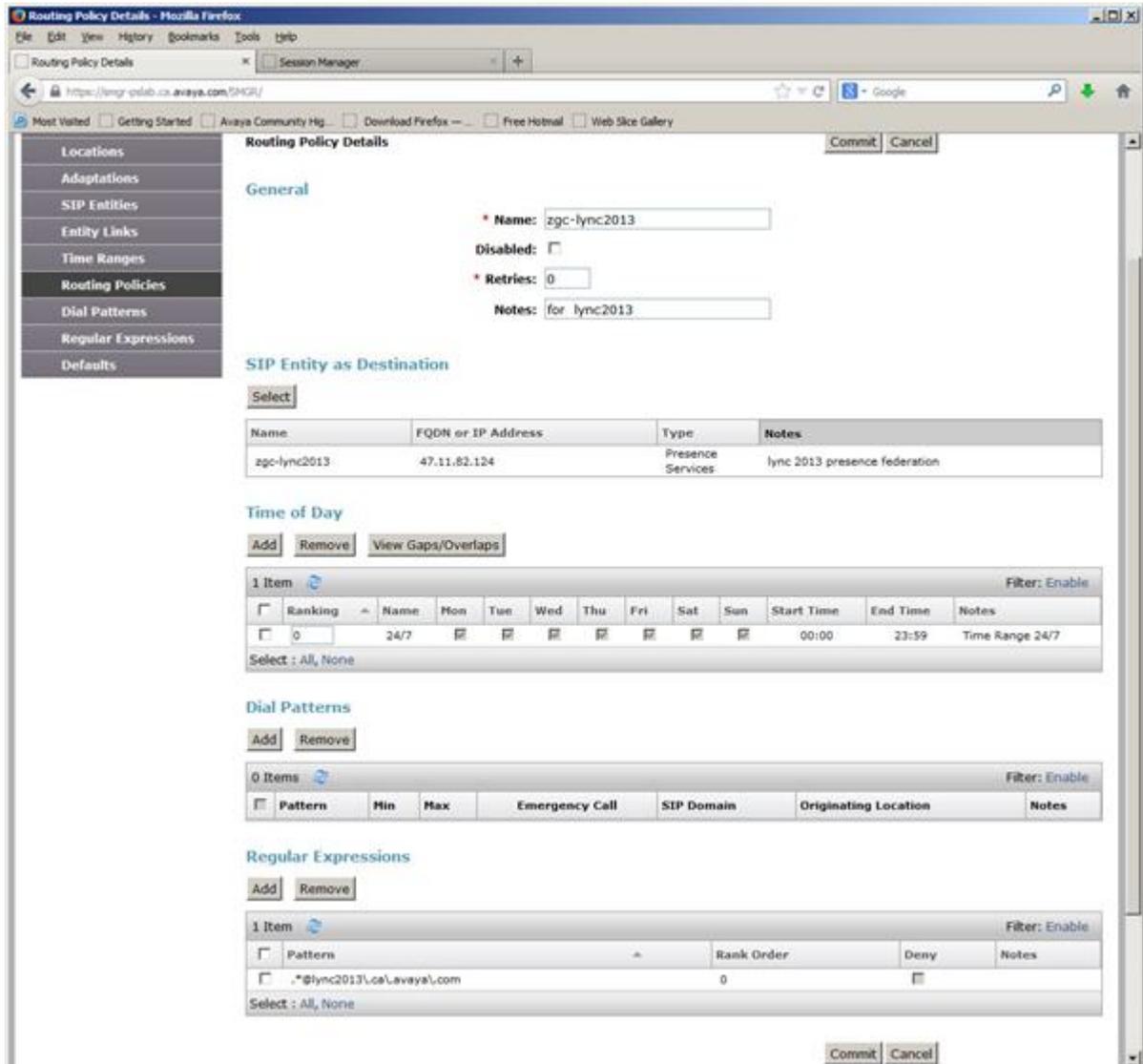
The routing policy must be configured so that the SIP messages are routed to Lync edge server and Presence Services servers.

Create one policy for the Lync edge server and create a policy for each Presence Services nodes if there are multiple nodes in the PS cluster.

### Procedure

1. Log in to the System Manager web console.
2. Click **Routing > Routing Policies > New**.
3. On the **Routing Policy Details** page, enter the following values:
  - **Name:** Enter a name for the policy.
  - **Retries:** Select **0**.
4. Select the SIP entity as destination. For example, the Lync edge server.
5. In the **Regular Expressions** section, click **Add** to select the corresponding regular expressions.

- Click **Select** to add the expression to the policy.



- Click **Commit** to save the change.
- Use the above steps to create the policy for each Presence Services node.

## Adding or updating the existing Communication Manager application

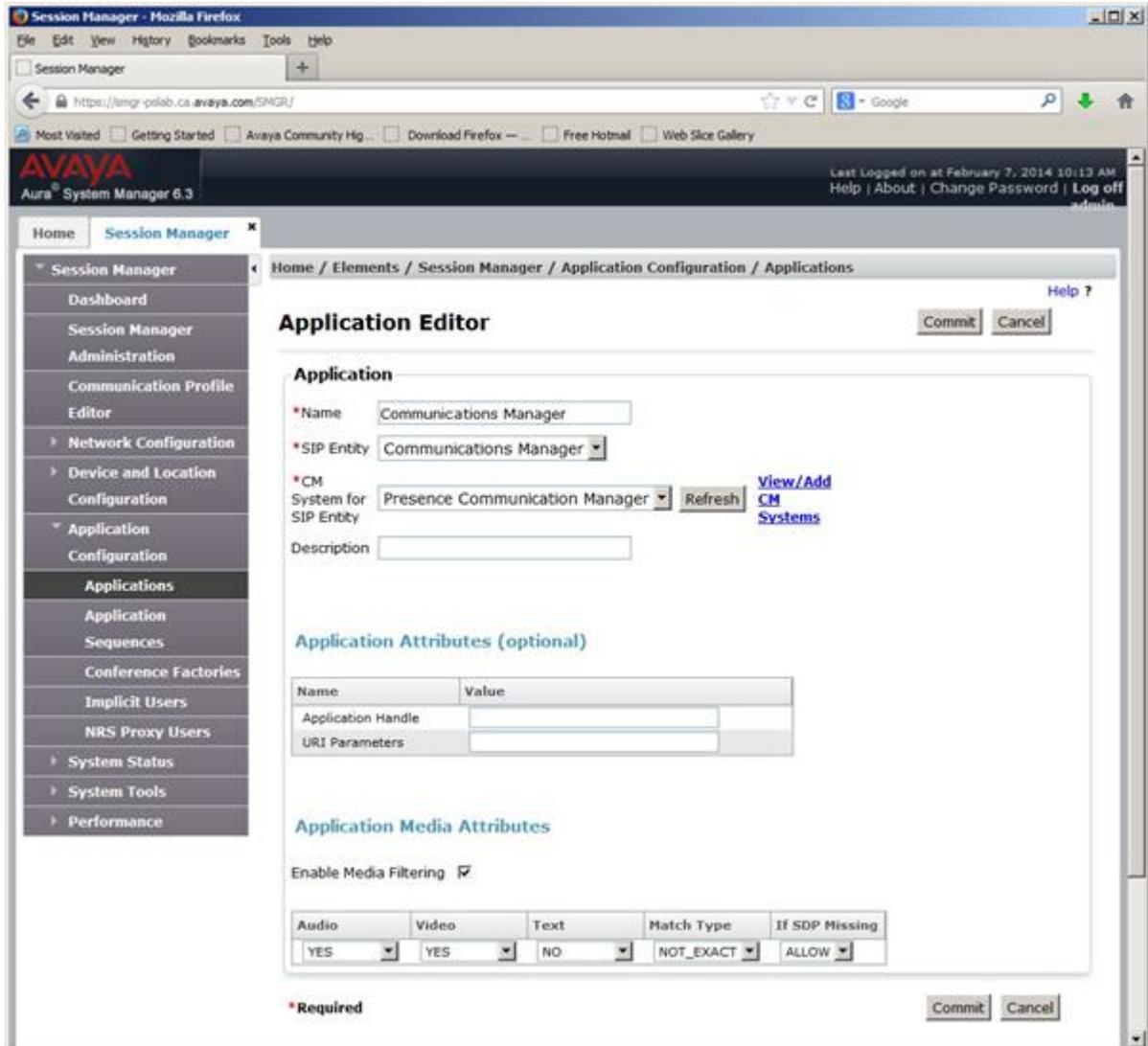
### About this task

If the user has a Communication Manager application defined in the application sequence, then the Communication Manager application must be added or updated according to the following procedure.

### Procedure

- Log in to the System Manager web console.

2. Click **Elements > Session Manager > Application Configuration > Applications**.
3. Click **New** to create a new Communication Manager application or select the existing Communication Manager application and click **Edit**.
4. In the **Application Editor Application** section, enter the following values:
  - **Name**: Enter a name for the Communication Manager application.
  - **SIP Entity**: Select the corresponding Communication Manager instance.
  - **CM System for SIP Entity**: Select the corresponding Communication Manager entity.
5. In the **Application Editor Application Media Attributes** section, enter the following values:
  - Select **Enable Media Filtering** check box.
  - **Audio**: Select **YES**.
  - **Video**: Select **YES**.
  - **Text**: Select **NOT\_ONLY**.
  - **Match Type**: Select **NOT\_EXACT**.
  - **If SDP Missing**: Select **ALLOW**.



6. Click **Commit** to save the changes.

## Updating the Avaya Aura® user configuration

### About this task

For the Avaya Aura® users configured in System Manager, you must configure the following:

- For each user, you must define the home Presence Services server in the Presence Profile. The users can be distributed to all Presence Services nodes evenly in the cluster.
- For each user, you must define a communication address of the **Avaya SIP** type that has the same value as the **Avaya Presence/IM** communication address of the user. This setting is necessary for Session Manager to route the messages to the Presence Services users from the Lync server.

### Procedure

1. Log on to the System Manager web console.

2. Click **User Management > Manage Users**.
3. Select the user to be updated, and click **Edit**.
4. In the **User Profile Edit** section, enter the following values:
  - **Communication Address**: Create the Avaya SIP communication address which is the same as the Avaya Presence/IM communication address. The user and domain portion must be identical.
  - **Presence Profile**: Select the home Presence Services system. Use the same Presence Services server as defined in the application sequence in this field.
5. Click **Commit** to save the changes.
6. Repeat the steps for all users that are federated to the Lync server.

## Presence Services multi-domain support with Lync federation using Session Manager as edge server

The following are the requirements of Presence Services multi-domain support with Lync federation using Session Manager as edge server:

- A DNS SRV record is required for the Lync federation for each Presence Services domain.
- The multiple Presence Services domains must have a common prefix or suffix in order to use the domain wildcard on Lync server. For example, the wildcard can be `presence.*` or `*.avaya.com`.

You need to add the domain wildcard in the provider section of SIP Federated Providers. Click the **Federation and External Access – SIP Federated Providers** link on the Lync server control panel to access SIP Federated Providers.

- The Lync configuration change requires some time to take effect. It is recommended to restart both Presence Services and Lync servers, and wait 30 minutes after the configuration change.

**\* Note:**

The edge server defined for the provider and the DNS SRV record must be the Session Manager SIP FQDN.

**\* Note:**

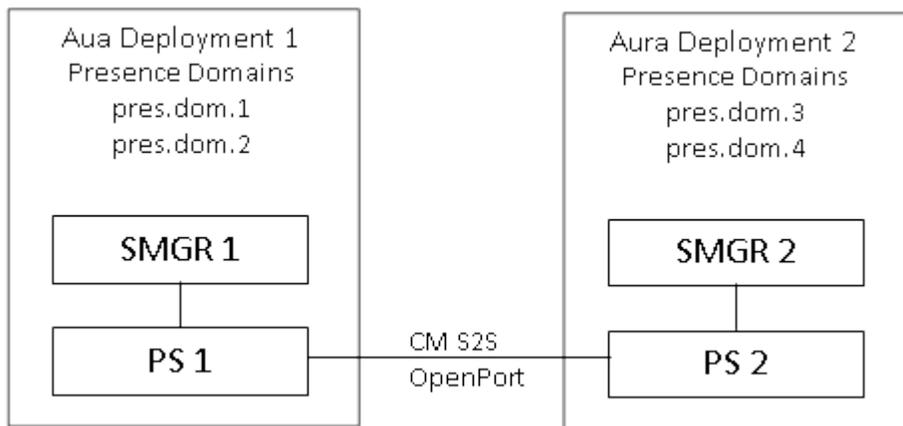
Multiple domains with distinct domain name are not supported with Lync federation.

---

## Federation between Avaya Aura<sup>®</sup> domains

Presence Services supports federation between two independently-administered Avaya Aura<sup>®</sup> deployments, each with a dedicated System Manager and a different presence domain(s). For example, in the following diagram:

- Avaya Aura<sup>®</sup> deployment 1 supports two presence domains (pres.dom.1, pres.dom.2). That is, two Avaya SIP routing domains have been defined, both of which are used to configure Avaya Presence/IM communication addresses for users in this deployment.
- Avaya Aura<sup>®</sup> deployment 2 supports two presence domains (pres.dom.3, pres.dom.4). That is, two different Avaya SIP routing domains have been defined, both of which are used to configure Avaya Presence/IM communication addresses for users in this deployment.
- The two Presence Services servers are federated. As a result, users in the Avaya Aura<sup>®</sup> deployment 1 can exchange presence and IM messages with users in Avaya Aura<sup>®</sup> deployment 2.



**\* Note:**

Presence Services does not support federation between Presence servers when **Inter-Tenant Communication Control** is enabled on System Manager.

### Related Links

[Checklist for configuring federation between Avaya Aura domains](#) on page 224

[Enabling rich Presence](#) on page 225

---

## Checklist for configuring federation between Avaya Aura<sup>®</sup> domains

XMPP federation is used to federate Avaya Aura<sup>®</sup> domains. Use the following checklist to configure XMPP federation between Avaya Aura<sup>®</sup> domains. The first six steps are required for any XMPP federation, for example, between Presence Services and an Openfire server, but the last step is specifically required for federation between Avaya Aura<sup>®</sup> domains.

No.	Task	Link	✓
1	Configure federated domains.	<a href="#">Configuring federated domains</a> on page 143	
2	Add a Server-to-Server Connection Manager component.	<a href="#">Adding a Server-to-Server Connection Manager component</a> on page 144	
3	Add an OpenPort component.	<a href="#">Adding an OpenPort component</a> on page 147	
4	Configure DNS server.	<a href="#">Configuring the DNS server</a> on page 151	
5	Verify domains are resolvable.	<a href="#">Verifying domains are resolvable</a> on page 156	
6 (Optional)	Enable logging.	<a href="#">Troubleshooting</a> on page 157	
7	Enable rich Presence.	<a href="#">Enabling rich Presence</a> on page 225	

### Related Links

[Federation between Avaya Aura domains](#) on page 224

---

## Enabling rich Presence

### Procedure

1. Log on to Presence Services XCP Controller.
2. On the Presence Services XCP Controller home page, in the **Configuration view** field, click **Advanced configuration**.
3. In the **Components** section, scroll down to the Server-to-Server Connection Manager component that you created for XMPP federation, and click **Edit**.

The system displays the Connection Manager Configuration page.

4. In the **Connection Manager Configuration > Add a New Command Processor** section, within the table identify the S2S Command Processor component that was previously created, and click **Details**.

The system displays the S2S Command Processor Configuration page.

5. In the **Director Configuration** section, click **Details** in the **Actions** column next to XMPP Outgoing Server Director.

The system displays the XMPP Outgoing Server Director Configuration page.

6. In the **XMPP Outgoing Server Director** section, in the **Enable rich presence** field, select **yes**.

7. Click **Submit**.

The system displays the S2S Command Processor Configuration page.

8. Click **Submit**.

The system displays the Connection Manager Configuration page.

9. Click **Submit**.

The system returns to the Presence Services XCP Controller web console.

10. Click **Restart the system**.

#### **Related Links**

[Federation between Avaya Aura domains](#) on page 224

# Chapter 7: Maintenance Operations

---

## Presence commands

Presence Services comes prepackaged with a number of post installation tools that support debugging and maintenance. This chapter provides information about the command line interface (CLI) as well as additional information for more complex commands.

### Related Links

- [Quick reference commands](#) on page 227
- [backup.sh tool](#) on page 229
- [restore.sh tool](#) on page 230
- [prescert tool](#) on page 232
- [swversion.sh tool](#) on page 234
- [getpslogs.sh tool](#) on page 235
- [changelP.sh tool](#) on page 235
- [updateLogLevel.sh tool](#) on page 236
- [watchers.sh tool](#) on page 237
- [configureNMS.sh tool](#) on page 238
- [generateTestAlarm.sh tool](#) on page 240
- [Using the setProductID.sh tool](#) on page 241
- [Using the getProductID.sh tool](#) on page 241
- [im\\_manager.sh tool](#) on page 241
- [Error Levels](#) on page 245

---

## Quick reference commands

The Presence CLI command table explains the CLI commands and their usage in an alphabetical order.

Command	Location	Description
<code>backup.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Backs up the existing configuration of the XCP Controller including a snapshot of the database, which would include users and archived messages.

Command	Location	Description
<code>changeIP.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Updates the Presence Services config files with the new IP, if the IP of a machine changes post Presence Services installation.
<code>configureNMS.sh</code>	<code>\$SPIRIT_HOME/scripts</code>	Sends Simple Network Management Protocol (SNMP) traps to multiple Network Management System (NMS) for each alarm.
<code>generateTestAlarm.sh</code>	<code>\$SPIRIT_HOME/scripts/utils</code>	Tests if alarms are working.
<code>getProductID.sh</code>	<code>\$SPIRIT_HOME/scripts/utils</code>	Fetches the product ID of ProductType.
<code>getpslogs.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Collects all the Presence Services related log files and creates a zip of them for inspection.
<code>im_manager.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Manages the IM database.
<code>prescert</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Provides an administration of certs for the Presence Services tool, such as creates export, import, and so on.
<code>presstatus</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Provides status of the running core processes and components in the XCP Controller.
<code>restore.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Restores a previously backed up configuration.
<code>setProductID.sh</code>	<code>\$SPIRIT_HOME/scripts/utils</code>	Sets the product ID, which identifies the installation instance.
<code>start.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Starts Presence Services, such as jabber, xcp controller, and postgres.
<code>stop.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Stops Presence Services such as jabber, xcp controller, and postgres.
<code>swversion.sh</code>	<code>/opt/Avaya/Presence/presence/bin</code>	Prints the versions of the packages that have been installed including the Presence Services and 3rd party packages.
<code>updateLogLevel.sh</code>	<code>/opt/Avaya/Presence/jabber/xcp/bin</code>	Updates dynamically the log level of the Jabber XCP components, such as increase/decrease/check log level without restarting any processes.
<code>watchers.sh</code>	<code>\$PRES_HOME/presence/bin</code>	Displays the JIDs of active users being watched by JID or the JIDs of active users watching JID.

## Related Links

[Presence commands](#) on page 227

[changeIP.sh tool](#) on page 235

## backup.sh tool

The backup, restore, and update scripts are installed in the folder, `/opt/Avaya/Presence/presence/bin`. When you install Presence Services, the system creates a temporary staging directory and a final archive directory. The staging directory is fixed at `/var/tmp/presence/backup`. During a backup procedure, `backup.sh` and its subscripts write files to the staging directory. Then `backup.sh` tars up the staging director and places the resulting file into the archive directory by default. So `backup.sh` stores an individual backup as a single compressed tar file. By default, `backup.sh` names the file using the date format (current day and time down to seconds.)

Backup stores Presence configuration files and database tables into a compressed archive file. Backup saves the archive in the archive directory if a location is not specified as a component of the filename.

### \* Note:

When you run the `backup.sh` command, the Presence server goes down.

### backup.sh [ -f<filename> ]

### \* Note:

See the `-f` option in the OPTION section below for the name of the archive. See the `PRESENCE_ARCHIVE_DIR` environment variable in the ENVIRONMENT section below for the location of the archive directory.

An archive captures the state of a Presence installation as recorded in its configuration files and databases. Once an archive is made, the state it contains can be recovered by restoring the archive (with `restore.sh`) onto an installation of Presence where the executable files are identical to those from which the archive was derived. Depending on what has happened to the Presence installation since the archive was made, recreating its previous state may involve uninstalling and reinstalling Presence, to reset the state of its executables, and then restoring the archive.

Alternatively, the update process uses the backup tool to move from one release of PS 6.0 to a later release. However, it cannot restore an archive taken from a later version of Presence to an earlier version of Presence.

## Option

**-f <filename>** Names the archive file. If you do not specify the path component then the archive will be stored in the archive directory. If you do not use the `-f` option the archive is by default named `backup_<year>_<month>_<day>_<hour>_<minute>_<seconds>.tgz` and stored in the archive directory. Ffor the location of the archive directory, see the `PRESENCE_ARCHIVE_DIR` environment variable in the ENVIRONMENT section below.

## Environment

`PRESENCE_ARCHIVE_DIR`

Sets the archive directory. If you do not set the environment variable, then the system by default sets the archive directory to `/var/presence/backup/archive`.

### Result

However, a 0 is not a completely reliable indicator of success, and you must inspect the backup log at `/var/log/presence/backup.log` for errors.

### Examples

#### Assuming `PRESENCE_ARCHIVE_DIR` is unset

- `backup.sh` (run on 16 November 2009 at 1:05:43 PM)  
Creates `/var/presence/backup/archive/backup_2009_11_16_13_05_43.tgz`.
- `backup.sh -f ./elvis.tgz`  
Creates `elvis.tgz` in the current directory.

#### Assuming `PRESENCE_ARCHIVE_DIR` is set to `"/tmp"`

- `backup.sh` (run on 16 November 2009 at 1:05:43 PM)  
Creates `/tmp/backup_2009_11_16_13_05_43.tgz`.
- `backup.sh -f ./elvis.tgz`  
Creates `elvis.tgz` in the current directory.

### Related Links

[Presence commands](#) on page 227

---

## restore.sh tool

### \* Note:

As a prerequisite, you must first stop the Presence server before performing a restore.

**Restore** recovers the Presence configuration files and database tables from a compressed archive file. The system looks for the archive in the default directory if a location is not specified as a component of the filename.

**restore.sh** [ `-f <filename>` ]

### \* Note:

See the `-f` option in the *Option* section for the name of the archive. For the location of the archive directory, see the `PRESENCE_ARCHIVE_DIR` environment variable in the *Environment* section.

An archive captures the state of a Presence Services installation as recorded in the configuration files and databases of the Presence server. You can rollback Presence Services to the previous state by restoring to an older installation of Presence. However, the executable files must be identical to those from which the archive was derived.

Depending on what has happened to the Presence installation since the archive was made, you might have to recreate the previous state of Presence Services. This might involve reinstalling

Presence Services, to reset the state of its executables, and then restoring the archive. You can also restore an archive to a later version of Presence Services if permitted by the `restore.sh` of that later version. This process allows the configurations to migrate with upgrades and patches.

An archive taken from a later version of Presence Services cannot be restored to an earlier version of Presence Services.

Use `restore.sh` to restore a valid FROM version to a valid TO version of Presence Services. A valid FROM is a version from which you upgrade or rollback Presence Services, while a valid TO is a version to which you downgrade or upgrade Presence Services. `restore.sh` migrates data automatically, even between releases. For example, upgrade FROM 6.1.5 TO 6.2.0 is supported, but an upgrade FROM 6.1.0 to 6.2.0 is not supported. For more information about the supported upgrades, see the latest release notes on the Avaya Support Web site at, <http://support.avaya.com>.

When run without any options, `restore.sh` displays the state of the `PRESENCE_ARCHIVE_DIR` environment variable and lists the contents of the archive directory.

## Options

- f <filename>** This option is mandatory. You must name the archive file that you want to restore. If you do not specify the path component then the system assumes that the archive resides in the archive directory. If you run `restore.sh` without any options, the system displays the name of the archive directory and the contents of the archive directory. You can use the `PRESENCE_ARCHIVE_DIR` environment variable to specify the archive directory.

## Environment

`PRESENCE_ARCHIVE_DIR`

Sets the archive directory. If you do not set an environment variable, then the system sets the archive directory to `/var/presence/backup/archive` by default. If you do not include a directory component along with the `-f` option, then `restore.sh` looks for the file in the archive directory.

The transient settings of this environment variable are ineffective. The installation and archiving scripts ignore the variables unless sourcing `/etc/profile` sets it.

## Exit Status

Returns 0 on success, something else on error. A return of 0 is not a completely reliable indicator of success. You must inspect the log file `/var/log/presence/backup.log` for errors.

## Example

Assuming `PRESENCE_ARCHIVE_DIR` is unset

- `restore.sh` — Displays that the name of the archive directory is `/var/presence/backup/archive` and displays its contents.
- `restore.sh -f elvis.tgz` — Restores `/var/presence/backup/archive/elvis.tgz`.
- `restore.sh -f ./elvis.tgz` — Restores `elvis.tgz` in the current directory.

Assuming `PRESENCE_ARCHIVE_DIR` is set to `/tmp`

- `restore.sh` — Displays that the name of the archive directory is `/tmp` and displays its contents.

- `restore.sh -f backup_2009_11_16_13_05_43.tgz` — Restores `/tmp/backup_2007_11_16_13_05_43.tgz`.
- `restore.sh -f ./backup_2009_11_16_13_05_43.tgz` — Restores `backup_2009_11_16_13_05_43.tgz` in the current directory.

## Related Links

[Presence commands](#) on page 227

---

## prescert tool

Use the `prescert tool` to manage the local Presence Services keystore. The Presence Services installation uses the `prescert` tool to retrieve the required certificates from the System Manager server. You can also use the tool after the installation for adding and removing certificates. Additionally, using the `prescert` tool you can view the various `prescert` tool commands and specify the SCEP password. You must execute the command as a root user.

### Syntax

```
prescert <command>[PEM<PEM file>] [ALIAS<Keystore alias>]
```

```
./prescert
```

### Description

Presence Services supports any (valid) trusted certificate, for example it supports the following interfaces:

- SIP
- XMPP
- Microsoft OCS
- System Manager (RMI and Web services)
- AES

By default, Presence Services uses a single key certificate, which the Trust Management services within System Manager generates. Presence Services uses the following trust certificates:

- The Avaya SIP certificate, which is used for trusting Avaya SIP elements, such as Avaya Aura<sup>®</sup> Session Manager.
- The Avaya Aura<sup>®</sup> System Manager enterprise certificate.
- Avaya Product Root CA certificate

You can import additional trust certificates. For example, a certificate for interoperability with Microsoft OCS.

### Considerations

Insert any considerations that the user be made aware of.

### Files

Files are located in `/opt/Avaya/Presence/presence/bin`.

**Related Links**

[Presence commands](#) on page 227

[Specifying SCEP password using prescert tool](#) on page 233

[Command summary](#) on page 233

**Specifying SCEP password using prescert tool****Procedure**

1. Log in to the Presence server as a root user.
2. At the command prompt, type `cd $PRES_HOME/presence/bin` to go to the bin directory.
3. At the command prompt, in the `$PRES_HOME/presence/bin` directory, type `./prescert reconfigureAll scep pw xxx`, where `xxx` is the SCEP password.
4. To update the new configuration, restart Presence Services.

**Related Links**

[prescert tool](#) on page 232

**Command summary**

The following table provides the list of commands that can be used to administer certificates and keys for Presence Services.

Command	Description
Create	Load new server and CA certificates into the local JKS keystore
delete alias <alias-name>	Delete an alias from the JKS keystore
delete pem <pem-file-path>	Delete a PEM file from the hard disk
refresh alias <alias-name>	Execute the create command if the alias in the JKS keystore is out of date
verify alias<alias-name>	Check an alias in the JKS keystore for expiration
verify pem <pem-file-path>	Check a PEM file on the hard disk for expiration
import pem <pem-file-path>	Import a PEM file into the JKS keystore
export alias <alias-name>	Extract the server private key and certificate from the JKS keystore to PEM files
exportTS <pem-file-path>	Extract trusted certificates from the JKS truststore to an PEM file with a generated filename in the <code>/opt/Avaya/Presence/jabber/xcp/certs</code> directory
list	List the contents of the JKS keystore
status	Generate certificate status information from the JKS keystore into <code>/opt/Avaya/Presence/jabber/xcp/etc/ps-certs.csv</code> for use by the <code>presstatus</code> tool
reconfigureAll	Create the JKS keystore and PEM files

Command	Description
verifyCertificates	Verify the certificates in the PEM files to ensure they are still in date
addTrusted pem <pem-file-path> [alias <alias-name>]	Add a trusted certificate to the JKS keystore and trust PEM file
removeTrusted alias <alias-name>	Remove a trusted certificate from the JKS keystore and trust PEM file

### Related Links

[prescert tool](#) on page 232

---

## swversion.sh tool

The `swversion.sh` tool is used to view the version of the Presence Services application and the embedded packages.

### Syntax

```
[./swversion.sh]
```

### Description

The `swversion.sh` is used to view the versions of the software installed by the Presence Services installation. You must execute the command as a root user.

### Example

The following example shows a command that is used to view the versions of software. `cd /opt/Avaya/Presence/presence/bin`

```
./swversion.sh
```

### \* Note:

To view all the available commands, use `./swversion.sh - -help`.

### Example Output

```
[root@ips23-105 bin]# ./swversion.sh --help
Usage: swversion.sh [ -a | --all | -v | --verbose | -q | --quiet |
-? | --help]
```

### Files

Files are located in `/opt/Avaya/Presence/presence/bin`.

### Related Links

[Presence commands](#) on page 227

---

## getpslogs.sh tool

Use the `getpslogs.sh` command tool to gather all the required logs from the Presence server. You can then archive all the logs and create a zip file for a specified range of days. The default number of days (duration) for the logs is set as to 7. These logs, in turn, help the Presence Services support team to troubleshoot problems.

### Related Links

[Presence commands](#) on page 227

[Using the getpslogs.sh tool](#) on page 235

## Using the getpslogs.sh tool

### Procedure

1. Log in to the Presence server as a root user.
2. Go to the `/opt/Avaya/Presence/presence/bin` directory.
3. Run the command `./getpslogs.sh`.

The system archives the logs from `/var/log`, `/var/lib/pgsql/data/pg_log` and `opt/Avaya/Presence/jabber/xcp/var/log/` and generates the output.

### Related Links

[getpslogs.sh tool](#) on page 235

---

## changeIP.sh tool

### About this task

Using this tool, you can change the IP address stored in the Presence Services configuration files. You must execute the command as a root user. Change the IP address of the server (network interface) manually. The `changeIP.sh` script only changes the IP addresses within the Presence Services product.

### Procedure

1. Log in to the Presence server as a root user.
2. Stop Presence Services by using the `/opt/Avaya/Presence/presence/bin/stop.sh` command.

#### Warning:

Before you proceed, verify that Presence Services has been stopped. To verify, use the `monit summary` command.

3. Change the IP address of the server manually by using the `vi /etc/sysconfig/network-scripts/ifcfg-eth0` command.

4. Modify the IPADDR field with the new IP address and then save the file.
5. Restart network service by using the `service network restart` command. If you are using a remote shell session, you will lose the session on this IP.
6. Using a remote shell session, restart another session with the new IP.
7. Go to the bin folder. For example: `cd /opt/Avaya/Presence/presence/bin.`
8. At the command prompt, type `./changeIP.sh<old IP address><new IP address>`. Presence Services starts automatically after you make the changes.  
For more information, see *Quick reference commands*.
9. Log in to Presence Services Web Controller and verify that all the services are in a running state.

### Related Links

[Presence commands](#) on page 227

[Quick reference commands](#) on page 227

---

## updateLogLevel.sh tool

Using the `updateLogLevel.sh` command line tool you can update or check the log level of Presence Services XCP Components dynamically without restarting Presence Services. You can verify the log level of the component by selecting various options, such as increase, decrease, or check.

### Syntax

By default, the system can dynamically update log level of the following components:

cm-1	Connection Manager
cm-2	OCS Connection Manager
sip-ps-1	SIP Presence Server
sip-proxy-1	SIP Proxy
sip-bulksub-1	SIP Bulk Subscription Server
CORE-ROUTER	Core Router

The following command arguments are available for the components:

increase	-i   --increase
decrease	-d   --decrease
check	-c   --check

### Related Links

[Presence commands](#) on page 227

[Using the update log level tool](#) on page 237

## Using the update log level tool

### Procedure

1. Log in to the Presence server as a root user.
2. Go to the `/opt/Avaya/Presence/jabber/xcp/bin` directory.
3. At the command prompt, type the command, `./updateLogLevel.sh`

For example, Connection Manager is `cm-1` in a default installation.

- a. To increase the log level of the Connection Manager, at the command prompt, type `./updateLogLevel.sh cm-1 -i`
- b. To decrease the log level of the Connection Manager, at the command prompt, type `./updateLogLevel.sh cm-1 -d`
- c. To check the log level of the Connection Manager, at the command prompt, type `./updateLogLevel.sh cm-1 -c`

### Example Output

```
[localhost]# ./updateLogLevel.sh cm-1 -i
cm-1 is now logging at level (WARNING)
```

### Related Links

[updateLogLevel.sh tool](#) on page 236

---

## watchers.sh tool

Using the **watchers.sh** command line tool, you can display the JIDs of active users being watched by JID or the JIDs of active users watching JID.

### Syntax

`./watchers.sh`

<code>./watchers.sh --watching &lt;jid&gt;</code>	Displays the JIDs of active users being watched by JID.
<code>./watchers.sh --watched &lt;jid&gt;</code>	Displays the JIDs of active users watching JID.
<code>./watchers.sh [ --help   -help   -? ]</code>	Displays this help page.

### Related Links

[Presence commands](#) on page 227

[Using the watchers.sh tool](#) on page 237

## Using the watchers.sh tool

### Procedure

1. To display JIDs of active users being watched by JID:
  - a. Log in to the Presence server as a root user.

- b. At the command prompt, type `cd $PRES_HOME/presence/bin` to go to the bin directory.
- c. At the command prompt, in the `$PRES_HOME/presence/bin` directory, type `./watchers.sh --watching <jid>`.

For example, SIP client, `user700000@pres.reg.avaya.com`, subscribes to `user700001@pres.reg.avaya.com`. To check who is watched by `user700000@pres.reg.avaya.com`, type `user700000@pres.reg.avaya.com` for the `<jid>` in the above command.

#### Output

```
user700000@pres.reg.avaya.com is watching
  user700001@pres.reg.avaya.com      1 subscriptions
1 users and 0 rosters
```

2. To display JIDs of active users watching JID:

- a. Log in to the Presence server as a root user.
- b. At the command prompt, type `cd $PRES_HOME/presence/bin` to go to the bin directory.
- c. At the command prompt, in the `$PRES_HOME/presence/bin` directory, type `./watchers.sh --watched <jid>`.

For example, SIP client, `user700000@pres.reg.avaya.com`, subscribes to `user700001@pres.reg.avaya.com`. To check who is watching `user700001@pres.reg.avaya.com`, type `user700001@pres.reg.avaya.com` for the `<jid>` in the above command.

#### Output

```
Users watching user700001@pres.reg.avaya.com
  istdistributor@pres.reg.avaya.com  1 subscriptions
  user700000@pres.reg.avaya.com     1 subscriptions
2 watchers
```

### Related Links

[watchers.sh tool](#) on page 237

---

## configureNMS.sh tool

Using Presence Services, you can send Simple Network Management Protocol (SNMP) traps to multiple Network Management System (NMS) for each alarm. To enable this, Presence Services uses the System Manager spiritAgent. By default, Presence Services does not configure NMS.

### Syntax

```
./configureNMS.sh
```

### Related Links

[Presence commands](#) on page 227

[Using the configureNMS.sh tool](#) on page 239

[Testing SNMP Trap/Alarm](#) on page 240

## Using the configureNMS.sh tool

### About this task

You can run the `./configureNMS.sh` command directly from the command line as follows:

### Procedure

1. To add the NMS:
  - a. Log in to the Presence server as a root user.
  - b. At the command prompt, type `cd $SPIRIT_HOME/scripts` to go to the scripts directory.
  - c. At the command prompt, in the `$SPIRIT_HOME/scripts` directory, type `./configureNMS.sh [IP] [Port] [Community]`. For example, `./configureNMS.sh 10.0.0.2 162 public`.  
  
The system displays the Entry for IP Address 10.0.0.2 added successfully message.
  - d. Restart the spiritAgent service using the `# service spiritAgent restart` command.
2. To remove the NMS:
  - a. Log in to the Presence server as a root user.
  - b. At the command prompt, type `cd $SPIRIT_HOME/scripts` to go to the scripts directory.
  - c. At the command prompt, in the `$SPIRIT_HOME/scripts` directory, type `./configureNMS.sh -r [IP] [Port]`. For example, `./configureNMS.sh -r 10.0.0.2 162`.  
  
The system displays Entry for IP address 10.0.0.2 removed successfully.
  - d. Restart the spiritAgent service using the `# service spiritAgent restart` command.
3. To list all the configured NMS systems:
  - a. Log in to the Presence server as a root user.
  - b. At the command prompt, type `cd $SPIRIT_HOME/scripts` to go to the scripts directory.
  - c. At the command prompt, in the `$SPIRIT_HOME/scripts` directory, type `./configureNMS.sh -l`.  
  
The system displays the configured NMS systems.

### Related Links

[configureNMS.sh tool](#) on page 238

## Testing SNMP Trap/Alarm

### Procedure

1. Log in to System Manager Web Console.
2. On System Manager Dashboard, under **Services**, click **Events**.
3. On the Events page, click **Alarms** in the left navigation pane.

The system displays the alarms on the Alarming page. You can view the details of the alarm.

### Related Links

[configureNMS.sh tool](#) on page 238

---

## generateTestAlarm.sh tool

The generate test alarm command is used to test if alarms are working. Using the generate test alarms command you can ensure whether the Presence Systems are running properly. Later, you can clear the generated test alarm.

### Syntax

<code>./generateTestAlarm.sh</code>	Generates Test Alarm
<code>./generateTestAlarm.sh -c</code>	Clears Test Alarm

### Related Links

[Presence commands](#) on page 227

[Using the generateTestAlarm.sh tool](#) on page 240

## Using the generateTestAlarm.sh tool

### Procedure

1. Log in to thePresence server as a root user.
2. At the command prompt, type `cd $SPIRIT_HOME/scripts/utils` to go to the utils directory.
3. At the command prompt, in the `$SPIRIT_HOME/scripts/utils` directory, type `./generateTestAlarm.sh`.  
The Test Alarm is generated.
4. To clear the Test Alarm, use the `./generateTestAlarm.sh -c` command.

### Example Output

```
[root@ips23-105 utils]# ./generateTestAlarm.sh
Test alarm generated.
[root@ips23-105 utils]# ./generateTestAlarm.sh -c
Clear event for test alarm generated.
```

### Related Links

[generateTestAlarm.sh tool](#) on page 240

---

## Using the setProductID.sh tool

### Procedure

1. Log in to the Presence server as a root user.
2. At the command prompt, type `cd $SPIRIT_HOME/scripts/utils` to go to the utils directory.
3. At the command prompt, in the `$SPIRIT_HOME/scripts/utils` directory, type `./setProductID.sh PS [ProductID]`.
4. Restart the spiritAgent service using the `# service spiritAgent restart` command.

### Related Links

[Presence commands](#) on page 227

---

## Using the getProductID.sh tool

### Procedure

1. Log in to the Presence server as a root user.
2. At the command prompt, type `cd $SPIRIT_HOME/scripts/utils` to go to the utils directory.
3. At the command prompt, in the `$SPIRIT_HOME/scripts/utils` directory, type `./getProductID.sh PS [ProductID]`.

For example, if the product ID is 2244668800, then the system displays [2244668800] for [ProductID].

### Related Links

[Presence commands](#) on page 227

---

## im\_manager.sh tool

The `im_manager` script is installed in the folder `/opt/Avaya/Presence/presence/bin`. The `im_manager` manages the IM Transcripts database.

The `im_manager` is a stand-alone command line tool to manipulate the Instance Message (IM) Archive database. You can use the tool to:

- View the size of the IM database
- Backup the IM database
- Restore the IM database
- Purge old data from the IM database

You can run the `im_manager` in the following modes:

- **Interactive mode.** You can use a menu to run specific actions.
- **Command line mode.** You can run command line arguments to perform specific actions. This allows you to automatically schedule backups and purges of the database.

### Related Links

[Presence commands](#) on page 227

[Using Interactive mode](#) on page 242

[Using Command line mode](#) on page 245

## Using Interactive mode

### About this task

You can use `im_manager` without any command line arguments.

### Procedure

1. Open an SSH session using PuTTY and log in to the Presence server as a root user.
2. At the command prompt, type `/opt/Avaya/Presence/presence/bin/im_manager.sh`.

The system opens the IM Transcripts Web Services Manager interface and displays the following options:

- a. Database size
- b. Backup database
- c. Restore database
- d. Purge database
- e. Quit

```
IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

█
```

3. Enter **1**.

The system returns the number of records in the database. For example:

```

IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

1
IM Transcripts database contains 0 records.
Press return...
█

```

4. Enter **2**.

The system writes a file to the users' home directory (on Presence Services) with the complete contents of the IM Archive database. The file includes a date/time stamp so that old backups are not over written. For example:

```

IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

2
Enter directory to write backup [/root]
Backing up DB: /root/im_database_2013-05-03_14.00.18.dump
  - please wait
0 records backed up.
Press return...
█

```

5. Enter **3**.

The system takes one of the archive files created by the backup tool and adds all the messages into the database. For example:

```
IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

3

Enter filename of dumped database, or empty string to return to menu

No dump file entered.
Press return...
█
```

6. Enter 4.

The system removes old messages from the database. You must tell the tool which records it should keep based on the age of the message in full days. For example:

```
IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

4

Enter number of days worth of records to keep.
 1 will keep only todays records
 0 will remove all records
 Empty string will return to menu
0
0 records removed.
Press return...
█
```

7. Enter 0.

The system quits the IM Transcripts Web Services Manager interface. For example:

```
IM Transcript Web Service Manager

1) Database size
2) Backup database
3) Restore database
4) Purge database
0) Quit

0
[root@ps-gis bin]#
```

### Related Links

[im\\_manager.sh tool](#) on page 241

## Using Command line mode

### About this task

You can also run `im_manager` directly from the command line. Using Command Line Interface, other scripts or scheduling utilities can automatically back up and/or purge the database. For example, cron.

### Related Links

[im\\_manager.sh tool](#) on page 241

---

## Error Levels

The system may return some of these values.

- 0 - No error
- 1 - Syntax error
- 2 - Help displayed
- 3 - Missing file
- 4 - IO error
- 5 - Command failed
- 6 - Postgres not running
- 99 - Internal error

### Related Links

[Presence commands](#) on page 227

---

## Changing the System Manager hostname on Presence Services

### About this task

Perform this task when you change the hostname of your System Manager.

### Procedure

1. Log in to the Presence server as a root user.
2. Ensure that the new System Manager hostname is resolvable on Presence Services.
3. To resolve the hostname, using the FQDN, ping System Manager from the Presence server and then ping Presence Services from the System Manager server.
4. Alternately, you can add the hostname entry in the `/etc/hosts` file. For example, `<System Manager IP> <System Manager FQDN> <System Manager Short Hostname>`.
5. Stop the DRS service on Presence server by performing the following commands: 

```
# monit stop drs# service drs stop
```
6. Execute the `changeSMGR.sh` script located under `$PRES_HOME/install/scripts/`. For example, 

```
# ./changeSMGR.sh <new hostname of System Manager ><ws port><naming port><login><password><enroll password>
```
7. Wait till Presence replica reaches the synchronized state. To verify the synchronized state, see the Replication section in System Manager Web Console.
8. Verify the following changes:
  - a. To test the alarm on the Presence server, use the `generateTestAlarm.sh` command, located under `$SPIRIT_HOME/scripts/utils`.
  - b. To test the alarms System Manager, log in to System Manager Web Console as an administrator, and select the **Events/Alarm** section.

 **Note:**

Changing System Manager hostname means only changing the hostname of System Manager on Presence Services and not replacing the System Manager server.

### Related Links

[Updating Presence Services entity link in Session Manager](#) on page 246

[Updating client configuration](#) on page 247

---

## Updating Presence Services entity link in Session Manager

### About this task

If you have configured SIP entities for Presence Services on System Manager, then modify those SIP entities as follows:

## Procedure

1. Log in to System Manager Web Console.
2. On System Manager Dashboard, click **Elements > Routing > SIP Entities**.
3. On the SIP Entities page, if the system displays Presence Services, click it in the **Name** column.

The system displays the SIP Entity Details page.

4. On the SIP Entity Details page, change the SIP Entity IP address to the new IP address, then click **Commit**.

## Related Links

[Changing the System Manager hostname on Presence Services](#) on page 246

---

## Updating client configuration

### About this task

Configure the client, such as Avaya one-X<sup>®</sup> Communicator, to use new Presence IP address as follows:

### Procedure

1. On the General Settings dialog box of Avaya one-X<sup>®</sup> Communicator, select **IM and Presence** on the left pane.
2. Select the **Enable Instant Messaging and Presence** check box.
3. In the **Server** field, enter the IP address of IM and Presence server.
4. Click **OK**.

## Related Links

[Changing the System Manager hostname on Presence Services](#) on page 246

---

## Monit

A service called monit regulates and monitors the activities of a number of services in Presence Services. You can access monit using a Web GUI or using a command line interface (CLI).

Monit starts, stops, and monitors the following services in Presence Services:

- xcp\_sip\_proxy
- xcp\_presence\_model
- xcp\_presence\_container
- spiritAgent
- log-harvester

- postmaster (PostgreSQL server)
- drs (Data Replication Service)
- jabberd
- cm (Extensible Communication Platform (XCP) Web page)
- tomcat

Under normal operating conditions, the monit service starts as soon as Presence Services starts. Monit monitors these services using a heartbeat method. Monit takes certain dependencies into account. This means that if Service A depends on Service B, monit starts Service B before starting Service A. The dependencies result in a controlled start-up order.

The dependencies are as follows:

- spiritAgent depends on log-harvester
- log-harvester depends on jabberd
- jabberd depends on postmaster & DRS
- DRS depends on postmaster

Postmaster, tomcat, and cm do not depend on any other service. Monit can start Tomcat and cm without affecting another service on the system. If monit restarts DRS, then monit stops postmaster, log harvester, and spiritAgent. As soon as DRS has started and is running, monit starts postmaster, jabberd, log harvester, and spiritAgent.

In addition to these services, monit monitors the following services in Presence Services, but does not directly start and stop them. The stop/start status of jabberd determines their stop/start status:

- xcp\_connection\_manager
- xcp\_sip\_proxy
- xcp\_presence\_model
- xcp\_presence\_container

Monit can also monitor a number of ports:

- 5432 for postmaster
- 7400 for jabberd
- 7430 for webcam

Monit saves logs to the `/var/log/messages` folder on the Presence server. A configurable filter called log-harvester determines which events should trigger an alarm and which events it should simply log as regular activity.

### Related Links

[Viewing monit using a CLI](#) on page 249

[Suspending and restarting the monitoring of a service](#) on page 249

---

## Viewing monit using a CLI

### About this task

Using the Presence server CLI, you can view a summary list of the status of all the monitored processes. Using the CLI, you can also display more detailed information about individual monitored processes.

### Procedure

1. To display a summary, type `monit summary`.
2. To display details, type `monit status`.

### Related Links

[Monit](#) on page 247

---

## Suspending and restarting the monitoring of a service

### About this task

If you need to perform an administration task on one of the monitored services, such as the PostgreSQL server, you must stop the monitoring of the service, perform the administration task, and then restart the monitoring of the service. If you do not stop the monitoring, monit continues to attempt to restart the service when it is offline for the maintenance. You can stop the monitoring of a service using the Presence server CLI.

### Procedure

1. To suspend the monitoring of a service, for example, `postgres: monit stop postgres`.
2. To restart the monitoring of a service, for example, `postgres: monit start postgres`.

### Related Links

[Monit](#) on page 247

---

## Checking your Presence Services license status

### Before you begin

To log in to the command line interface (CLI) on the Presence server or to view and edit a file on the Presence server, you must use a terminal emulator application such as PuTTY. PuTTY is a Windows SSH client. Using PuTTY, you can gain access to Windows virtual machines. You can download PuTTY from <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

## Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to obtain root access.
2. On the command prompt, type `$PRES_HOME/presence/bin/presstatus`.
3. Press `Enter`.

---

# Network parameters

---

## Network parameters overview

When you install a new Presence server, you must configure the network parameters to ensure that the new Presence server work with the other devices and end points in the network. To make the devices and end points that the server integrates with work successfully, you must change the following network parameters:

- Primary DNS
- Default gateway
- Domain search list
- Default netmask
- Presence Services IP address
- Presence Services hostname

Network parameters control the interaction of all devices, such as communication ports. When you set the network parameters, you can enable secure network access using options, such as SSL and intercache communication. You can modify the network parameter configuration using the System Platform Web interface.

---

## Configuring network parameters

### Changing primary DNS

#### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.
3. On the Server Management page, in the **General Network Settings** section, change the value of primary DNS in the **Primary DNS** field. For example, change `135.64.21.5` to `135.64.21.33`.

4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

## Verifying the primary DNS changes

### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. To verify the changes, go to `/etc/resolv.conf`. For example, at the command prompt, type `more /etc/resolv.conf`. The system displays the new primary DNS value, for example, `nameserver 135.64.21.33`.

## Changing the default gateway

### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.
3. On the Server Management page, in the **General Network Settings** section, change the value of the default gateway in the **Default Gateway** field. For example, change `135.64.21.1` to **135.64.21.3**.
4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

## Verifying the default gateway changes

### Procedure

1. Log in to the Presence Services server as a cust user, and then use the `su` command to change to root.
2. To verify the changes, go to the `/etc/sysconfig.network-scripts/ifcfg-eth0` file. For example, at the command prompt, type `more /etc/sysconfig.network-scripts/ifcfg-eth0`. The system displays the new default gateway IP address.

## Changing the domain search list

### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.

3. On the Server Management page, in the **General Network Settings** section, change the value of the domain search list in the **Domain Search List** field. For example, change `du.rnd.avaya.com` to `ga.rnd.avaya.com`.
4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

## Verifying the domain search list changes

### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. To verify the changes, go to the `/etc/resolv.conf` file. For example, at the command prompt, type `more /etc/resolv.conf`. The system displays the new domain search list value, for example, `search ga.rnd.avaya.com`.

## Changing the default netmask

### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.
3. On the Server Management page, scroll to **Domain Network Interface > Domain-0 > avpublic**. For the avpublic bridge, change the **Netmask** field. For example, change `255.255.255.0` to `255.255.254.0`.
4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

## Verifying the default netmask changes

### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. To verify the new changes, go to the `/etc/sysconfig/network-scripts/ifcfg-eth0` file. For example, at the command prompt, type `more /etc/sysconfig/network-scripts/ifcfg-eth0`. The system displays the new default netmask value.

## Changing the Presence Services IP address

### Before you begin

Ensure that the new IP address of Presence Services is resolvable by System Manager. You can do this by adding the new Presence Services IP address to the `/etc/hosts` file on the System Manager Web interface or on the DNS server.

## Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.
3. On the Server Management page, scroll to **Template Network Configuration > Global Template Network Configuration > IP address of the presence\_va**. Change the IP address of Presence by changing the value of the **IP address of the presence\_va** field. For example, change 135.64.21.137 to 135.64.21.166.
4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

## Next steps

### Note:

After you change the Presence Services IP address, you must modify all the clients using the Presence Services IP to use the new Presence Services IP address and restart the system, if required. Also, you must modify all the Presence Services SIP Entity links with the new Presence Services IP address.

## Verifying the Presence Services IP address changes

### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. To verify the changes, go to `/etc/sysconfig/network-scripts/ifcfg-eth0`. For example, at the command prompt, type `vi /etc/sysconfig/network-scripts/ifcfg-eth0`. The system displays the new Presence Services IP address value.

## Testing the Presence Services IP address changes

### Test 1: Checking the components

#### Procedure

1. Log in to the Presence Services XCP Controller Web interface, for example, `https://<Presence Services IP Address>:7300/admin`.
2. Scroll down to the **Components** section and ensure that all the Presence components are running.

### Test 2: Checking the test alarms

#### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.

2. To verify that the system receives the test alarms, go to: `$SPIRIT_HOME/scripts/`  
`utils/`
3. Run the script, `./generateTestAlarm.sh`.
4. Log in to System Manager Web Console. On the Home page, click **Events > Alarming** and check if the system receives test alarms.

### Test 3: Checking the replication

#### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the Home page, click **Services > Replication**. On the Replication page, under Replica nodes, wait till the system acquires a synchronized status for the Presence replica. The replication is working correctly if the system acquires a synchronized state.

For more information on SIP Entity links, see *Administering Avaya Aura® Presence Services*.

## Presence Services hostname changes

### Changing the Presence Services hostname on the System Platform deployments

#### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the System Platform dashboard, click **Server Management > Network Configuration**.
3. On the Server Management page, scroll to **Template Network Configuration > Global Template Network Configuration > presence\_va hostname**. Change the Presence hostname by changing the value of the **presence\_va hostname** field. For example, change `pssv21167.du.rnd.avaya.com` to `pssv21166.du.rnd.avaya.com`.
4. Click **Save**. The system displays the **Changing network settings may require you to login again into web console. Are you sure?** dialog box.
5. Click **OK** to confirm.

### Changing the Presence Services hostname in the non-System Platform deployments

#### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. At the command prompt, type `$PRES_HOME/presence/bin/changePSFQDN.sh`.
3. To view the logs, type `more /opt/Avaya/Presence-VA/psva/ps-sp-utils/SPchangeParam.log`.

## Testing the Presence Services IP address changes

### Test 1: Checking the components

#### Procedure

1. Log in to the Presence Services XCP Controller Web interface, for example, `https://<Presence Services IP Address>:7300/admin`.
2. Scroll down to the **Components** section and ensure that all the Presence components are running.

### Test 2: Checking the test alarms

#### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. To verify that the system receives the test alarms, go to: `$SPIRIT_HOME/scripts/Utils/`
3. Run the script, `./generateTestAlarm.sh`.
4. Log in to System Manager Web Console. On the Home page, click **Events > Alarming** and check if the system receives test alarms.

### Test 3: Checking the replication

#### Procedure

1. Log in to the System Platform Web interface as an administrator, for example, `https://<console domain IP address>/webconsole`.
2. On the Home page, click **Services > Replication**. On the Replication page, under Replica nodes, wait till the system acquires a synchronized status for the Presence replica. The replication is working correctly if the system acquires a synchronized state.

For more information on SIP Entity links, see *Administering Avaya Aura® Presence Services*.

## Reconfiguring the LPS client

#### Procedure

1. Log in to the Presence server as a cust user and then use the `su` command to change to root.
2. Take a backup of LPS client file `generic.keystore.jks`.
3. Replace the LPS client `generic.keystore.jks` file with the `generic.keystore.jks` of Presence Services, which is located under `$PRES_HOME/jabber/xcp/certs/`.
4. Update the hostname name entry in the LPS `.properties` file with the new hostname value.

## Reconfiguring the SIP Tester client

#### Procedure

1. In the SIP tester client, take a backup of `generic.keystore.jks` file.

2. Replace the SIP tester generic.keystore.jks file with the generic.keystore.jks of Presence Services, located under `$PRES_HOME/jabber/xcp/certs/`.

## Reconfiguring OCS

To complete the reconfiguration for OCS, perform the following steps:

1. Modifying the Presence server CA certificate to the Microsoft Edge Server Trusted Root certificates
2. Modifying the OCS Edge IM service provider
3. Adding New Host (A)
4. Modifying the SRV record for new hostname
5. Modifying a reverse pointer
6. Testing DNS records from Microsoft Edge Server
7. Restart the OCS Edge server

### Related Links

[Modifying the Presence server CA certificate to Microsoft Edge Server Trusted Root certificates](#) on page 256

[Modifying the OCS Edge IM service provider](#) on page 257

[Adding New Host \(A\)](#) on page 195

[Modifying the SRV record for a new hostname](#) on page 258

[Modifying a reverse pointer](#) on page 258

[Testing DNS records from Microsoft Edge Server](#) on page 258

### ***Modifying the Presence server CA certificate to Microsoft Edge Server Trusted Root certificates***

#### **Procedure**

1. On the Presence Services server, locate the certificate with a name similar to export-xxx.trusts in the `$PRES_HOME/jabber/xcp/certs` directory. and copy to the Microsoft Edge server.
2. Copy the export-xxx.trusts certificate to the Microsoft Edge server.
3. Import the new hostname certificates in Edge Server to Microsoft . To do so, perform the following:
  - a. Click **Start > Run**.  
The system displays the management console window.
  - b. Open Certificates Snap-in for Edge Server
  - c. Open Certificates/Trusted Root Certification Authorities/Certificates.
  - d. Remove the certificate may display as Default.
4. Import the new hostname certificates in Edge Server to Microsoft
  - a. Open Certificates Snap-in for Edge Server

- b. Open Certificates/Trusted Root Certification Authorities/Certificates.
- c. In the left-hand pane, click **All Tasks > Import**.

The system launches the Certificate Import Wizard. Follow the steps of the Wizard and browse for the export-xxx.trusts file you copied in the earlier steps.

- d. Verify that the copied certificate is in the Certificates/Trusted Root Certification Authorities/ Certificates list. You may need to use the refresh button to update the list. The certificate may display as Default.

### Related Links

[Reconfiguring OCS](#) on page 256

### *Modifying the OCS Edge IM service provider*

#### Procedure

1. Click **Start > All Programs > Administrative Tools > Computer Management**.

The system displays the Computer Management window.

2. In the left navigation pane, expand **Services and Applications** and then select **Microsoft Office Communications 2007**.
3. Right-click **Microsoft Office Communications 2007** and then click **Properties**.
4. On the **IP Provider** tab, click **Edit**.
5. In the **Network address of the IM service provider Access Edge** field, enter the new Presence Services FQDN.
6. Click **OK**.

### Related Links

[Reconfiguring OCS](#) on page 256

### *Adding New Host (A)*

#### Procedure

1. On the OCS DNS server, right-click the domain that you just created and select **New Host (A)**.
2. In the New Host dialog box, enter the Presence server name and IP address. For example, `ipsdemo-ips1.ipsdemo.com`.
3. Click **Add Host > Done**.

#### **Note:**

When you add New Host (A) in DNS, check the associated pointer. This associated pointer may eliminate the need to add the machine name to the Reverse Lookup Zone if that zone already exists.

### Related Links

[Reconfiguring OCS](#) on page 256

### ***Modifying the SRV record for a new hostname***

#### **Procedure**

1. Log in to the OCS DNS server.
2. In the **Service** field, enter `_sipfederationtls`.
3. In the **Port number** field, enter `5061`.
4. In the **Host offering this service** field, enter the FQDN of the new Presence Service server hostname.

For example, `chat.pres.test.com` or `chat.example.com` for the two example domains given earlier.

5. Click **OK** and then click **Done**.

#### **Related Links**

[Reconfiguring OCS](#) on page 256

### ***Modifying a reverse pointer***

#### **Procedure**

1. On the OCS DNS server, in the left navigation pane, select **Reverse Lookup Zones > New Zone**.
2. Right-click on **Reverse Lookup Zone**.
3. Find the Pointer (PTR) record for the IP address of Presence server.
4. Double click the Pointer (PTR) record for the IP address of the Presence server, change the value in the Host name field with the new hostname of the Presence server.

#### **Related Links**

[Reconfiguring OCS](#) on page 256

### ***Testing DNS records from Microsoft Edge Server***

#### **Procedure**

1. Open a console on the Microsoft Edge.
2. Run `nslookup <FQDN for Presence Services>`.  
The system displays the IP address of Presence Services.
3. Run `nslookup <IP address of Presence Services>`.  
The system displays the FQDN of Presence Services.
4. Run `<JID domain of Presence Services>`.

The system displays the FQDN and IP address of Presence Services and port 5061.

#### **Related Links**

[Reconfiguring OCS](#) on page 256

---

## Checking the outcome of the changed network parameters

To see the outcome of the changed network parameters, see the SPchangeParam.log file.

### About this task

Use this task when you want to check the results for any of the network parameter changes.

### Procedure

1. Log in to the Presence server as a cust user and then use the su command to change to root.
2. To view the logs, type `more /opt/Avaya/Presence-VA/psva/ps-sp2utils/SPchangeParam.log`.

---

## Configuring network parameters on the non-System Platform deployments

### Changing the DNS servers

#### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.

The Presence server might be in a running state and using the `changeDNSServer.sh` command does not stop Presence Services.

2. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeDNSServer.sh -h`.

The system displays a Help window to show how to use the `changeDNSServer.sh` command.

3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeDNSServer.sh <DNS Server IP>`.

#### Note:

You can specify multiple DNS search domains by using a comma separated file. For example, `/opt/Avaya/Presence/presence/bin/changeDNSServer.sh <DNS server IP1>,<DNS server IP2>`.

### Changing a DNS search domain

#### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.

The Presence server might be in a running state and using the **changeDomainSearchList.sh** command does not stop Presence Services.

2. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeDomainSearchList.sh -h`.

The system displays a Help window to show how to use the **changeDomainSearchList.sh** command.

3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeDomainSearchList.sh <DNS search domain>`.

 **Note:**

You can specify multiple DNS search domains by using a comma separated file. For example, `/opt/Avaya/Presence/presence/bin/changeDomainSearchList.sh <DNS search domain1>,<DNS search domain2>`.

## Changing an IP address of Presence Services

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeIP.sh -h`.

The system displays a Help window to show how to use the **changeIP.sh** command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeIP.sh <current IP address> <new IP address>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.

The **changeIP.sh** command stops and restarts Presence Services.

## Changing the FQDN of Presence Services

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSFQDN.sh -h`.

The system displays a Help window to show how to use the **changePSFQDN.sh** command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSFQDN.sh <new FQDN of Presence Services>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.  
The `changePSFQDN.sh` command stops and restarts Presence Services.

## Changing the IP address and FQDN of Presence Services together

### Procedure

1. Log in to the Presence server as a cust user, and then use the `su` command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSFQDN.sh -h`.  
The system displays a Help window to show how to use the `changePSFQDN.sh` command.
4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSFQDN.sh <new FQDN of Presence Services> <new IP address of Presence Services>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.  
The `changePSFQDN.sh` command stops and restarts Presence Services.

## Changing Network Mask

### Procedure

1. Log in to the Presence server as a cust user, and then use the `su` command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeNetMask.sh -h`.  
The system displays a Help window to show how to use the `changeNetMask.sh` command.
4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeNetMask.sh <new network mask>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.  
The `changeNetMask.sh` command stops and restarts Presence Services.

## Changing the Gateway IP address for Presence Services

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeGW.sh -h`.

The system displays a Help window to show how to use the `changeGW.sh` command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeGW.sh <new Gateway IP address>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.  
The `changeGW.sh` command stops and restarts Presence Services.

## Changing the timezone for Presence Services

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSTimezone.sh -h`.

The system displays a Help window to show how to use the `changePSTimezone.sh` command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changePSTimezone.sh <Continent/Capital>`.
5. Enter `Y` when the system displays a message to continue with the configuration change.
6. Click **Yes** if you want to restart the Presence server, or click **No** if you want to restart the Presence server later.

## Changing an enrollment password

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.

The Presence server might be in a running state and using the `changeEnrollmentPassword.sh` command does not stop Presence Services.

2. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeEnrollmentPassword.sh -h`.

The system displays a Help window to show how to use the **changeEnrollmentPassword.sh** command.

3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeEnrollmentPassword.sh <new enrollment password>`.

## Changing the System Manager FQDN

### About this task

Use the **changeSMGR.sh** command only when you change the System Manager FQDN. The **changeSMGR.sh** command does not support reconfiguration of Presence Services to use a new System Manager.

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSMGR.sh -h`.

The system displays a Help window to show how to use the **changeSMGR.sh** command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSMGR.sh <new System Manager FQDN> [-w<webservices port>] [-n <naming port>] [-l <login>] [-p <password>] [-e <enrollment password>]`.

The **changeSMGR.sh** command stops and restarts Presence Services.

## Changing an AES IP address

### About this task

Use this procedure to change an AES IP address. If you did not configure AES on Presence Services, the **changeAES\_IP.sh** command will be ineffective.

### Procedure

Log on to the XCP Controller Web interface, to change the AES IP address for the Software-only deployments.

## Changing an Alternative WebLM FQDN on Presence Services

### About this task

Use this procedure to change an alternative WebLM FQDN. If you did not configure Alternative WebLM on Presence Services, the **changeAltWebLM.sh** command will be ineffective.

## Procedure

Log on to the XCP Controller Web interface, to change the alternative WebLM FQDN for the Software-only deployments.

## Changing a Session Manager IP address on Presence Services

### About this task

If you configured more than one Session Manager on Presence Services, the `changeSM_IP.sh` command is ineffective.

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSM_IP.sh -h`.

The system displays a Help window to show how to use the `changeSM_IP.sh` command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSM_IP.sh <new IP address of Session Manager>`.

The `changeSM_IP.sh` command stops and restarts Presence Services.

## Changing a Session Manager FQDN on Presence Services

### About this task

If you configured more than one Session Manager on Presence Services, the `changeSM_FQDN.sh` command is ineffective.

### Procedure

1. Log in to the Presence server as a cust user, and then use the su command to get root access.
2. Ensure that the Presence server is in a running state. For more information about restarting the Presence server, see [Restarting the system](#) on page 19.
3. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSM_FQDN.sh -h`.

The system displays a Help window to show how to use the `changeSM_FQDN.sh` command.

4. At the command prompt, type `/opt/Avaya/Presence/presence/bin/changeSM_FQDN.sh <new FQDN of Session Manager>`.

The `changeSM_FQDN.sh` command stops and restarts Presence Services.

---

# Certificate configuration

---

## Refreshing Presence Services certificates for System Manager

Use the `changeSMGR.sh` tool to refresh the presence certificate configuration for System Manager.

### Syntax

```
changeSMGR.sh <new SMGR FQDN> [-w <ws port>] [-n <naming port>] [-l <login>] [-p  
<password>] [-e <enrollment password>]
```

### Files

Files are located in `/opt/Avaya/Presence/presence/bin`.

---

## Creating new certificates in the Presence server

### About this task

The `prescert` tool is inside the `/opt/Avaya/Presence/presence/bin` folder. The `bin` folder contains the `changeSMGR.sh` script that you can use to update the certificates in System Manager.

### Procedure

1. Log in to the Presence server as a root user.
2. Navigate to the `bin` folder. For example, type `cd /opt/Avaya/Presence/bin`.
3. For more information on the `prescert` tool, at the command prompt, type `sh prescert`.

The system displays a list of commands to modify or update a Presence certificate.

4. To create new certificates, at the command prompt, type `sh prescert create scep pw xxx`, where `xxx` is the SCEP password.

The create new certificate script updates the certificates in the System Manager trust management system. For any reason, if the system does not update the certificates, use the `changeSMGR.sh` tool. For more information, see [Refreshing Presence Services certificates for System Manager](#) on page 265.

# Appendix A: Access Control Lists

---

## ACL scripts

---

### presuseracls tool

Use the `presuseracls` tool to view, create, modify, or delete user level ACLs. To view the user level Access Control List (ACL), run this script on the Presence server or on the System Manager server, as a root user. To create, modify, or delete user level ACLs, run this script on System Manager as a root user. If you choose to use the `presuseracls` tool on System Manager, copy the `presuseracls` script from the Presence server to the System Manager server. For more information, see *Configuring Authorization ACLs on System Manager*.

**\* Note:**

You must restart the Presence Services server if you run this script on System Manager to create, modify or delete user level ACLs.

#### Syntax

```
./presuseracls
```

Usage	Result
<code>./presuseracls &lt;presentityloginname&gt;</code>	Displays all the user level ACLs for the given <code>presentityloginname</code> .
<code>./presuseracls -c (--create) allow block presentity watcher</code>	Creates an ACL
<code>./presuseracls -c (--create) allow block presentity -ext watcher</code>	Creates an ACL for an external watcher
<code>./presuseracls -m (--modify) allow block presentity watcher</code>	Modifies an ACL
<code>./presuseracls: -d (--delete) presentity</code>	Deletes all ACL for a presentity
<code>./presuseracls -d (--delete) presentity watcher</code>	Deletes all ACL for a presentity watcher pair
<code>./presuseracls --delete -allow</code>	Deletes all allow ACLs for each user
<code>./presuseracls --delete -block</code>	Deletes all block ACLs for each user
<code>./presuseracls --delete -all</code>	Deletes all ACLs for each user
<code>./presuseracls -p presentity</code>	Shows presentity ACL

Usage	Result
<code>./presuseracls -w watcher</code>	Shows watcher referenced ACL
<code>./presuseracls --help</code>	Displays help page.

## Related Links

[Using the presuseracls tool](#) on page 267

## Using the presuseracls tool

### Before you begin

Start an SSH session using PuTTY and connect to the Presence server or System Manager server using their IP addresses.

### Procedure

1. To view user level ACLs:
  - a. Log in to the Presence server as a root user.
  - b. On the Presence server, navigate to the `/opt/Avaya/Presence/presence/bin` folder.
  - c. At the command prompt, type `chmod +x presuseracls` to change the presuseracls tool mode to an executable mode.
  - d. Use one of the following:
    - Option 1. Type `./presuseracls <presentityloginname>` and press **Enter** to display all the user level ACLs for a particular presentity login name.
    - Option 2. Type `./presuseracls` and press **Enter** to display all the user level ACLs.
2. To delete a user level ACL:
  - a. Copy this script in a temporary folder on the System Manager server. For example, `/tmp/directory`.
  - b. Log in to the System Manager as a root user.
  - c. Run the command, `chmod +x presuseracls`, to convert the presuseracls to an executable.
  - d. Get the **presentityloginname** information from the Presence Services for the ACL that needs to be deleted.
  - e. Run `./presuseracls -d <presentityloginname>` to delete user level ACLs for a particular presentity login name.
3. To create a user level ACL:
  - a. Copy this script in a temporary folder on the System Manager server. For example, `/tmp/directory`.
  - b. Log in to the System Manager as a root user.

- c. Run `./presuseracls -c <allow> or <block> <presentityloginname> <watcherloginname>` to create a user level ACL for a particular presentity watcher login name.

### Example 1: Show the user 55013's current list of ACLs by presentity

(Note: domain is optional for show)

```
[root@soalaba131 ~]# ./presuseracls -p 55013
presentity      | pid |          watcher          | wid | ruletype | ruleid |
infotype|      updated
-----+-----+-----+-----+-----+-----+-----+-----+
55013@aceaura.avaya.com| 1292 | 55013@aceaura.avaya.com| 1292 |         |         |
|      50 | 2012-09-20 16:54:50.435
55014@aceaura.avaya.com| 1293 | ALLOW          | 181 | 50 | 2012-09-21
10:39:41.835
55013@aceaura.avaya.com| 1292 | dog2001@aceaura.avaya.com | 150 | ALLOW      | 184
|      50 | 2012-09-20 16:54:50.435
55013@aceaura.avaya.com| 1292 | 55011@aceaura.avaya.com   | 229 | ALLOW      | 183
|      50 | 2012-09-20 16:54:49.929
(3 rows)
```

### Example 2: Show who is watching 55013:

```
[root@soalaba131 ~]# ./presuseracls -w 55013
presentity      | pid |          watcher          | wid | ruletype | ruleid |
infotype|      updated
-----+-----+-----+-----+-----+-----+
55014@aceaura.avaya.com| 1293 | 55013@aceaura.avaya.com   | 1292 | ALLOW      | 180
|      50 | 2012-09-20 17:14:15.6(1 row)
```

### Example 3: Modify a single presentity watcher pair ACL:

```
[root@soalaba131 ~]# ./presuseracls -m block 55013@aceaura.avaya.com
55011@aceaura.avaya.com
UPDATE 1
root@soalaba131 ~]# ./presuseracls -p 55013
presentity      | pid |          watcher          | wid | ruletype | ruleid |
infotype|      updated
-----+-----+-----+-----+-----+-----+
55013@aceaura.avaya.com| 1292 | 55014@aceaura.avaya.com   | 1293 | ALLOW      | 181 |
|      50 | 2012-09-21 10:39:41.835
55013@aceaura.avaya.com| 1292 | dog2001@aceaura.avaya.com | 150 | ALLOW      | 184 |
|      50 | 2012-09-20 16:54:50.435
55013@aceaura.avaya.com| 1292 | 55011@aceaura.avaya.com   | 229 | BLOCK      | 183 |
|      50 | 2012-09-28 12:17:12.320265
(3 rows)
```

### Example 4: Delete a single presentity watcher pair ACL:

```
[root@soalaba131 ~]# ./presuseracls -d 55013@aceaura.avaya.com 55011@aceaura.avaya.com
DELETE 1
[root@soalaba131 ~]# ./presuseracls -p 55013
presentity      | pid |          watcher          | wid | ruletype | ruleid |
infotype|      updated
-----+-----+-----+-----+-----+-----+
55013@aceaura.avaya.com| 1292 | 55014@aceaura.avaya.com   | 1293 | ALLOW      | 181
|      50 | 2012-09-21 10:39:41.835
55013@aceaura.avaya.com| 1292 | dog2001@aceaura.avaya.com | 150 | ALLOW      | 184
|      50 | 2012-09-20 16:54:50.435
(2 rows)
```

**Example 5: Create a single presenty watcher pair ACL:**

```
[root@soalaba131 ~]# ./presuseracls -c allow 55013@aceaura.avaya.com
55011@aceaura.avaya.com
INSERT 0 1
[root@soalaba131 ~]# ./presuseracls -p 55013
presenty      | pid | watcher                                | wid | ruletype | ruleid |
infotype| updated
-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+
55013@aceaura.avaya.com| 1292 | 55014@aceaura.avaya.com | 229 | ALLOW | 195 |
50 | 2012-09-28 12:19:50.899063
55013@aceaura.avaya.com| 1292 | dog2001@aceaura.avaya.com | 1293 | ALLOW | 184 |
50 | 22012-09-21 10:39:41.835
55013@aceaura.avaya.com| 1292 | dog2001@aceaura.avaya.com | 150 | ALLOW | 184 |
50 | 2012-09-20 16:54:50.435(3 rows)
```

**Related Links**

[presuseracls tool](#) on page 266

## User default ACL policy script

Use the `./user-default-acl-policy.sh` script as a root user to view, create, and delete the default ACL settings for a user. Use PuTTY to open an SSH session and connect to the System Manager server. The default location of the `./user-default-acl-policy.sh` on the Presence server is, `/opt/Avaya/Presence/presence/bin`. Use the `chmod +x ./user-default-acl-policy.sh` command to change the mode to an executable mode.

To run the script from System Manager, copy the script from the Presence server using a file transfer client and copy the script on System Manager.

**\* Note:**

You must restart the Presence Services server if you run this script on System Manager to create or delete the default ACL settings for a user.

**`./user-default-acl-policy.sh [ -c allow/block/confirm | -d ] user@domain`**

Using `./user-default-acl-policy.sh`, you can perform the following:

- Show the default ACL policy for a user.
- Create a user default ACL policy with allow, block, and confirm states.
- Delete a user default ACL policy.

where,

- `-c`, creates an ACL
- `-d`, deletes an ACL
- and, if you do not enter any parameter, the system displays the default ACL policy script options. For example:
  - `./user-default-acl-policy.sh -c ALLOW | BLOCK | CONFIRM user@domain`
  - `./user-default-acl-policy.sh -d user@domain`
  - `./user-default-acl-policy.sh user@domain`

**\* Note:**

You can create or delete a user default ACL policy only from System Manager. However, to show the current status of the default ACL policy for a user, you can run the `./user-default-acl-policy.sh` script from both System Manager and Presence server.

**Example 1: Show the default ACL policy for the 55010 user, which is not yet created**

```
[root@abcd ~]# ./user-default-acl-policy.sh 55010
discriminator | aclid | name | acl
-----+-----+-----+-----
(0 rows)
```

**Example 2: Create a user default ACL policy for the 55010 user with a confirm state**

```
[root@abcd ~]# ./user-default-acl-policy.sh -c confirm 55010@abc.avaya.com
INSERT 0 1
```

**Example 3: Show the confirm state for the 55010 user**

```
[root@abcd ~]# ./user-default-acl-policy.sh 55010
discriminator | aclid | name | acl
-----+-----+-----+-----
UD | 994 | 55010@abc.avaya.com | CONFIRM
(1 row)
```

**Example 4: Delete the default ACL policy for the 55010 user**

```
[root@abcd ~]# ./user-default-acl-policy.sh -d 55010@abc.avaya.com
DELETE 1
```

**Example 5: Show status of the deleted 55010 user**

```
[root@abcd ~]# ./user-default-acl-policy.sh 55010
discriminator | aclid | name | acl
-----+-----+-----+-----
(0 rows)
```

---

## User default policy domain ACL script

Use the `./user-default-policy-domain.sh` script to create or delete the user default ACL policy for all users that have an Other XMPP or Microsoft SIP communication address within a specific domain. The default location of the script on the Presence server is: `/opt/Avaya/Presence/presence/bin`. You must run the script from System Manager. For more information, see *Running the user-default-policy-domain.sh ACL script*.

**\* Note:**

You must restart the Presence Services server if you run this script on System Manager to create or delete the user default ACL policy.

```
./user-default-policy-domain.sh [ -c allow/block | -d ] domain
```

Using the `./user-default-policy-domain.sh` script, you can perform the following:

- Create a user default ACL policy with Allow or Block states for all users with an Other XMPP or Microsoft SIP communication address in *domain*
- Delete the user default ACL policy for all users with an Other XMPP or Microsoft SIP communication address in *domain*.

where,

- `c`: creates a user default ACL policy.
- `d`: deletes a user default ACL policy.
- "domain" matches the domain portion of the Other XMPP or Microsoft SIP communication address of a user.

For example:

- `./user-default-policy-domain.sh -c ALLOW xmpp.com` creates a user default ACL policy with Allow state for all users with an Other XMPP or Microsoft SIP communication address in *xmpp.com* domain.
- `./user-default-policy-domain.sh -c BLOCK xmpp.com` creates a user default ACL policy with Block state for all users with an Other XMPP or Microsoft SIP communication address in *xmpp.com* domain.
- `./user-default-policy-domain.sh -d xmpp.com` deletes the user default ACL policy with for all users with an Other XMPP or Microsoft SIP communication address in *xmpp.com* domain.

### Related Links

[Running the user-default-policy-domain.sh ACL script](#) on page 139

---

## Access Levels

---

### Presence access levels

Presence access levels are defined in terms of Presence classes. An access level can contain a single Presence class or a set of classes. Access rules defined in the Presence ACLs (Access Control Lists) then apply to all classes in an access level.

For the purpose of access control, presence information is partitioned into the following Presence access levels:

- Telephony
- All

The All access level is always defined and always includes complete Presence information. An access level can also contain an inversion of a set of classes for convenience. In other words, administrators can define an access level to contain all classes that are not in the selected set of classes. This makes it easier to define access levels, such as all classes except Phone.

---

## Defining rules

If you define a specific rule to an ACL, then that takes precedence over a generic rule. For example, in the same ACL, levels including just one class have precedence over multiple-class levels which in turn have precedence over the level All.

The ACLs in each band are arranged in such a way that an ACL applicable to a single watcher or presentity pair (more specific) takes precedence over more generic ACLs applicable to all watchers or all presentities and also the ones applicable to all pairs.

---

## Filtering

Presence information is filtered, so each watcher can see only that part of Presence that the watcher is allowed to see. Both the Presence owner and system administrator can control the level of Presence allowed to the watcher.

Presence filtering is done with granularity of tuple. Filtering is based on the value of the class element and does not affect the person element of Presence.

---

## Soliciting confirmation

You can create an ACL, apply the levels, and then solicit confirmation from the user. If you have set the ACL to CONFIRM, then the system sets the ACL level to Pending till it receives confirmation from the Presence owner or presentity when online the next time. The presentity can decide to set the ACL level to Allow or Block or any other level of access for the watcher using LPS. If you do not set the Confirm level, the system works with no user interaction.

 **Note:**

Only the System Manager console can manage System Wide ACL. There is no Web console to manage User ACL. It is the responsibility of Presence Services clients to manage user ACL.

---

## Presence access levels in System Manager

System Manager provides basic access levels grouped into default ACLs. Using the default ACLs, you can set the filtering to Allow, Block, or Confirm states. Each ACL can have multiple-level definitions.

The list of default ACLs arranged in order of priority is as follows:

- System Default for all watchers and all presentities with the lowest precedence.
- User ACL for each watcher or presentity pair controlled by the user.
- User Default for each presentity controlled by the user. With this access level, you can have fine-grained control over the level of presence available for the watcher.

---

## Viewing presence access levels

### Procedure

1. Log on to the System Manager web console as an administrator.
2. On the System Manager dashboard, click **Users > User Management > System Presence ACLs**.

The page displays all defined presence access levels.

---

## Creating Presence access levels

### Procedure

1. Log on to the System Manager web console as an administrator.
2. On System Manager dashboard, click **Users > User Management**.
3. In the left navigation pane, click **System Presence ACLs**.
4. On the Presence ACL page, click **New**.
5. Fill in details of the new access level.
6. Click **Save**.

---

## Modifying presence access levels

### Procedure

1. Log on to the System Manager web console as an administrator.
2. On the System Manager dashboard, click **Users > User Management**.
3. In the navigation pane, click **System Presence ACLs**.

4. On the Presence ACL page, select the access level that you want to modify.
5. Click **Edit**.
6. Modify the details of the access level.
7. Click **Save**.

 **Note:**

Access level **All** is predefined and cannot be modified or deleted.

## Deleting Presence access levels

### Procedure

1. Log on to the System Manager web console as an administrator.
2. On the System Manager dashboard, click **Users > User Management**.
3. In the navigation pane, click **System Presence ACLs**.
4. On the Presence ACL page, select the access level that you want to delete.
5. Click **Delete**.

## Presence ACL field descriptions

Name	Description
<b>Access Level</b>	The presence information for which the access control rules are set. The options are: <ul style="list-style-type: none"> <li>• <b>Telephony:</b> The telephony-related presence information for which you can set an access permission.</li> <li>• <b>All:</b> All types of presence information for which you can set an access permission.</li> </ul>
<b>Action</b>	The access control permission for the presence information. The options are: <ul style="list-style-type: none"> <li>• <b>Allow:</b> Provides the watcher the access to the presence information for the access level.</li> <li>• <b>Block:</b> Blocks the watcher from accessing the presence information for the access level.</li> <li>• <b>Confirm:</b> Requires confirmation from the presentities for the watcher to access the presence information of presentities.</li> <li>• <b>Undefined:</b> Access to the presence information for the access level is undefined for the watcher.</li> </ul>

# Appendix B: Configuring users in System Manager to enable Presence and Instant Messaging

---

## Communications address terminology

One of the key concepts in Avaya Aura® is the use of Canonical Addressing. A canonical address is a SIP Address of Record (AOR) that is used as route by the core and uniquely identifies a single user across all sites in the Enterprise. The Avaya SIP Reference Architecture specifies three forms of canonical address:

1. E.164 International Format. E.164 is a standard of the ITU-T that specifies the international public telecommunications numbering plan. There are four types of E.164 numbers, one each for geographic areas, global services, networks, and groups of countries. All types of this format start with a +, followed by the Country Code, and end with a Subscriber Number. For some formats, there are other digits between the Country Code and the Subscriber Number. In all cases, the combination of digits can be no more than 15 digits, with the Country Code accounting for between 1 and 3 of these digits. An example of an E.164 number is +13035351234.
2. Enterprise Private Numbering Format. This format has a numeric string of variable length as the user part and a domain: 1234567890@enterprise.com. While the user part is of variable length, the complete address must be unique across the enterprise. The user part does not need to be unique. For example, you can have 123456@ease.enterprise.com and 123456@west.enterprise.com. However, the qualified domain name (FQDN) must be specified. It is usually better to have unique user parts for simplicity. Additionally, not all applications differentiate beyond the user part. Therefore, System Administrators must provision all users with communication addresses containing unique user parts. Note that the Enterprise Private Numbering Format can be set to E.164 without the "+". While technically this may be considered to be a Public rather than Private format, it is called Private for the purposes of this section.
3. Alphanumeric Handle Format. The alphanumeric handle is a user part that is a combination of letters and numbers and a domain. For example, JohnSmith123@enterprise.com. As indicated, the user part can be a combination of upper and lower case letters and numbers, but it need not be a combination of all three. However, the user part must not overlap with the E.164 International or Enterprise Private Numbering formats.

Other terminology used to describe communication addresses is as follows:

1. Long Form. A synonym of the Enterprise Private Numbering format. However, Avaya does not recommend this format as it can be ambiguous.
2. Short Form. Equates a short dial format accepted by Avaya Aura® Communication Manager. As not all people include dialing prefixes, this format can also be ambiguous, and Avaya does not recommend its use.

---

## Network login

One of the differences between Avaya Aura® and previous Avaya systems is the scope of the user's communications sessions.

Earlier, when end users logged into Communication Manager, they could log in with a short form address in the form of an Avaya Extension (AVXT) that was known to the Communication Manager receiving the login. However for Avaya Aura®, the user logs in to the Network rather than into Communication Manager. Therefore, they must use a communications address (also called a handle) that has network scope.

In the current implementation, a consistent login is used across all endpoints and clients for Presence and IM to function properly. End users must use the Enterprise Private Numbering Format as not all endpoints/clients accept entry of a +.

This is a change for the end users, as previously they were able to log in using an extension number (short form). In Avaya Aura® 6.0 release, Avaya recommends that an Enterprise Canonical communications address be used for the login. To help mitigate the impact, You can set up Enterprise Private Numbering plans of variable length including shorter handles, as long as they are unique across the Enterprise.

---

## Configuring Users

Avaya recommends that you configure each user with two communication addresses:

1. E.164 International Format
2. Enterprise Private Numbering Format

System Manager displays the User Configuration page as follows:

The screenshot shows the 'Communication Profile' configuration page. It includes a table for 'Communication Address' with the following data:

Type	Handle	Domain
Avaya E.164	+13035354424	avaya.com
Avaya SIP	5354424	avaya.com

Below the table, there are three checkboxes:  Session Manager Profile,  Endpoint Profile, and  Messaging Profile.

**\* Note:**

Avaya SIP communications address could also be 3035254424 or 13035354424, depending on the Enterprise Private Numbering Format that has been selected.

You must also provision communication addresses for auxiliary systems, such as the addresses in Endpoint Profile used by AES and Microsoft OCS (discussed below). Provisioning makes the Presence information from these sources available to users.

In Release 6.0, only a single Communications Profile must be provisioned for a user. Multiple Communications Profiles hamper the functioning of Presence and IM for the user.

## Adding contacts

### About this task

It is important that you add contacts in a fashion that ensures Presence and IM function properly. Avaya recommends that you maintain contacts in E.164 format. As the end users do not use this format initially, clients can convert other formats to E.164 prior to storing them in SMGR. If there is no provisioned E.164 address, then use the Enterprise Private Number format. A client determines the acceptance of a format.

You can add contacts in three different ways. However, all endpoints/clients do not implement all three mechanisms:

## Procedure

1. Manual entry. The end user types in the information.
2. Enterprise Directory lookup. The end user enters some details about the contact, and the endpoint/client looks in the directory for a matching entry. If a matching entry is found, it is added to the System Manager database as a contact for which Presence and IM are allowed. If there is no match, then the system disables Presence and IM with that contact.
3. Entry from Call Log. The end user can select a contact from an incoming, outgoing, or missed call log and add the contact to the Contact List. The same matching rules as described in item (2) are applied to determine if Presence and IM are available with the new contact. Note that not all clients support adding contacts from a call log.

When a match is not found in SMGR, then Presence and IM are not available for that contact, even if they are present in the System Manager database as a provisioned user. The primary reason for not finding a match is the use of different number formats. For example, short versus long number strings, use of dialing prefixed numbers, and so on.

Mapping a SMGR user is important when adding a contact from the Enterprise Directory. If mapping fails, then the contact is considered to be external, and Presence and IM are not available to the user. This mapping typically uses either the E.164 communications address or the binary unique identifier found in the Directory that has been imported through a directory synchronization or bulk import into System Manager.

In addition to having a match, in Avaya Aura® 6.0 you need to provision a contact with a Session Manager Communication Profile (CommProfile) for Presence and IM to be available for that contact, even if the contact does not use SIP. This limitation is being removed in the Avaya Aura® 6.1.

Presence Services can provide the Presence of Enterprise users that have accounts with Microsoft Office Communications Server (OCS). For this to work, the OCS address of the contact must be provisioned in System Manager. This means that IM to OCS users who are not provisioned as Avaya Aura® users will not be available in this release.

When a Presence client starts, it assumes it can watch the presence of all members on its Contact List. To achieve this, the client subscribes to the User Contact List that contains all contacts by sending the list to the Presence Services. When the system updates the list with either additions or deletions, Presence Services is notified. Presence Services automatically updates the Presence subscriptions, closing subscriptions for deleted entries and creating new subscriptions to added entries. Depending on the load on the system, modification and deletion of existing contacts may take a few minutes to become visible in a client Contact List.

---

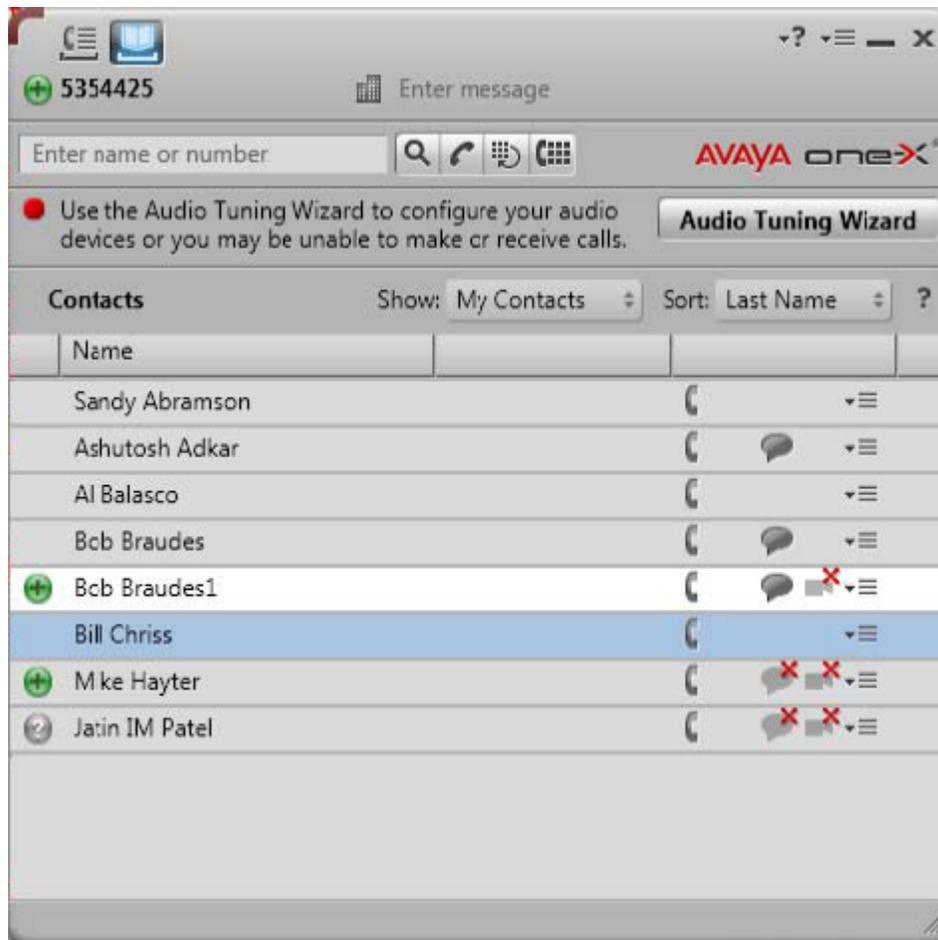
## Presence and Instant Messaging

Two major new features in Avaya Aura® 6.0 are the incorporation of aggregated Presence information and the ability to send instant messages between users. Presence information is

aggregated from multiple sources, including hardphones and soft clients that register with Avaya Aura® Session Manager through SIP, such as:

- Avaya one-X® Communicator
- AES for H.323, DCP, and Analog endpoints
- Java API
- Microsoft Office Communicator 2005 and 2007 clients based on OCS 2007 R2
- XMPP clients based on an XMPP federated server

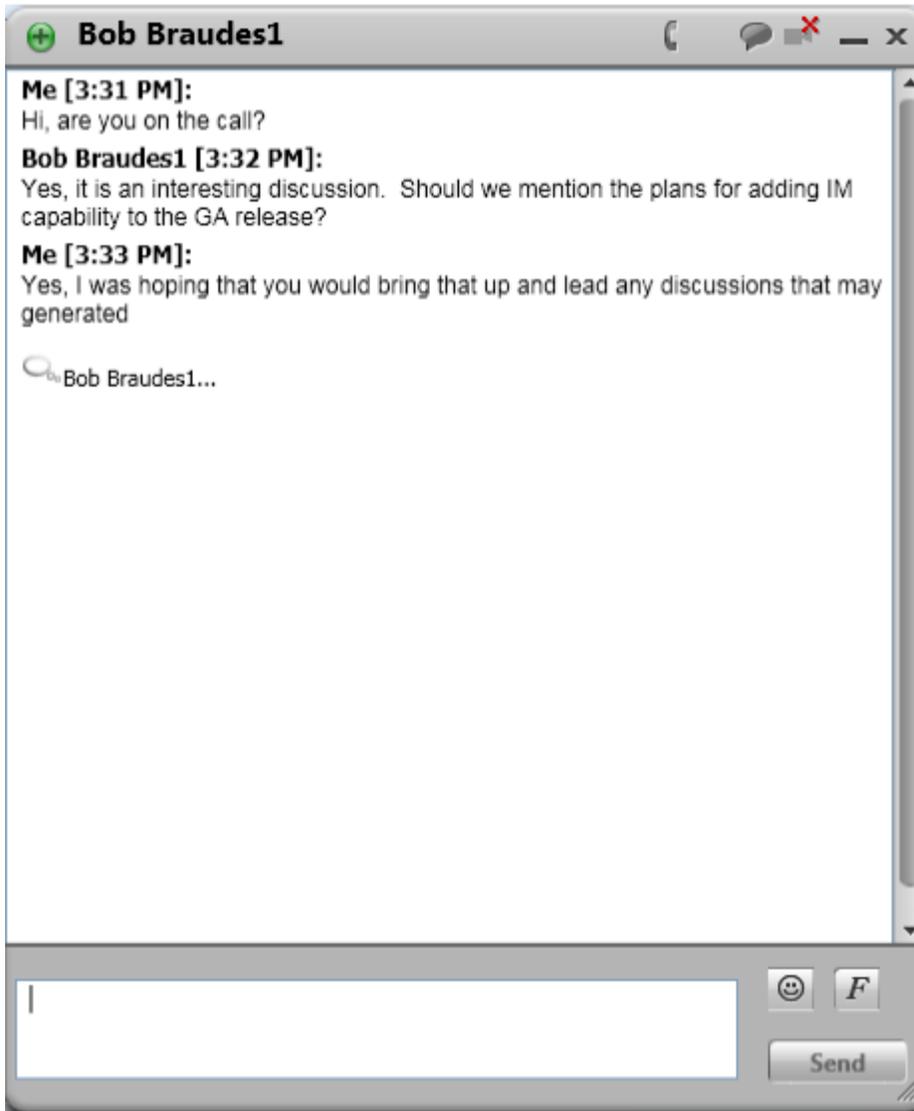
Presence information is sent from Presence Services to clients over SIP or through Java API. Information is filtered individually for each Watcher (person viewing Presence state of another user) / Presentity (the user being watched) pair. The Presence Services clients then render the Presence information for various watchers in a client-specific format. For example, Avaya one-X® Communicator displays Presence information as follows:



The left column shows the Presence status of people being *watched* by the user (Presentity) 5354425. The icons in the second column from the right show whether a given user is available in each modality used by the presentity. For example, Mike Hayter is available for a telephone call but not available for either IM or video. If a user is not provisioned in System Manager, then the user can avail Presence information nor IM. Similarly, if there are no provisioned e-mail addresses, then

the system does not display the e-mail icon. Another restriction for the 6.0 release is that Presence for H.323, DCP, and Analog users can only be seen if those users are on the watcher's Contact List. This includes viewing their Presence state in Call Logs and in Directory Searches.

When an IM session is initiated in Avaya one-X® Communicator, a new window opens that shows the contents of the IM:



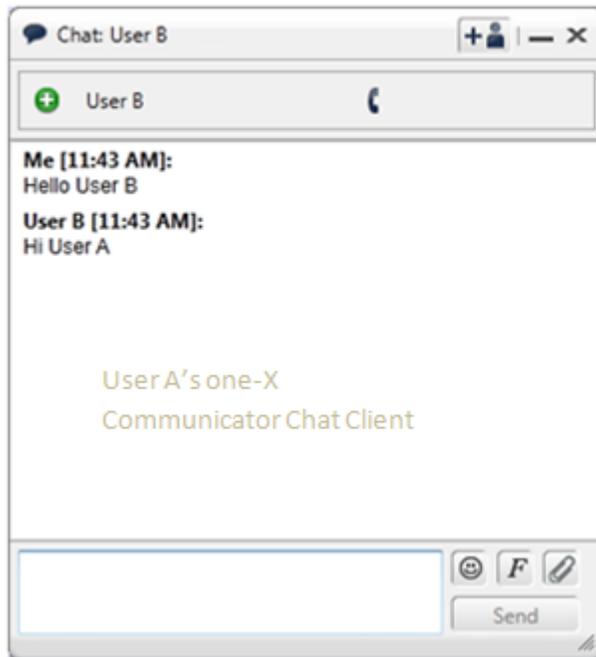
This works in a manner similar to most IM clients.

There are a number of different scenarios for IM communication, especially when users logs into multiple devices simultaneously. The four scenarios illustrates what the user can expect with IM clients logs into the Presence server.

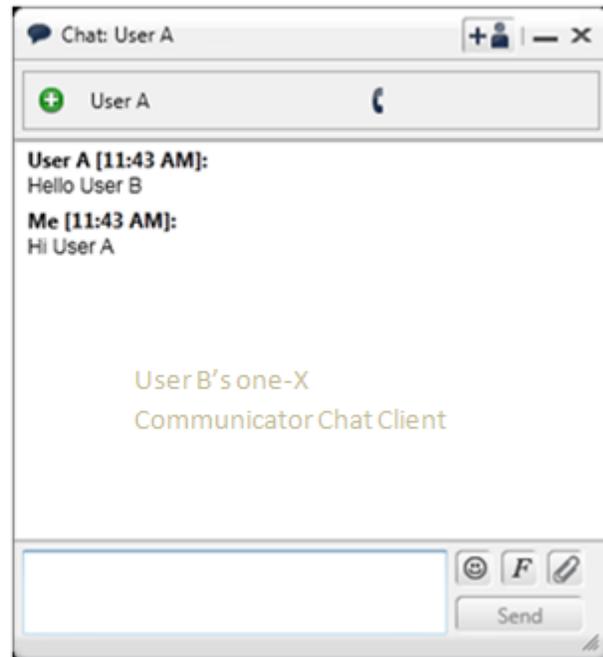
### User A and User B use one client each

This is the simplest scenario and works in a manner similar to most IM clients. User A's messages appear in User B's client and User B's messages appear in User A's client as shown in the Avaya one-X Communicator Chat windows.

User A Chatting with User B



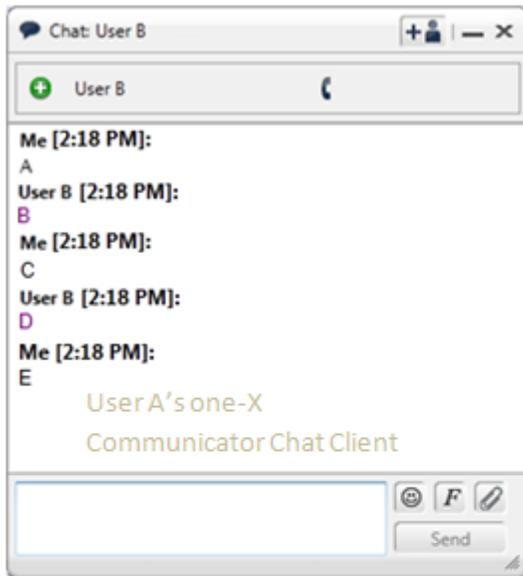
User B chatting with User A



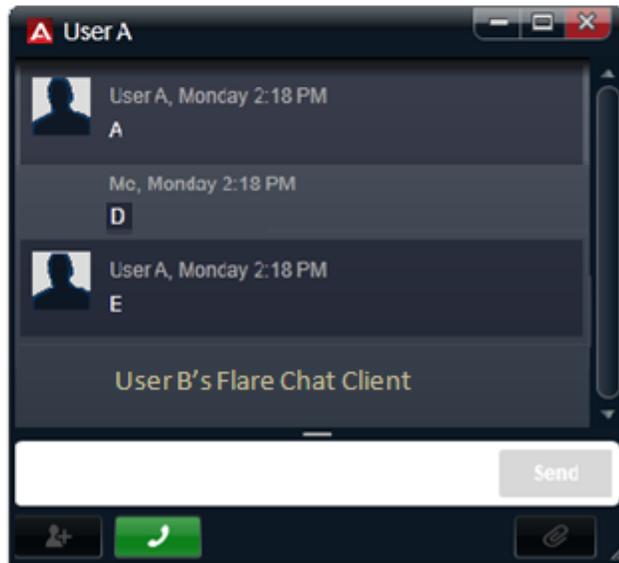
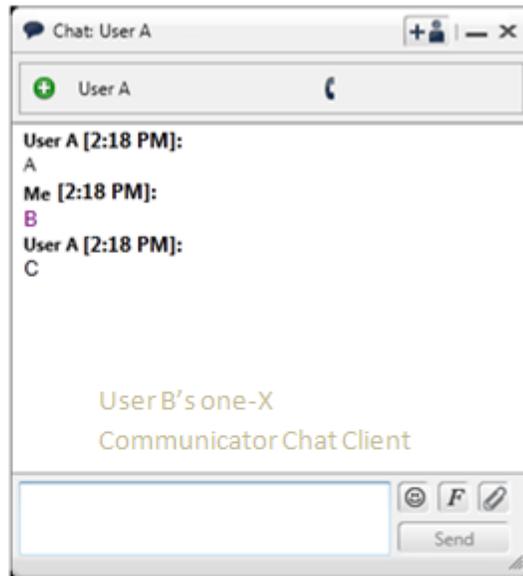
### User A has single client and User B uses multiple clients

In this Scenario User B is logged into two clients, such as one-X Communicator and Avaya Flare. When User A initiates a chat with user B, the initial message is displayed on both the clients. However, once User B responds to the initial chat message, user A's subsequent responses are directed to the client that sent the reply.

User A Chatting with User B



User B chatting with User A



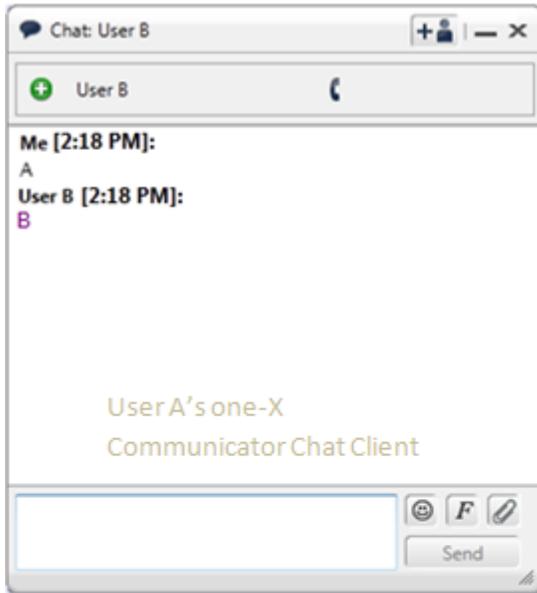
Note that if User B responds to A using his Flare client, User A's client in turn responds back to the Flare client and not the one-X Communicator client as shown in message "D" and "E".

### User A has multiple clients and User B uses one client

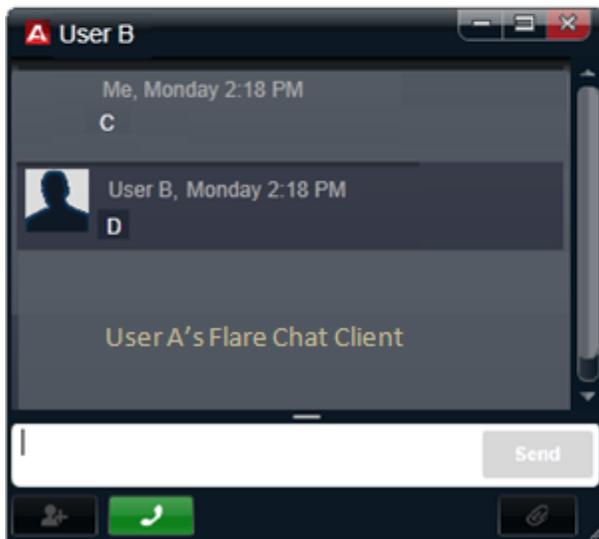
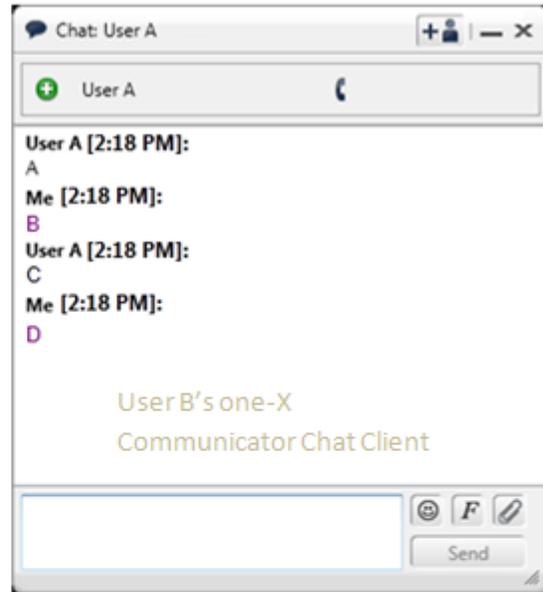
In this Scenario User A is logged into two clients and User B is logged into one client. In this scenario, User A is effectively creating two chat sessions, one is created when User A sends the message "A" from the one-X Communicator client and another is created when User A sends the message "C" from the Flare client. Even though this results in two chat sessions, User B's one-X Communicator client does not expose those details to User B.

When User A continues the chat in the Flare chat window, the system generates a new thread ID. This means, for any application that archives the conversations, the conversation from the Flare window may appear as a different conversation.

User A Chatting with User B



User B chatting with User A

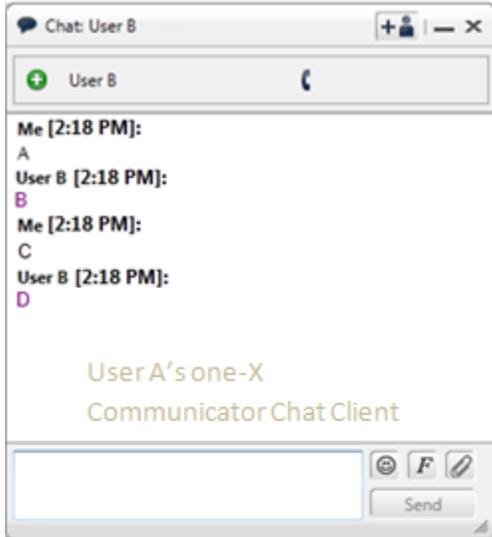


**User A has multiple clients and User B has multiple clients**

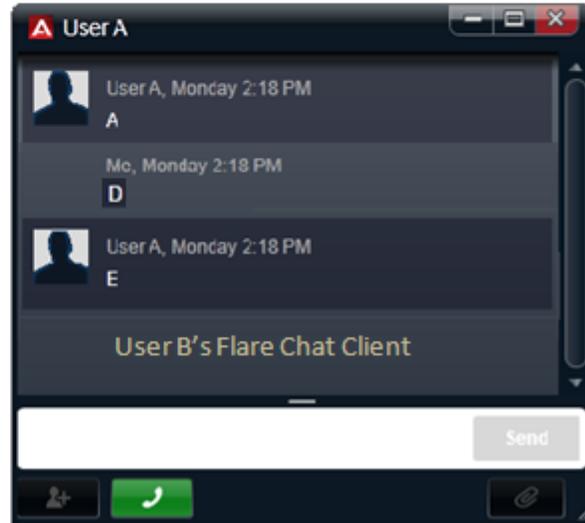
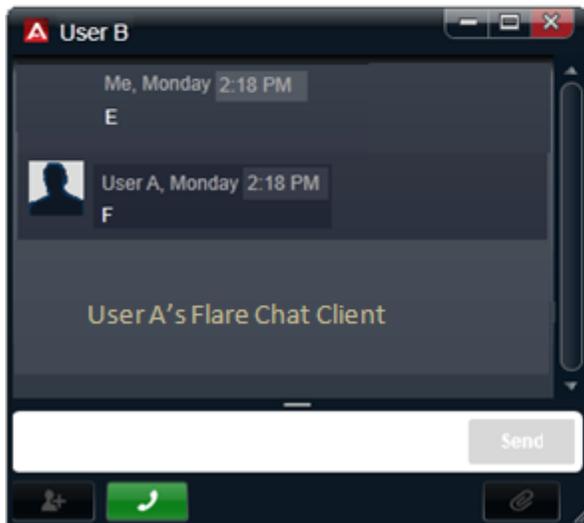
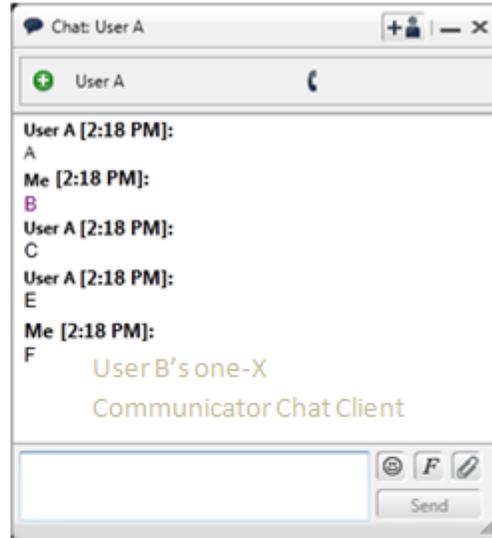
In this Scenario, User A is logged into two clients and User B is logged into two clients. Similar to the previous scenario, User A is effectively creating two chat sessions, one is created when User A sends the message “A” from the one-X Communicator client and another is created when User A sends the message “E” from the Flare client. In all cases, User B’s chat sessions return messages back to the originator of each individual message.

When User A continues the chat in the Flare chat window, the system generates a new thread ID. This means, for any application that archives the conversations, the conversation from the Flare window may appear as a different conversation.

User A Chatting with User B



User B chatting with User A



# Appendix C: Configuring the Presence Services server for Avaya one-X<sup>®</sup> Client Enablement Services

## Procedure

1. Log in to the Presence Services XCP Controller web interface.
2. Select the **Advanced** configuration view.
3. Add the Avaya one-X<sup>®</sup> Client Enablement Services host names to the Trusted TLS host names:
  - a. On the Presence Services XCP Controller main page, click **Edit** next to **Global Routing Settings**.
  - b. On the Global Settings Configuration page, scroll down to the **Mutually Trusted TLS Hostnames** section, and type the host names in the **Host Filters** text box.

The host names must match the CN value obtained from the root certificate from WAS.

### **Note:**

To obtain the CN name from WAS, select **Security > SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates**. Type the FQDN of the Avaya one-X<sup>®</sup> Client Enablement Services machine.

4. Type the details of AES Collector:
  - a. On the Presence Services XCP Controller main page, click **Edit** next to **AES Collector**.
  - b. On the AES Collector Configuration page, scroll down to the **AES Collector Component** section.
  - c. In the **Default AES Username** field, type the user name.  
For example, `admin_login`.
  - d. In the **Default AES Password** field, type the password.  
For example, `admin1_password`.
5. To change the **Log in to PostgreSQL** settings, log in to the system console of the Presence Services server.

6. Access the Presence Services server CLI, and verify the following settings:

- a. Type `cd /var/lib/pgsql/data`.
- b. In the data directory, type the **vi pg\_hba.conf** command to modify the `pg_hba.conf` file, and type the exact IP address ranges with proper masking bit at the end of the file.

For example, `hosts all all 148.147.146.145/32 md5`.

**\* Note:**

The subnet is of the one-X Client Enablement Services server. The subnet supports communication between one-X Client applications and the Presence server.

- c. In the data directory, type the **vi postgresql.conf** command to modify the `postgresql.conf` file and set **listen\_addresses = \***.
- d. To restart the postgres sql service, type `service postgresql restart`.

**\* Note:**

System Manager handles Presence Services on Avaya one-X® Client Enablement Services. You can enable Presence Services only for the users who are defined on System Manager. Such users are superset of the users who are defined on Avaya one-X® Client Enablement Services. Therefore, you can see the presence of a user who is defined only in System Manager and not in Avaya one-X® Client Enablement Services.

# Appendix D: CS 1000 with Presence Services

When you implement Presence Services with CS 1000, you can configure Avaya one-X<sup>®</sup> Communicator to be the watcher as well as allow other system to watch Avaya one-X<sup>®</sup> Communicator. However, with non-Avaya one-X<sup>®</sup> Communicator phones, such as analog and digital; using Presence, they can be watched but cannot be watchers.

You can now administer CS 1000 using System Manager. Using System Manager Web Console you can perform the following tasks to enable Presence Services:

- Creating a subscriber
- Creating a Presence account
- Adding a telephony

## Related Links

[Creating a subscriber](#) on page 287

[CS 1000 Presence publisher](#) on page 288

[Configuring Presence publisher](#) on page 289

---

## Creating a subscriber

### Procedure

1. Log in to System Manager Web Console.
2. On System Manager Dashboard, click **User Management**.  
The system displays the User Management page.
3. Click **User Management > Manage Users > New**.  
The system displays the New User Profile page.
4. On the **Identity** tab, enter the following details:
  - a. **Last Name**: Last name of the subscriber.
  - b. **First Name**: First name of the subscriber.
  - c. **Login Name**: Login name of the subscriber.

- d. **Password:** Password for the subscriber.
5. On the **Communication Profile** tab, enter the communication profile password and then confirm the communication profile password for the CS 1000 end point user.
6. In the Communication Address section, click **New**.
  - a. In the Type field, click the type of end point that you want to add. For example, Avaya SIP or Avaya E.164.
  - b. In the **Fully Qualified Address** field, enter the handle and domain details. For example, in the Handle field, enter +35311230121.
  - c. From the **Domain** field, select a domain. For example, avaya.com.
  - d. Click **Add**.

 **Important:**

You must add at least one SIP/E.164 Handle on the Communication Profile for the 1XC-SIP, H.323, Flare, 96xx, SIP and other watchers, to see the presence status of a CS1000 user. If you do not add a SIP/E.164 handle, the system does not display the presence status of the CS1000 user on the watchers.

7. To save the changes, click **Commit**.
8. Enter the details of the new subscriber, such as Last name, First name, Employee ID, and so on.

 **Note:**

You do not need to fill in all the details except username and domain for Presence Services. You may have to fill in other details if one-X Client supports OpenLDAP. You must fill in the password if you want to synchronize the password of all the presence and telephony accounts to the same password for this subscriber. This password is not active until password synchronization is done. Once it is done, it replaces the existing Communication Profile Password (for example, the default Presence Account password) for the Presence Services of this user. The same password is also sent to the CS 1000 Call Server to update the UPWD. UPWD is the login password for the SIP Line Telephony account.

9. To save the changes, click **Save**.

#### Related Links

[CS 1000 with Presence Services](#) on page 287

---

## CS 1000 Presence publisher

The CS 1000 Presence publisher sends SIP messages to the Presence server whenever there is a change in the status of the call for all CS 1000 line phones that do not use XMPP protocol. The Presence publisher uses the SIP Publish message to capture the change in the call status and

sends to the Presence Server which in turn sends the status change using XMPP protocol to the one-X client.

### Related Links

[CS 1000 with Presence Services](#) on page 287

---

## Configuring Presence publisher

### Procedure

1. Log in to System Manager Web Console, click **Administrators**.  
The system displays the Administrative Users page of the CS 1000 Unified Communication Management (UCM).
2. Under **Network**, click **Elements**.  
The Elements page displays the existing elements.
3. On the Elements page, select the **Element Manager (EM)** element with element type CS 1000. The system displays the System Overview page.
- 4.
5. Under System, click **IP Network** to open a sub menu. Click **Nodes** , **Servers**, and **Media Cards**.  
The system displays IP Telephony Nodes.
6. Click the node in which you want to configure the Presence publisher.  
The system displays the Node Details page.
7. To configure Presence publisher, select the **Presence Publisher** application.
8. From the **IM and Presence server type** drop-down list, select the server type. For example, Aura PS.
9. Fill in all the other fields as required.
10. In the Outbound Proxy server section, you can:
  - Send the SIP publish message directly to the Presence server
  - Send SIP publish message to Session Manager, which in turn routes the messages to the Presence server
11. Fill in the Outbound Proxy settings with the IP address of the Presence Services:
  - If you want to send the SIP publish messages directly to the Presence Services.
  - Otherwise, fill in the IP address of the Session Manager if you are using Session Manager to route the SIP publish messages.

12. If you are using Session Manager to route the SIP publish messages, you must configure a Presence server SIP Entity and a Session Manager to Presence server SIP Linkage in System Manager.

For more information on how to do configurations in UCM, see [https://support.avaya.com/css/Products/P0715/All\\_Documents](https://support.avaya.com/css/Products/P0715/All_Documents)

- Unified Communications Management Common Services Fundamentals Avaya Communication Server 1000, Doc ID: NN43001-116

#### **Related Links**

[CS 1000 with Presence Services](#) on page 287

# Appendix E: Presence Services field descriptions

Field	Description
Presence Services name	<p>Install Presence Services in a different domain from OCS. This allows for federation between OCS and Presence Services.</p> <p>This needs to be resolvable by a DNS SRV record.</p> <p><b>* Note:</b></p> <p>Presence Services must have a static IP address. Do not attempt to dynamically assign IP address through Dynamic Host Configuration Protocol (DHCP) as this may cause the system to become unstable in the future.</p> <p>Presence Services must also have an FQDN assigned to it.</p>
System Manager Configuration settings	
System Manager Host PANTHER_HOST	<p><b>* Note:</b></p> <p>The host name is required here (not the IP address) for certificate validation purposes. You must also ensure that you can access the System Manager server. For example, using the ping command from either side or DNS lookup. For a template installation from CDMO, the System Manager must be running at the time of Presence Services installation, because the installer attempts to register the new Presence Services instance and get a new certificate for it.</p> <p>If you are not using DNS server, you must make additional entries to <code>/etc/hosts</code> field.</p>
Web Services Port. PANTHER_WS_PORT	<p>System Manager Web Services Port</p> <p>Port used by System Manager to expose its Web Services- defaults to 443</p> <p>The port matrix table makes sure that all these port numbers are valid. The default values can be accepted as they appear. If you have changed these values in System Manager then</p>

Field	Description
	<p>you need to make sure that these values here match them. The port matrix table is available at <a href="https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=MTAwMDkzNzE3">https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=MTAwMDkzNzE3</a>. Please contact your Avaya Support Representative for information.</p> <p><b>* Note:</b> This is a numeric value and the system displays this default value automatically.</p>
<p>Naming Service Port. PANTHER_NAMING_PORT</p>	<p>System Manager Naming Service Port</p> <p>Port used by System Manager to expose its Naming Service – defaults to 1399</p> <p><b>* Note:</b> This is a numeric value and the system displays this default value automatically.</p>
<p>System Manager Login PANTHER_LOGIN</p>	<p>System Manager Login</p> <p>The System Manager administrator login name used by System Manager to get access to its services</p> <p><b>* Note:</b> You can use the system/system username in System Manager, or you can create a Presence-specific username on System Manager with administrator privileges.</p>
<p>Password PANTHER_PASSWORD</p>	<p>The System Manager</p> <p>The password associated with the System Manager Login name</p>
<p>Secure Connection PANTHER_SECURE</p>	<p>Set to <b>true</b> to enable System Manager secure connections, or <b>false</b> to disable</p>
Presence Services Configuration settings	
<p>Router Realm ROUTER_REALM</p>	<p>Router Realm</p> <p>A unique name (within the cluster) of Presence Services instance – defaults to presence</p> <p>The <b>Realm</b> is a unique string used to identify the router and all of its components. The realm was supplied during installation. If necessary, you can change the realm after you have installed the server. To do this, you must change the realm's setting in the Global Settings Configuration screen and in the web-cm.xml file.</p>
<p>Router Cluster ROUTER_CLUSTER</p>	<p>Router Cluster</p> <p>The name of the cluster to which Presence Services belongs – defaults to cluster1</p>

Field	Description
	<p><b>* Note:</b></p> <p>The <b>Cluster</b>, specified during installation, is a unique string that identifies your XCP server installation. Clusters enable the server to use dynamic routing in high-scale installations where multiple XCP core routers are required. All of the routers that need to interact must be in the same cluster, and must be installed on the same network subnet. If necessary, you can change the cluster after you have installed the XCP server. To do this, you must change the cluster's setting in the Global Settings Configuration screen and in the web-cm.xml file.</p>
Server IP Address IP_ADDRESS	Server IP Address  IP address of Presence server – defaults to current IP address. If it is xxx.xxx.xxx.xxx, change to a valid IP address.
Collector/Distributor Support PS_CONTAINER_ENABLE	Enables the Presence container. The container is required to support Presence collectors, distributors and other associated components. Disabling this components is effectively an XCP only installation, and most other components on this panel will automatically be disabled – defaults to true  Set to <b>true</b> to enable Collector/Distributor support, or <b>false</b> to disable
Session Manager Integration	Adds integration with the Avaya Aura® Session Manager  Set to <b>true</b> to enable Session Manager integration, or <b>false</b> to disable.  The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.
SIP Client Support SIP_CLIENT_SUPPORT_ENABLE	Enables access from Avaya SIP clients through SIP PS component  Set to <b>true</b> to enable SIP client support, or <b>false</b> to disable  The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.
XMPP-IM Functionality Set to “true” to enable, or “false” to disable. XMPP_IM_ENABLE	Enables the XMPP functionality for clients, such as, Avaya one-X Communicator, Avaya 96x1 deskphones  Set to <b>true</b> to enable XMPPIM functionality, or <b>false</b> to disable  The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.
AES Collector Component	Enables the Application Enabled Services (AES) collector  Set to <b>true</b> to enable the AES Collector, or <b>false</b> to disable  The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.

Field	Description
	Set to true if you would like to collect presence information from non-SIP phones, such as, H323 and DCP telephones and SIP telephones administered as OPTIM extensions, through an AES connected to a Connection Manager.
<p><b>* Note:</b></p> <p>The installer does not display configuration pages for components that are disabled on Presence Services Configuration panel. If you enable a component on the Presence Services Configuration panel, an appropriate component configuration panel is displayed.</p>	
Available XMPP-IM Components Setting	
SIP Gateway for OCS	<p>Enables the SIP Gateway to communicate with the Office Communications Server (OCS) collector.</p> <p>Set to <b>true</b> to enable the SIP Gateway for OCS to get presence information from OCS IM federation between the Avaya clients such as, Avaya A175 Desktop Video Device or Avaya one-X Communicator to Microsoft Office Communicator clients based on OCS 2007/R2.</p> <p>Ensure that you can access the OCS server. For example, using the ping command from either side or DNS lookup. The operating system should be able to convert the host name to an IP address.</p> <p>Ensure that you can access the OCS clients. For example, using the ping command from either side or DNS lookup. The operating system should be able to convert the host name to an IP address.</p> <p>The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.</p>
Message Archiver Component MSG_ARCHIVE_ENABLE	<p>Enables a component that archives IM messages</p> <p>Set to <b>true</b> to enable the IM archiver, or <b>false</b> to disable</p> <p>The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.</p>
IM Transcripts Component	<p>Enables the Instant Messaging (IM) Transcripts component. This is used to read the archived messages</p> <p>Set to <b>true</b> to enable the IM transcripts, or <b>false</b> to disable</p> <p>The default is <b>true</b> in the graphical installation and <b>false</b> in the template installation.</p> <p><b>* Note:</b></p> <p>The IM Transcripts component is only available if the Message Archiver has been enabled.</p> <p>If you set this to false after selecting the Message Archiver Component then the system will archive your</p>

Field	Description
	messages but you will not be able to access them from the IM Transcripts Web server.
Session Manager Configuration Setting	
The Session Manager Configuration Panel is displayed only if Session Manager Integration is enabled on the Presence Components panel.	
Session Manager Addresses SESSION_MANAGER_HOST	The IP address of the Session Manager server. Enter a valid Session Manager Asset IP address. You can add multiple Session Managers using comma-separated IP addresses.
AES Component Configuration Setting	
The AES Configuration Panel is displayed only if the AES Collector is enabled on the Presence Components panel.	
AES Login AESUSERNAME	AES Login The universal login for AES servers. You must be a CTI User in AES with "Unrestricted Access".
AES Password AESPASSWORD	AES Password The universal password to for AES servers  * <b>Note:</b> Configuring Presence Services for multiple AES hosts is easier if all of the hosts support the same user name and password for Telephony Server Application Programming Interface (TSAPI) access. If this is not possible, pick one of the user name/password pairs to use with the installation and then configure the rest after installation. See the XCP help pages for more information.
SIP Gateway for OCS Configuration setting	
The SIP Gateway for OCS Panel is displayed only if the SIP Gateway for OCS component is enabled on the XMPP-IM Components panel.  If you set the SIP Gateway for OCS component to <b>false</b> , do not edit the attendant default values in the template installation.	
incOCS	Set to <b>true</b> to enable the SIP Gateway for OCS , or <b>false</b> to disable.
OCS Edge OCS_EDGE	OCS FQDN The hostname of the OCS Edge server.  * <b>Note:</b> A host name is required here (not IP address) for certificate validation purposes.  Ensure that you can access the OCS Edge server. For example, using the ping command from either side or DNS

Field	Description
	lookup. The operating system should be able to convert the host name to an IP address.
OCS SIP Domain OCS_SIP_DOMAIN_ENTRY	OCS SIP Domain  This is the sip domain used by OCS servers. For example, if you login to your Office Communications Client with User@ms.com, then the sip domain is "ms.com".
OCS SIP Port OCS_SIP_PORT	OCS SIP Port. A numeric value.  The port used by the SIP stack – defaults to 65061.
<p><b>* Note:</b> Systems that have an OCS Gateway enabled usually use a common Edge and Domain.</p>	
Presence Class IST_PRESENCE_CLASS	Presence class used for conversion from pidf document. Valid settings are: <b>Phone, Calendar, Avaya IM &lt;Jabber&gt;, Internet IM, Enterprise IM, Avaya Application, and Line of Business (LOB) Application.</b>  You do not need to manage the classes here. Refer to the Administering Presence Services guide for more information. This guide is available from <a href="http://support.avaya.com">http://support.avaya.com</a> .
<p><b>* Note:</b> Additional JSMs can be added after the Presence Services has been installed.</p>	
IM Transcripts Component setting	
<p>The IM (Instant Messaging) Transcripts web service component provides the web service interface. Third-party components use this interface to retrieve details of archived IM messages from the central presence database.</p> <p>The IM Transcript Panel is displayed only in the Advanced Mode if the IM Transcripts is enabled on the XMPP-IM Components Panel. It is not displayed in the Standard Mode as all of the default values can be safely accepted.</p> <p>If you set IM Transcripts to <b>false</b>, do not edit the attendant default values in the template installation.</p>	
IM_ENABLE	Set to <b>true</b> to enable the IM Transcripts, or <b>false</b> to disable  <b>* Note:</b> The IM Transcripts web service can be installed using only default parameters.
Database User Name IM_USERNAME	The database user name used to read IM Transcript records – defaults to xcp_user
Database Password IM_PASSWORD	The password associated with Database user name – defaults to jabber
Local Presence Database Configuration setting	
<p>The Local Presence Database Configuration Panel is displayed only in the Advanced Mode. It is not displayed in the Standard Mode as all of the default values can be safely accepted. The template installation displays all fields.</p>	

Field	Description
Password DBPASSWORD	Password The database login password – defaults to presence123
Host DBHOST	Host The machine that is used to host the local database – defaults to localhost
Port DBPORT	Port. A numeric value. The port used to connect to the local database – defaults to 5432
Database Name DBNAME	Database Name The name of the database instance used for the user data – defaults to presence
Data Replication Service Configuration setting	
The Data Replication Panel (which defines data is copied from System Manager to the local database) is displayed only in the Advanced Mode. It is not displayed in the Standard Mode as all of the default values can be safely accepted.	
External ID REPLICATION_EXTERNAL_ID	External ID Unique external id for data replication. This ID must be the fully qualified host name of the Presence server.
Node Group ID REPLICATION_NODE_GROUP_ID	Node Group ID Data Replication Node Group ID The id of the replication group – defaults to “psreplica”
Local JMX Port REPLICATION_LOCAL_JMX_PORT	Data Replication Local JMX Port Local JMX port to be used by the local Replication service – defaults to 2009
Master JMX Port REPLICATION_MASTER_JMX_PORT	Data Replication Master JMX Port JMX port of the Master Replication service System Manager server – defaults to 2009. The local JMX Port and the Master JMX Port exchange information. For example, they exchange presence status information on System Manager.   <b>Note:</b> The JMX Port is the port used by the Java Management Extensions framework. The local replication service is the client side and the Master replication service the server side of the Data Replication Service provided by System Manager.  Both the Local and Master JMX Ports should have the same value as the value of “drs.local.jmx.port”property in “\$JBOSS_HOME/server/avmgmt/deploy/

Field	Description
	symmetricds.war/WEB-INF/classes/symmetric.properties” file on the System Manager server.
Polling Interval (ms) REPLICATION_POLL_INTERVAL	Polling Interval (ms). A numeric value.  The time interval, in milliseconds, between polls for data changes – defaults to 5000
<p><b>* Note:</b></p> <p>The fully qualified host name of the Presence server as provided in the External Id parameter. The System Manager server must be able to access the Presence server. For example, using the ping command from either side or DNS lookup. The operating system should be able to convert the host name to an IP address.</p>	
Licensing Service Configuration service	
The Licensing Configuration Panel is displayed only in the Advanced Mode. It is not displayed in the Standard Mode as all of the default values can be safely accepted.	
Polling Interval for license updates	The time interval, in seconds, for polling for licence updates – defaults to 300  (LICENSING_POLL_INTERVAL)
Polling interval for license renewal	The time interval, in seconds, for polling for licence renewals – defaults to 300  (LICENSING_RENEW_INTERVAL)
SAL Logging Service Configuration setting	
SAL Organization FQDN Name SPIRIT.FQDN	This value must match the SAL Organization fully qualified domain name (FQDN) on the System Manager server  <p><b>* Note:</b></p> <p>A trailing dot (.) is required at the end of the this field.</p>
SAL Platform Qualifier Name SPIRIT.platformqualifier	This value must match the SAL Platform Qualifier name on the System Manager server  SAL Organiztion FQDN Name – with trailing dot (‘.’)  The SAL Organization FQDN Name and SAL Platform Qualifier Name values must match the values on the setting on the System Manager server. To obtain these values log into the System Manager GUI and select <b>System Manager Data &gt; Settings &gt; SPIRIT &gt; DataTransportConfig</b> .
<p><b>* Note:</b></p> <p>The SAL Organization FQDN Name and SAL Platform Qualifier Name values must match the values on the setting on the System Manager server. To obtain these values log into the System Manager GUI and select <b>System Manager Data &gt; Settings &gt; SPIRIT &gt; DataTransportConfig</b>.</p>	
Trust Management Service Configuration setting	
Enrollment Pasword	This is the simple certificate enrollment password provided for Presence servers

Field	Description
SCEP_PASSWORD	<p> <b>Note:</b></p> <p>This System Manager enrollment password must not have expired.</p>
<p> <b>Note:</b></p> <p>The <b>Enrollment Password</b> value must match the password on the System Manager server. To obtain this value log into the System Manager GUI and select <b>Security &gt; Certificates &gt; Enrollment Password &gt; End Entity Profiles</b>. The <b>End Entity Profiles</b> value must match the System Manager server. To see the available profiles log into the System Manager GUI and select <b>Security &gt; Certificates &gt; Authority &gt; Edit End Entity Profiles</b>.</p> <p> <b>Important:</b></p> <p>Presence Services does not get installed if the enrollment password contains a dollar (\$) sign.</p>	
End Entity Profiles TM_SCEP_PROFILE	<p>Avaya recommends that Presence Services users only use the INBOUND_OUTBOUND_TLS profile – defaulted to INBOUND_OUTBOUND_TLS</p> <p>End Entity Profiles. Valid settings are: INBOUND_OUTBOUND_TLS, OUTBOUND_TLS, INBOUND_TLS, and EMPTY.</p> <p>Transport Layer Security (TLS) is the definition of the security layer between Presence Services and System Manager. System Manager only supports "INBOUND_OUTBOUND_TLS" in this release.</p>
Summary Panel	The Summary Panel reminds which packs to install and to what location. If you do not want to install Presence Services, then click <b>Quit</b> button.
Installation Panels	The Installation Panels show you how the installation is progressing. This information is written to a log file at: <code>/opt/Avaya/Presence/</code> . If for some reason the installation fails, this file contains useful diagnostic information. The installation typically takes about 25 minutes, depending upon the components that need to be installed, hardware, and network performance.
Installation Summary Panel	The Installation Summary Panel is displayed when the installation is complete. You are prompted to install the Presence Services License to System Manager before continuing. You will also be able to open the XCP home page. When you click on the <b>Done</b> button the silent installation files are written to <code>/opt/Avaya</code> .

# Appendix F: Sample deployment configurations

## OCS Gateway configuration worksheet

The OCS Gateway configuration worksheet identifies the set of configuration parameters that are when you enable an OCS Gateway. It is important that you know the values for the following parameters before starting the configuration process.

Configuration parameter Name	Parameter value	Default valued presented on the configuration screen
OCS Domain		
PS SIP Domain <sup>16</sup>		The service router name configured during installation, for example, pres.ipsdemo.com.
Transport		tls
Port <sup>17</sup>		
Expires		86400
Subscription Failure retry		3600
Server Failure retry		3600
PS IP address		
SIP Proxy Port <sup>18</sup>		
PS server FQDN		
SIP SUBSCRIBE Contact Port <sup>19</sup>		
TLS keystore full file path <sup>20</sup>		
TLS trust store full file path <sup>21</sup>		

<sup>16</sup> The Service Router Name solicited during the installation process is the Presence Services presence domain.

<sup>17</sup> The system provides a default port, 5061. You must change this port to a free port, typically to 65061. The convention for backend SIP servers is to use 5061 with an integer value from the set 1,2,3,4,5,6 prepended to create the port. Note that any value greater than 6 pushes the port value beyond the acceptable range of TCP ports.

<sup>18</sup> The SIP Proxy port is 5061.

<sup>19</sup> The contact port should be that of the SIP Proxy, that is 5061.

<sup>20</sup> Currently, TLS keystore full file path is `/opt/Avaya/Presence/jabber/xcp/certs/generic.pem.jabber`

<sup>21</sup> Currently, TLS trust store full file path is `/opt/Avaya/Presnce/jabber/xcp/certs/generic.trusts`

# Appendix G: Process flow of a SIP Subscribe

---

## The SIP OCS Gateway component

---

### Inbound requests

The inbound requests originate from the OCS/Lync and route through the OCS/Lync Edge server and the Presence Services SIP Proxy. The Presence Services SIP Proxy is instrumental in directing SIP requests from the OCS/Lync system to the OCS Gateway. You can achieve this through the routing rules defined in SIP Proxy. Inbound SIP requests are subject to routing rules, which are defined on the To and From header fields of a SIP request. The inbound routing rules directs certain SIP requests originating from an OCS/Lync system to the OCS Gateway.

#### Related Links

[Overview - OCS Gateway](#) on page 169

---

### Outbound requests

The outbound requests are the SIP requests that the system initiates as a result of Avaya Aura<sup>®</sup> client initiated requests destined for an OCS/Lync enterprise user. These requests are processed by Presence Services and are routed internally through the OCS Gateway. In the current Presence Services implementation, these requests are XMPP requests that originates from an Aura client.

For example, an Avaya Aura<sup>®</sup> enterprise user logged on a 1XC-H.323 or 1XC-SIP client can click on a user in their contact list and initiate an IM with that peer enterprise user. The 1XC clients then indicates that the target user has two IM addresses: an Avaya Aura<sup>®</sup> XMPP handle and an OCS/Lync handle. If the initiating user selects the OCS/Lync handle, then the Avaya Aura<sup>®</sup> client sends an XMPP IM message to Presence Services and then Presence Services routes this IM message internally through the OCS Gateway. This is because the system configures the OCS Gateway to handle communications with the OCS/Lync domain and the address used in the request contains the OCS/Lync domain.

Outbound SIP requests route through a SIP Proxy of Presence Services, then to the OCS/Lync Edge, and then into the OCS/Lync server. The SIP communication is based on a federated deployment of Presence Services with OCS/Lync. The configuration on OCS/Lync Edge is for

federated inter-working. Therefore, you must configure Presence Services for federation as an IM provider on the OCS/Lync Edge server.

Additionally, to establish TLS communications and achieve server authentication, it is necessary that the CA TLS/SSL certificate of the Certificate Authority, which signed the TLS/SSL certificates of Presence Services and OCS/Lync Edge, are imported into each of the trust stores on Presence Services and the OCS/Lync Edge respectively. With the appropriate Presence Server Host records and SRV records configured in the DNS service associated with the OCS/Lync Edge and the OCS/Lync server, you establish this trust relationship.

Use the following domains as an illustration:

- The PS domain is pres.ipsdemo.com
- The OCS/Lync domain is ipsdemo.com
- The PS server FQDN is ipsdemo-ips1.ipsdemo.com
- The OCS/Lync Edge server external FQDN is ipsdemo-winsrv2.glob.ipsdemo.com
- The OCS/Lync server is ipsdemo-winsrv1.glob.ipsdemo.com

If you are enabling the OCS Gateway during installation, then you must know the appropriate values for the following parameters on the Presence server:

- OCS/Lync Edge: The external FQDN of the OCS/Lync Edge server, for example, ipsdemo-winsrv2.glob.ipsdemo.com
- OCS/Lync SIP domain: The OCS/Lync domain, for example, ipsdemo.com
- OCS/Lync SIP Port: 65061

These parameters set up the OCS Gateway configuration together with the default settings for non-solicited parameters. You can also use these parameters to configure the OCS Gateway routing rules in the SIP Proxy.

The SIP Proxy plays an integral part in the processing of a SIP request that the system sends to the OCS/Lync server and in handling the SIP requests received from the OCS/Lync server to Presence Services. You must define routing rules in the SIP Proxy, which routes SIP requests to their appropriate destination servers. Two rules govern the flow of SIP requests to and from OCS/Lync:

- The outbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests from Presence Services to OCS/Lync have a rule which specifies that if the To header is set to the OCS/Lync domain and if the From header is from the Presence Services domain, then you must apply the default SIP routing rule.
- The inbound SIP (SUBSCRIBE, INVITE, ACK, NOTIFY) requests have a rule which specifies that if the To header contains the Presence Services domain and the From header contains the OCS/Lync domain, then the request is to be routed to the OCS Gateway.
- The default SIP routing rules determine the destination IPS address of the target domain. This requires the configuring of a Host mapping in the Proxy. This Host mapping maps an OCS/Lync domain to the external FQDN of the OCS/Lync Edge server. The external FQDN of the OCS/Lync edge server must be resolvable and requires an entry in the /etc/hosts file.

### Related Links

[Overview - OCS Gateway](#) on page 169

---

## Initiating a SIP SUBSCRIBE from the OCS server to Presence Services

A SIP SUBSCRIBE is initiated from the OCS server to an Avaya Aura® user when the OCS user adds the presence handle of an Avaya Aura® user to their buddy list. Following are the possible scenarios:

- Scenario 1: Avaya Aura® user is logged on the SIP client and the pending subscription notified in watcher information.
- Scenario 2: Avaya Aura® user is logged on an XMPP client (1XC-H323), and the pending subscription delivered in an XMPP subscribe packet.
- Scenario 3: Avaya Aura® user is logged on a legacy phone, and the pending subscription remains pending as the end user will not receive a notification of the pending subscription.

### Avaya Aura® user is logged on the SIP 1XC client

- MOC/Lync user adds a presence handle of an Avaya Aura® user to the buddy list. The handle contains the Presence Services domain.
- OCS server sends SIP SUBSCRIBE from an OCS user to the presence handle of the Avaya Aura® user.
- DNS resolution routes the SIP SUBSCRIBE to OCS Edge server.
- OCS Edge server resolves the Presence Services domain to the Presence server host.
- OCS Edge sends SIP SUBSCRIBE to the Presence server (SIP Proxy).
- SIP Proxy authenticates the OCS Edge server during the TLS session creation.
- SIP Proxy receives SIP SUBSCRIBE from OCS-domain to Presence Services-domain.
- SIP Proxy applies routing rules and forwards SIP SUBSCRIBE to OCS Gateway.
- OCS Gateway sets up SIP session and sends 200 OK response.
- OCS Gateway internalizes the SIP SUBSCRIBE to an internal XMPP subscribe.
- Presence Services processes subscribe and sets up pending roster subscription.
- Authorization Manager checks ACLs, but as the From address is not an Avaya Aura® user, Authorization Manager checks the Federation Domain configuration. Subscribe is treated as CONFIRM and requires explicit user authorization.
- SIP Presence Services sends NOTIFY presence.winfo to Avaya Aura® SIP client with pending subscription.
- SIP Presence Services sends NOTIFY through Session Manager, using the Route Set created.
- SIP clients authorizes the subscribe using PUBLISH presence.wauth.
- SIP Presence Services sends a subscribed packet to authorize internal roster subscription.
- XMPP Roster is updated from pending to FROM.
- OCS Gateway receives subscribed packet and creates a 200 OK response.
- OCS Gateway sends 200 OK response to OCS Edge server through the SIP Proxy.
- SIP Proxy receives 200 OK response and forwards to OCS Edge on an existing connection.

- OCS Gateway creates NOTIFY status pending empty body.
- OCS Gateway sends NOTIFY to OCS Edge through SIP Proxy.
- SIP Proxy applies Outbound routing rules To OCS-domain From Presence Services-domain.
- SIP Proxy resolves OCS-domain to the OCS Edge server.
- SIP Proxy sends NOTIFY to the OCS Edge server.
- Composite presence of Aura user (subscriber) is generated for the OCS user.
- Composite presence sent to OCS Gateway.
- OCS gateway applies composite presence mapping policy and maps the Aura user's overall presence. This is the first activities element in the composite PIDF's person element into a single tuple PIDF document.
- OCS Gateway sends NOTIFY to the OCS user through a SIP Proxy, as per outbound proxy configured in OCS Gateway.
- SIP Proxy receives NOTIFY and applies routing rule: To OCS-domain From Presence Services-domain and routes request to OCS edge.
- OCS Edge resolves the NOTIFY and forward to the OCS server of the user.
- OCS server delivers presence to the MOC/Lync client of the user.

Internally, the SIP SUBSCRIBE for presence from OCS is managed as an XMPP Roster subscription, which is a permanent subscription. This remains extant until the subscription is explicitly removed, for example, a SIP SUBSCRIBE with a value, expires = 0. This value is translated internally to unsubscribe the request, and the XMPP roster subscription of the OCS user is removed.

**\* Note:**

The presence NOTIFY from the OCS Gateway is routed through the SIP Proxy. Ordinarily, this does not happen, but for the OCS Gateway, the outbound proxy configuration is set to create a next hop node as the SIP Proxy. An Aura SIP client is informed about a pending subscription through a watcher information notification. The authorization of the subscription is performed by sending a SIP PUBLISH on the presence.wauth package.

**Avaya Aura® user is logged on the XMPP 1XC-H323 client**

- MOC user adds a presence handle of an Avaya Aura® user to the buddy list. The handle contains the Presence Services domain.
- OCS server sends SIP SUBSCRIBE from an OCS user to the presence handle of the Avaya Aura® user.
- DNS resolution routes the SIP SUBSCRIBE to OCS Edge server.
- OCS Edge server resolves the Presence Services domain to the Presence server host.
- OCS Edge sends SIP SUBSCRIBE to the Presence server (SIP Proxy).
- SIP Proxy authenticates the OCS Edge server during the TLS session creation.
- SIP Proxy receives SIP SUBSCRIBE from OCS-domain to Presence Services-domain.
- SIP Proxy applies routing rules and forwards SIP SUBSCRIBE to OCS Gateway.
- OCS Gateway sets up SIP session and sends 200 OK response.

- OCS Gateway internalizes the SIP SUBSCRIBE to an internal XMPP subscribe.
- Presence Services processes subscribe and sets up pending roster subscription.
- Authorization Manager checks ACLs, but as the From address is not an Avaya Aura® user, Authorization Manager checks the Federation Domain configuration. Subscribe is treated as CONFIRM and requires explicit user authorization.
- Presence Services sends XMPP subscribe packet to XMPP client of the Avaya Aura®.
- Aura XMPP clients authorizes the subscribe sending an XMPP subscribed.
- XMPP Roster is updated from pending to FROM.
- OCS Gateway receives subscribed packet and creates a 200 OK response.
- OCS Gateway sends 200 OK response to OCS Edge server through the SIP Proxy.
- SIP Proxy receives 200 OK response and forwards to OCS Edge on an existing connection.
- OCS Gateway creates NOTIFY status pending empty body.
- OCS Gateway sends NOTIFY to OCS Edge through SIP Proxy.
- SIP Proxy applies Outbound routing rules To OCS-domain From Presence Services-domain.
- SIP Proxy resolves OCS-domain to the OCS Edge server.
- SIP Proxy sends NOTIFY to the OCS Edge server.
- Composite presence is generated for the OCS user.
- Composite presence sent to OCS Gateway.
- OCS Gateway applies composite presence mapping policy and maPresence Services Enterprise IM presence tuple to OCS PIDF. MaPresence Services highest priority tuple from composite PIDF.
- OCS Gateway sends NOTIFY to the OCS user through a SIP Proxy, outbound proxy configured in OCS Gateway.
- SIP Proxy receives NOTIFY and applies routing rule: To OCS-domain From Presence Services-domain and routes request to OCS edge.
- OCS Edge resolves the NOTIFY and forward to the OCS server of the user.
- OCS server delivers presence to the MOC client of the user.

**\* Note:**

The main difference between this flow and the SIP flow is that the subscribe packet is delivered to the Avaya Aura® XMPP client to indicate a pending subscribe. In the SIP case, the watcher information informs the client about a pending subscription.

**Avaya Aura® user logged on a legacy phone**

The subscription remains pending. The subscription is not authorized until the user logs on another device which can support the explicit authorization of the pending subscription.

---

## Initiating an IM conversation from Presence Services to the OCS server

An Avaya Aura® user can initiate an IM conversation with another enterprise user by adding the user as a contact and then clicking on the IM icon on the Avaya Aura® client interface. This action renders the IM contact addresses for that contact user. If the system provisions an OCS handle for the Avaya Aura® user, then the system initiates an IM conversation using the OCS contact address. The flow of such an IM conversation is as follows:

- Avaya Aura® user clicks on the IM icon of the contact user and then selects an OCS handle.
- Avaya Aura® user types a message and presses Enter to send the message.
- Avaya Aura® client sends XMPP message from an Avaya Aura® presence handle to an OCS handle.
- Presence Services Connection Manager receives message and routes the message to the OCS Gateway.
- OCS Gateway sets up a SIP session.
- OCS Gateway sends an invite to an OCS user handle from the presence handle.
- SIP Proxy receives an invite and applies outbound routing rule To OCS-domain From PS-domain.
- SIP Proxy sends invite to the OCS Edge server.
- The OCS Edge server resolves the OCS user address and sends an invite to the OCS server.
- The OCS server sends an invite to the MOC/Lync client of an OCS user.
- The system accepts an IM conversation and sends 200 OK response to OCS Gateway through the OCS Edge server and SIP Proxy.
- OCS Gateway sends ACK to complete the offer/answer exchange.
- The system converts XMPP IM message into SIP MESSAGE.
- The system sends SIP MESSAGE to SIP Proxy.
- SIP Proxy applies outbound routing rules and sends SIP MESSAGE to the OCS Edge server.
- OCS Edge routes MESSAGE to the OCS server.
- The OCS server delivers MESSAGE to MOC/Lync client.

---

## Initiating an IM conversation from the OCS server to Presence Services

A user on a MOC/Lync client can initiate an IM conversation with another Avaya Aura<sup>®</sup> user by using the presence handle of the Avaya Aura<sup>®</sup> user.

- MOC/Lync user clicks the Avaya Aura<sup>®</sup> presence user handle on the buddy list.
- MOC/Lync user types a message and presses Enter to send the message.
- MOC/Lync client sends SIP INVITE from the OCS user handle to the presence user handle.
- OCS Edge resolves the Presence Services domain to the Presence server host.
- OCS Edge sends SIP INVITE to SIP Proxy.
- SIP Proxy receives SIP INVITE and applies inbound routing rule To PS-domain From OCS-domain and sends SIP INVITE to OCS Gateway.
- OCS Gateway creates SIP session and sends 200 OK to complete the dialog.
- The OCS Edge server forwards ACK to SIP Proxy.
- SIP Proxy receives ACK and applies inbound routing rule To PS-domain From OCS-domain and sends SIP ACK to OCS Gateway.
- OCS Gateway receives ACK.
- The OCS Edge server forwards SIP INFO with a typing status to SIP Proxy
- SIP Proxy receives SIP INFO and applies inbound routing rule To PS-domain From OCS-domain and sends SIP INFO to OCS Gateway.
- OCS Gateway receives SIP INFO.
- OCS Gateway converts SIP INFO into XMPP message with chat state notification is composing.
- OCS Gateway sends an XMPP message to an Avaya Aura<sup>®</sup> user XMPP IM session.
- Presence Services Connection Manager forwards XMPP is composing message to the client of the Avaya Aura<sup>®</sup> user.
- OCS Edge server forwards SIP MESSAGE to SIP Proxy.
- SIP Proxy receives SIP MESSAGE and applies inbound routing rule To PS-domain From OCS-domain and sends SIP MESSAGE to OCS Gateway.
- OCS Gateway receives SIP MESSAGE.
- OCS Gateway converts the SIP MESSAGE to an XMPP message.
- OCS Gateway sends an XMPP IM message to the XMPP IM session of the Avaya Aura<sup>®</sup> user.
- Presence Services Connection Manager forwards XMPP is composing message to the client of the Avaya Aura<sup>®</sup> user.

# Appendix H: Configuration parameters and references

---

## SIP Proxy parameter reference

Presence Services has different User Agent (UA) servers to handle different SIP packages. To avoid contention, the UAs bind to different ports. A local stateless SIP proxy provides a single SIP address into a Presence Services node. This local proxy takes incoming requests on standard SIP ports and send the request by proxy over the local host to the appropriate SIP UA.

Given that the local proxy is the point of entry for all SIP requests into the Presence Services node, it can also perform the trusted host checks. The proxy communicates to other UAs through local host sockets so the local host is the UAs trusted host.

This section provides a reference for all of the parameters associated with the SIP Proxy component. The parameters are divided into subsections based on the configuration view in which the system displays them.

### Related Links

[SIP Proxy basic parameters](#) on page 308

[SIP Proxy intermediate parameters](#) on page 309

[SIP Proxy advanced parameters](#) on page 311

---

## SIP Proxy basic parameters

### Description

This parameter figures in the Components area on the main page of Presence Services XCP Controller Web interface. It helps you distinguish between components of the same type when you have more than one configured components. You can change the description as needed.

### Realm of the global configuration

Enables to specify the primary servers realm if you configure a list of trusted TLS hosts on your primary XCP server.

### SIP proxy routing rules

Enables to add routing rules for the SIP proxy.

## Default rule

This option enables to use to handle SIP requests that do not meet any of the configured routing rules.

## Forward request

Enables the system to forward SIP requests that do not meet any of the configured routing rules to specific hosts.

## Bounce request

Enables the system to bounce SIP requests that do not meet any of the configured routing rules.

## Percentage of max memory to use for the SIP stack

This memory is allocated when the SIP proxy system starts, so make sure that you have the memory available.

## Remote host configuration

### ID of the component to get this configuration from

This parameter is specific to SIP gateways. If you already have a SIP Host configured for another gateway, you can enter the ID of the component here to use the same configuration.

### Local configuration

Enables to configure a new SIP host.

### Add a new SIP transport

Enables to specify the type of transport protocol that the SIP clients are using. You can select the type of transport protocol as UDP, TCP, or TLS.

### Timeout for notify response to subscriptions with expires=0 (seconds)

The number of seconds to wait before the system times out the response for a Presence request.

---

## SIP Proxy intermediate parameters

### Router outbound connection information

Enables the Presence Services router to connect to the component. For example, if the component is running outside your firewall, using this option, the router can connect to the component safely rather than introducing security risks by letting the component connect to it. By default, components connect to the router using the routers Master Accept Port.

### Component IP

The IP address or host name of the system on which the component is installed.

## Port

The port that the component uses for communications.

## Password

The password that the router uses to authenticate the component.

## Execute an external command

Using this option, the router can start the component automatically. If you prefer to start the component from a command line, disable this option.

## Command line to run

A default command runs the component automatically. You can modify it, if needed.

### \* Note:

Do not use the `-B` argument with this component. Since the IPS logger is already a daemon process, its children must not be daemons.

Do not redirect output, because all output to `STDOUT` and `STDERR` are redirected to `/dev/null`.

## Hostnames for this component

This option specifies the hosts for which this component handles packets. Specify a host filter only if you want the component to be externally addressable. For example, if you want clients and other components or programs to communicate with it. This is because the `mod_disco` module in JSM uses host filters to return the component as something that is discoverable.

## Host Filters

The host names or IP addresses for which you want this component to handle packets. Separate each host name or address with a line break.

Host filters must be host names, or IPv4 or IPv6 addresses. If you use an IP address, the packet address must also use this IP address.

## Outbound proxy

You can ignore this option unless you are chaining SIP Proxy components. If you need to chain SIP proxies, contact technical Support.

## Proxy IP address

The IP address of the system on which the SIP Proxy is running.

## Proxy port

The SIP stack port being used by the proxy. This is the port of the transport the proxy is using.

## Proxy transport

The type of transport being used by the SIP Proxy.

## Component Logging (Jlog)

Enables to configure filtered level loggers that log messages to syslog and to a stream (stderr or stdout). You can enable either or both the syslog and stream loggers. These parameters are displayed in the controller's Intermediate and Advanced configuration views.

## SNMP Configuration

Select this option if you want to configure SNMP for the component.

### Enable SNMP

Leave this parameter set to Yes.

---

## SIP Proxy advanced parameters

### Runlevel

The order in which this component shuts down. The runlevel must be an integer value greater than or equal to 0. Component shutdown is executed in reverse order of the specified runlevel; components with the highest level (typically 80) shut down first.

 **Note:**

Do not change the runlevel unless you know exactly what you are doing and understand the effects that changing it will have. The default runlevel is provided to help the system shut down as smoothly as possible, and is based on this component's dependencies upon other components.

### Timeout for shutdown

The number of seconds that the server waits to receive acknowledgement from the component that the shutdown process has completed. If the component has not shut down by the time this time period has elapsed, the router leaves the process in its current state and continues shutting down other processes.

## Component properties

### Number of packets buffered when component is down

The number of packets bound for the component that must be buffered if the component goes down.

### Bounce error packets to stderr

Enables the router to send warnings to stderr when the component is down.

## Router outbound connection information

### Buffer size in bytes for outgoing data

The number of bytes the router must buffer when it sends information to the component. You may want to modify this element when working on performance enhancements.

### Buffer size in bytes for incoming data

The number of bytes the router must buffer when it receives information from the component. You may want to modify this element when working on performance enhancements.

### Send keepalives

Enables the router to send keep-alives to the component. The keep-alive helps prevent firewalls from dropping an unused connection to the component. If this option is set to `NO`, keep-alives are disabled.

### Log the delivery of packets to this component

Enables to log the data that the router delivers to the component. The information is logged to the loggers you set up during Presence Services Logger configuration (syslog, file, or stderr). Socket-level logging happens only at the debug level.

## Execute an external command

### Maximum interval in seconds to wait before restarting component

The maximum number of seconds after which the router tries to restart the component. If the component goes down, the router tries to restart it after 1 second. If the component does not start, the router multiplies the wait time by 1.5, and tries again. Once the maximum time interval that you specify for this parameter is reached, the router continues to retry after waiting this amount of time.

### Maximum number of times to restart component

The total number of restarts allowed. The default setting, `-1`, means unlimited.

### Interval in seconds at which to reset this value to 1 second

The number of seconds that the component has been up and running, after which to set the restart time back to 1 second.

### Path to binary

The directory path to the shell that launches the component. You can change the default setting if needed.

## SIP Proxy Tuning Parameters

### Server Connection Idle Timeout (seconds)

The number of seconds of idle time after which the SIP Proxy connection closes. If you prefer, you can enter `-1` to prevent the connection from ever timing out or `0` to timeout immediately after this component sends a final response to a SIP request. Setting the timeout to `0` is not recommended.

### Max TCP connections

The maximum number of active TCP connections allowed at one time.

**Max TLS sessions**

The maximum number of active TLS sessions allowed at one time.

**Thread count for SIP processing**

The number of threads you want to use for SIP processing.

**Interval to wait for SIP dialogs to shutdown cleanly before exiting the application**

The number of seconds to wait for SIP dialogs to shut down before the SIP Proxy stops.

**Maximum SIP subscription duration (seconds)**

The maximum number of seconds after which SIP subscriptions refresh. The Presence server negotiates with the SIP host within the range created by this value and the minimum value.

**Default SIP subscription duration (seconds)**

The default number of seconds after which SIP subscriptions refresh.

**Minimum SIP subscription duration (seconds)**

The minimum number of seconds after which SIP subscriptions refresh. The Presence server negotiates with the SIP host within the range created by this value and the maximum value.

**Maximum SIP publish duration (seconds)**

The maximum number of seconds after which SIP publishes refresh. The Presence server negotiates with the SIP host within the range created by this value and the minimum value.

**Default SIP publish duration (seconds)**

The default number of seconds after which SIP publishes refresh.

**Minimum SIP publish duration (seconds)**

The minimum number of seconds after which SIP publishes refresh. The Presence server negotiates with the SIP host within the range created by this value and the maximum value.

**Send/Receive buffer size (bytes)**

The number of bytes in the buffer that is used to send and receive SIP messages. The buffer must be large enough to hold the largest SIP Notify message and the largest pidf Presence body that you plan to support.

**TLS connection strict checking of hostname**

Enables the XCP server to verify that the name of the host making the TLS connection matches the host name that is in the certificate from that TLS connection.

**Expiration for a DNS Cache entry (seconds)**

The number of seconds that the XCP server caches the Presence server hosts DNS entry.

**Enable logging of SIP packets**

Enables to debug logging of SIP packets is enabled.

 **Caution:**

Activating this option can severely slow down the Presence servers performance

**Enable full SIP stack logging**

Enables to debug logging of the SIP stack is enabled.

 **Caution:**

Activating this option can severely slow down the Presence servers performance.

**Component Logging (Jlog)**

**Add a new custom logger**

If you create a custom logger for logging component information using the libjcore library, click **Go** to access the Custom Logger Configuration page.

**SNMP Configuration**

**Count errors**

Enables SNMP error counting.

 **Note:**

This option takes a great deal of server resource. Therefore, use it with caution.

# Appendix I: Presence Services cluster solution overview

---

## Presence Services cluster configuration

A Presence Services cluster can support up to eight nodes within the cluster and an additional node as a standby backup server. You must initially install each Presence Services server in the cluster as a standalone server. You must then form the cluster by configuring Router-to-Router (R2R) components on Presence Services servers in the cluster.

 **Note:**

In Presence Services 6.2, you no longer need to reinstall Presence Services server to add the server to the cluster, provided the Realm must be unique in the cluster.

### Related Links

[Configuring the Router-to-Router component](#) on page 315

[Sample R2R configuration](#) on page 316

[Verifying the jsmlID and SIP entity of Presence Services](#) on page 318

[User provisioning](#) on page 318

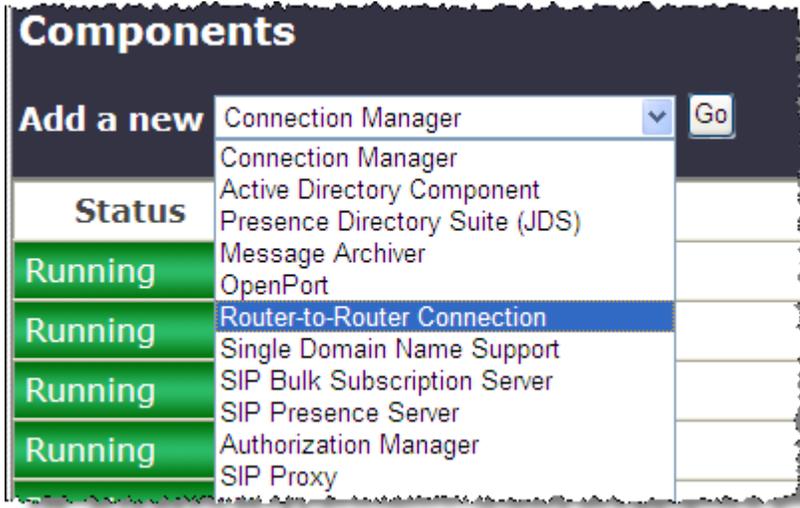
---

## Configuring the Router-to-Router component

### Procedure

1. Log on to the Presence Services XCP Controller web interface using the cust credentials.
2. Select the **Advanced configuration** view.

- In the **Components** section, in the **Add a new** field, select **Router-to-Router Connection** and then click **Go**.



The system displays the Router-to-Router Connection Configuration page.

- In the **Component IP** field, type the IP address of the Presence Services server with which this R2R component will communicate.
- Click **Submit**.
- Repeat Step 3 to Step 5 for all R2R components.
- Restart the Presence Services server.
- To verify the connection, run the `netstat n.n.n.n` command, where *n.n.n.n* is the IP address of other Presence Services server in the cluster.

### Related Links

[Presence Services cluster configuration](#) on page 315

## Sample R2R configuration

	2 node cluster	3 node cluster	4 node cluster	5 node cluster	6 node cluster	7 node cluster	8 node cluster
PS-1	R2R to PS-2	R2R to PS-2	R2R to PS-2 R2R to PS-3	R2R to PS-2 R2R to PS-3	R2R to PS-2 R2R to PS-3 R2R to PS-4	R2R to PS-2 R2R to PS-3 R2R to PS-4	R2R to PS-2 R2R to PS-3 R2R to PS-4 R2R to PS-5

PS-2	-	R2R to PS-3	R2R to PS-3 R2R to PS-4	R2R to PS-3 R2R to PS-4	R2R to PS-3 R2R to PS-4 R2R to PS-5	R2R to PS-3 R2R to PS-4 R2R to PS-5	R2R to PS-3 R2R to PS-4 R2R to PS-5 R2R to PS-6
PS-3	-	R2R to 1	R2R to PS-4	R2R to PS-4 R2R to PS-5	R2R to PS-4 R2R to PS-5 R2R to PS-6	R2R to PS-4 R2R to PS-5 R2R to PS-6	R2R to PS-4 R2R to PS-5 R2R to PS-6 R2R to PS-7
PS-4	-	-	R2R to 1	R2R to PS-5 R2R to 1	R2R to PS-5 R2R to PS-6	R2R to PS-5 R2R to PS-6 R2R to PS-7	R2R to PS-5 R2R to PS-6 R2R to PS-7 R2R to PS-8
PS-5	-	-	-	R2R to 1 R2R to 2	R2R to PS-6 R2R to 1	R2R to PS-6 R2R to PS-7 R2R to 1	R2R to PS-6 R2R to PS-7 R2R to PS-8
PS-6	-	-	-	-	R2R to 1 R2R to 2	R2R to PS-7 R2R to 1 R2R to 2	R2R to PS-7 R2R to PS-8 R2R to 1
PS-7	-	-	-	-	-	R2R to 1 R2R to 2 R2R to PS-3	R2R to PS-8 R2R to 1 R2R to 2
PS-8	-	-	-	-	-	-	R2R to 1 R2R to 2

							R2R to PS-3
--	--	--	--	--	--	--	-------------

### Related Links

[Presence Services cluster configuration](#) on page 315

---

## Verifying the jsmlD and SIP entity of Presence Services

### Procedure

1. Log on to the System Manager web console.
2. Navigate to **Elements > Routing > Domains**.
3. Verify that the entry has been created for the installed Presence Services server.
4. Navigate to **Services > Inventory > Manage Elements**.
5. Note the value of the **Name** field.
6. Click the Attributes tab.
7. Verify that the **jsmlD** field shows **jsm-1.<Presence Services realm>**.
8. Verify that the SIP entity has been created after Presence Services is installed:
  - a. Navigate to **Elements > Routing > SIP Entities**.
  - b. Select the check box next to the Presence Services entry, and click **Edit**.
  - c. Verify that the value of the **Name** field matches with the value that you noted in Step 5.

### Related Links

[Presence Services cluster configuration](#) on page 315

---

## User provisioning

In a Presence Services cluster, you can assign users to a single Presence Services server using the communication profile of the user on System Manager. You cannot assign users to the Presence Services server till you configure the presence domain, Presence Services inventory entry and Presence Services server SIP entity on System Manager. This configuration is part of user provisioning. Users can be provisioned in System Manager prior to installing Presence Services, but the users will not be presence enabled until Presence Services is installed and the provisioning of that user is updated.

### Related Links

[Presence Services cluster configuration](#) on page 315

## **Appendix J: Known Issue – Configuring Presence Server as the Exchange Server URL in the XCP configuration**

If the Presence Server itself is configured as the Exchange Server URI in the XCP configuration, this has a significant negative impact on Exchange Collector performance. The expected behavior, on configuring an invalid URL, is for the autodiscovery service to be called for each mailbox and subsequent refresh periods will flush out the invalid URL when it eventually is deemed to have no mailboxes associated with it. This is the actual behavior for invalid URL's other than the localhost. When 'localhost', '127.0.0.1' or '<Presence Server IP>' is specified in the Exchange Server URI, the web service call hangs on every second or third request and the length of time for which it hangs increases each time. The impact of this issue is that it would take a considerable length of time for the Collector to autodiscover the valid URL for all mailboxes.

# Glossary

**Avaya SIP Enablement Services**

Avaya servers running SIP Enablement Services perform proxy, registration, and redirection functions associated with SIP applications.

**CAM**

Avaya one-X<sup>®</sup> Agent Central Management is an optional Web-based solution that Avaya one-X<sup>®</sup> Agent customers can deploy based on their management requirement. It manages the operation for contact centers running Avaya one-X<sup>®</sup> Agent and provides the ability to manage all Avaya one-X<sup>®</sup> Agent features.

**Fully Qualified Domain Name**

The complete domain name for a specific host computer on the Internet. Fully Qualified Domain Name (FQDN) consists of the host name and the domain name, which includes the top-level domain. Every Web server requires a Domain Name System (DNS) server to translate FQDNs to IP addresses.

**Local Presence Services (LPS)**

Presence aware applications may use the Local Presence Services (LPS) to subscribe to Presence Services. Presence Services uses LPS to efficiently transfer presence information between the Presence Services server and the application servers.

**OCS Gateway**

OCS Gateway provides federation capability between the Presence Server and an OCS server, to enable peer-to-peer presence and IM between clients connected to Presence Server and Microsoft Office Communicator.

**Presence server**

Presence server collects presence information from various sources, such as Application Enablement Services (AES), Microsoft Office<sup>™</sup> Communicator Server (OCS), and eXtensible Messaging and Presence Protocol (XMPP) Server for presentities retrieved from User Data Store and distributes the presence of a given class, such as phone and enterprise IM users.

**Presence Services**

Presence Services is a single point of presence collection. It supports presence information gathering from a diverse range of sources. This information is aggregated on a per user basis, and then made available to presence aware applications.

**Presence Services Core eXtensible Communication**

Maintains a list of presence fragments for a given presentity and performs composition of these fragments. The Core XCP is the conduit between the collectors and distributors of presence information in the system.

**Platform (XCP)  
server****Solution Element  
(SE)**

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway.

**System Manager**

System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components.

**The SIP Bulk  
Subscription Server**

Supports bulk distribution of presence so that the transfer of presence information between Presence Services and LPS is efficient.

**XMPP Server**

An XMPP server that is used as a Presence source should be capable of handling large rosters.

# Index

## Special Characters

[./presuseracls](#) ..... [266](#)  
[./swversion.sh](#) ..... [234](#)

## A

Access Level ..... [274](#)  
access Levels ..... [271](#)  
ACL ..... [127](#), [273](#)  
acl script ..... [269](#)  
adding  
    Presence Service components ..... [49](#)  
    Session Manager ..... [43](#)  
adding a DNS SRV record ..... [151](#)  
adding AES ..... [50](#)  
adding AES Collector ..... [50](#)  
adding an entity link ..... [46](#)  
adding contacts ..... [277](#)  
adding endpoint profile ..... [54](#)  
adding exchange user handles on system manager ..... [69](#)  
adding Lotus Notes handle to a Domino user ..... [91](#)  
adding Presence Services as a SIP entity ..... [45](#)  
adding presentities ..... [128](#)  
administering Presence configuration properties ..... [23](#)  
advanced configuration view ..... [17](#)  
AES ..... [15](#), [50](#), [53](#), [55–57](#), [59](#), [263](#)  
AES Certificate ..... [53](#)  
AES Collector ..... [57](#)  
    system default value ..... [54](#)  
AES IP address ..... [263](#)  
AES Password ..... [56](#)  
AES Username ..... [56](#)  
AFT Handler ..... [118](#)  
Alarm ..... [240](#)  
allowing for Exchange Collector retrieval of Calendar Event  
    Subject information ..... [71](#)  
applying full access permissions ..... [71](#)  
architecture ..... [141](#)  
assignment name ..... [51](#)  
Aura watcher ..... [136](#)  
authentication ..... [104](#)  
authorization ACLs ..... [127](#)  
authorized ..... [124](#)  
authorized outgoing from addresses ..... [123](#)  
authorized outgoing to addresses ..... [123](#)  
autodiscovery service ..... [68](#)  
Avaya Aura presentity ..... [140](#)

## B

backup ..... [227](#)  
backup.sh ..... [229](#)

basic configuration view ..... [17](#)  
binding  
    director configuration ..... [112](#)  
binding director ..... [111](#)  
blacklisting ..... [119](#), [120](#)  
    hosts  
        IP address ..... [119](#)  
bounce request ..... [309](#)  
bulk export ..... [39](#)  
bulk export users through CLI ..... [42](#)  
bulk import ..... [39](#)  
bulk import and export ..... [39](#)  
bulk import and export using Excel ..... [39](#)  
bulk import of users ..... [40](#)

## C

CA ..... [199](#), [210](#)  
CA certificate ..... [186](#)  
cache table ..... [125](#)  
certificate ..... [53](#), [184](#), [199](#), [210](#)  
Certificate Authority ..... [185](#)  
change domain search list ..... [251](#)  
change hostname in presence domain ..... [254](#)  
change IP address ..... [252](#)  
change IP address and FQDN ..... [261](#)  
change IP address for AES on Presence Services ..... [263](#)  
change PS hostname ..... [254](#)  
changeSMGR.sh ..... [265](#)  
changing AES IP address on Presence Services ..... [263](#)  
changing alternative WebLM FQDN ..... [263](#)  
changing default logging level ..... [203](#)  
Changing default logging level for exchange collector ..... [72](#)  
changing DNS ..... [250](#)  
changing DNS search domain ..... [259](#)  
changing DNS servers ..... [259](#)  
changing enrollment password on Presence Services ..... [262](#)  
changing FQDN of Presence Services ..... [260](#)  
changing Gateway IP Address for Presence Services ..... [262](#)  
changing hostname ..... [246](#)  
changing IP address ..... [260](#)  
changing IP address after installation ..... [235](#)  
changing IP address of Presence Services ..... [260](#)  
changing Network Mask for Presence Services ..... [261](#)  
changing network parameters ..... [259](#)  
changing session manager FQDN ..... [264](#)  
changing session manager IP address ..... [264](#)  
changing System Manager FQDN on Presence Services ..... [263](#)  
changing timezone for Presence Services ..... [262](#)  
checking ..... [205](#)  
checking components ..... [253](#), [255](#)  
checking SIP trace ..... [205](#)

Checking the outcome of the changed network parameters .....	<a href="#">259</a>	connected hosts lists .....	<a href="#">125</a>
checking your Presence Services license status .....	<a href="#">249</a>	connection attempts .....	<a href="#">124</a>
Checklist		connection manager .....	<a href="#">102</a> , <a href="#">106</a> , <a href="#">110</a> , <a href="#">144</a>
integrating Domino Calendar with Presence Services .	<a href="#">75</a>	Connection Manager .....	<a href="#">101</a> , <a href="#">106</a> , <a href="#">110</a> , <a href="#">112</a> , <a href="#">115</a>
check test alarms .....	<a href="#">253</a> , <a href="#">255</a>	controller	
cipher suite order .....	<a href="#">201</a>	Router area on main page .....	<a href="#">18</a>
clears test alarm .....	<a href="#">240</a>	core router .....	<a href="#">108</a>
client configuration .....	<a href="#">247</a>	count .....	<a href="#">110</a> , <a href="#">314</a>
clients .....	<a href="#">108</a>	count errors .....	<a href="#">110</a> , <a href="#">314</a>
cluster configuration .....	<a href="#">315</a>	courses .....	<a href="#">11</a>
CM .....	<a href="#">56</a> , <a href="#">59</a>	create a subscriber .....	<a href="#">287</a>
command line .....	<a href="#">100</a>	create a user .....	<a href="#">287</a>
command line mode .....	<a href="#">245</a>	creating a Domino user .....	<a href="#">79</a>
command summary .....	<a href="#">233</a>	creating new certificates in the Presence server .....	<a href="#">265</a>
Communication Manager .....	<a href="#">16</a> , <a href="#">57</a>	cross-domain communication .....	<a href="#">32</a>
Communication Manager application .....	<a href="#">220</a>	CS1000 .....	<a href="#">287</a> , <a href="#">288</a>
communication profile password .....	<a href="#">32</a>	custom logger .....	<a href="#">110</a> , <a href="#">314</a>
communications address terminology .....	<a href="#">275</a>		
component .....	<a href="#">109</a> , <a href="#">312</a>	<b>D</b>	
component IP .....	<a href="#">122</a>	database .....	<a href="#">101</a>
Component IP .....	<a href="#">99</a> , <a href="#">107</a> , <a href="#">309</a>	database driver .....	<a href="#">101</a>
component logging .....	<a href="#">108</a> , <a href="#">311</a>	database password .....	<a href="#">101</a>
Components area .....	<a href="#">19</a>	database user name .....	<a href="#">101</a>
configuration .....	<a href="#">108</a> , <a href="#">309</a> , <a href="#">311</a>	default behavior .....	<a href="#">123</a> , <a href="#">124</a>
configuration properties .....	<a href="#">23</a>	default gateway .....	<a href="#">251</a>
configuration views .....	<a href="#">17</a>	default netmask .....	<a href="#">252</a>
configure .....	<a href="#">149</a>	default netmask changes .....	<a href="#">252</a>
configure Exchange Services for the Autodiscover Service	<a href="#">72</a>	default policy domain ACL script .....	<a href="#">270</a>
configure Openfire .....	<a href="#">149</a>	default rule .....	<a href="#">309</a>
configure SIP remote host .....	<a href="#">176</a> , <a href="#">213</a>	defining rules .....	<a href="#">272</a>
configure SIP stack .....	<a href="#">176</a>	description .....	<a href="#">99</a> , <a href="#">106</a>
configuring .....	<a href="#">289</a>	details of the Presence server .....	<a href="#">22</a>
AES .....	<a href="#">51</a>	dialback secret .....	<a href="#">122</a>
basic Connection Manager .....	<a href="#">102</a>	director configuration .....	<a href="#">122</a>
Communication Manager .....	<a href="#">51</a>	DND .....	<a href="#">56</a>
dialback password .....	<a href="#">118</a>	DNS .....	<a href="#">117</a> , <a href="#">151</a> , <a href="#">194</a> , <a href="#">195</a> , <a href="#">198</a> , <a href="#">207</a> , <a href="#">208</a> , <a href="#">250</a> , <a href="#">313</a>
HTTP binding director .....	<a href="#">112</a>	SRV records .....	<a href="#">159</a>
HTTP polling connection .....	<a href="#">115</a>	DNS change .....	<a href="#">250</a>
JSM .....	<a href="#">111</a>	DNS requirements .....	<a href="#">68</a>
OpenPort .....	<a href="#">117</a> , <a href="#">118</a>	DNS servers .....	<a href="#">259</a>
Web Command Processor .....	<a href="#">113</a>	DNS SRV record .....	<a href="#">151</a>
XMPP director .....	<a href="#">111</a>	domain search list .....	<a href="#">251</a> , <a href="#">252</a>
configuring an Openfire XMPP server .....	<a href="#">149</a>	DOMINO_CALENDAR_POLLING_PERIOD .....	<a href="#">97</a>
configuring authorization ACLs .....	<a href="#">127</a>	DOMINO_CALENDAR_REQUEST_RATE .....	<a href="#">97</a>
configuring cluster XMPP federation		DOMINO_OOTO_POLLING_PERIOD .....	<a href="#">97</a>
checklist .....	<a href="#">159</a>	DOMINO_OOTO_REQUEST_RATE .....	<a href="#">97</a>
configuring DIGEST-MD5 authentication using SASL .....	<a href="#">105</a>	DOMINO_PUBLISHING_PERIOD .....	<a href="#">97</a>
configuring Domino Collector		DOMINO_SERVER_URI .....	<a href="#">97</a>
post Presence Services installation .....	<a href="#">98</a>	DOMINO_USER_PASSWORD .....	<a href="#">97</a>
silent installation .....	<a href="#">95</a>	DOMINO_USERNAME .....	<a href="#">97</a>
software-only installation .....	<a href="#">92</a>	Domino Calendar .....	<a href="#">13</a> , <a href="#">75</a>
configuring OCS .....	<a href="#">175</a>	Domino Calendar web service .....	<a href="#">75</a>
configuring presence publisher .....	<a href="#">289</a>	Domino Calendar web service database .....	<a href="#">76</a>
configuring the federation domain .....	<a href="#">163</a>	Domino collector .....	<a href="#">75</a>
configuring users .....	<a href="#">276</a>	Domino Collector	
connected hosts .....	<a href="#">125</a>	parameters .....	<a href="#">97</a>

## Index

Domino Collector configuration .....	<a href="#">92</a>	Federated user and .....	<a href="#">140</a>
After Presence Services installation .....	<a href="#">92</a>	federated watcher .....	<a href="#">140</a>
Presence Services silent installation .....	<a href="#">92</a>	federation .....	<a href="#">134</a> , <a href="#">197</a> , <a href="#">198</a> , <a href="#">210</a>
Presence Services software-only installation .....	<a href="#">92</a>	Federation	
Domino Collector Configuration		Aura domains .....	<a href="#">224</a>
field descriptions .....	<a href="#">95</a>	federation domain .....	<a href="#">200</a>
Domino enterprise deployment .....	<a href="#">75</a>	field descriptions	
Do Not Disturb .....	<a href="#">13</a>	Domino Collector Configuration .....	<a href="#">95</a>
DOS attack .....	<a href="#">125</a>	filtering .....	<a href="#">272</a>
during installation .....	<a href="#">174</a> , <a href="#">212</a>	firewall .....	<a href="#">112</a> , <a href="#">114</a> , <a href="#">194</a> , <a href="#">207</a>
<b>E</b>		forward .....	<a href="#">309</a>
edge server .....	<a href="#">184</a> , <a href="#">185</a> , <a href="#">199</a> , <a href="#">210</a>	forward request .....	<a href="#">309</a>
Edge server .....	<a href="#">194</a> , <a href="#">207</a>	FQDN .....	<a href="#">45</a> , <a href="#">58</a> , <a href="#">59</a> , <a href="#">194</a> , <a href="#">207</a>
Edge Server .....	<a href="#">196</a> , <a href="#">209</a>	fully qualified domain name .....	<a href="#">260</a>
edge trust store .....	<a href="#">186</a>	<b>G</b>	
enable OCS .....	<a href="#">174</a> , <a href="#">211</a>	gateway .....	<a href="#">251</a>
enable Presence and IM services .....	<a href="#">24</a>	gateway change .....	<a href="#">251</a>
Enable SNMP .....	<a href="#">108</a> , <a href="#">311</a>	generate test alarm .....	<a href="#">240</a>
enabling AES Collector .....	<a href="#">55</a>	getProductID.sh .....	<a href="#">241</a>
enabling logging for Exchange Collector .....	<a href="#">73</a>	global configuration .....	<a href="#">308</a>
enabling logging for OCS Gateway .....	<a href="#">203</a>	guidelines for exchange collector performance tuning .....	<a href="#">70</a>
enabling OCS .....	<a href="#">170</a> , <a href="#">301</a>	<b>H</b>	
enabling optional logging .....	<a href="#">157</a> , <a href="#">158</a>	H.323 .....	<a href="#">53</a>
Endpoint editor .....	<a href="#">51</a>	High Availability .....	<a href="#">13</a>
endpoint profile .....	<a href="#">54</a>	host .....	<a href="#">195</a> , <a href="#">257</a>
endpoint profile user .....	<a href="#">54</a>	host filters .....	<a href="#">100</a> , <a href="#">108</a> , <a href="#">123</a> , <a href="#">124</a> , <a href="#">310</a>
enrollment password .....	<a href="#">262</a>	host ID .....	<a href="#">33</a>
entity link .....	<a href="#">246</a>	host information	
Lync edge server .....	<a href="#">216</a>	Session Manager .....	<a href="#">215</a>
entity links .....	<a href="#">46</a>	hostname .....	<a href="#">44</a> , <a href="#">125</a> , <a href="#">246</a> , <a href="#">254</a>
error levels .....	<a href="#">245</a>	hostname in Session Manager .....	<a href="#">44</a>
errors .....	<a href="#">110</a> , <a href="#">314</a>	HTTP .....	<a href="#">111</a> , <a href="#">112</a> , <a href="#">115</a>
Excel		<b>I</b>	
import .....	<a href="#">39</a>	ID mapping .....	<a href="#">47</a>
import user .....	<a href="#">40</a>	ID of the component .....	<a href="#">309</a>
exchange collector .....	<a href="#">60</a> , <a href="#">61</a> , <a href="#">64</a>	IM .....	<a href="#">13</a> , <a href="#">98</a> , <a href="#">196</a> , <a href="#">209</a> , <a href="#">241</a>
exchange collector configuration for autodiscovery .....	<a href="#">68</a>	im_manager.sh .....	<a href="#">241</a>
exchange collector logging level .....	<a href="#">72</a>	IM client .....	<a href="#">101</a> , <a href="#">110</a>
exchange collector overview .....	<a href="#">60</a>	IM clients .....	<a href="#">111</a>
exchange collector XCP configuration .....	<a href="#">61</a>	IM communication address .....	<a href="#">26</a>
exchange parameters .....	<a href="#">63</a>	import	
exchange server configuration for Presence Services		user data .....	<a href="#">39</a>
integration .....	<a href="#">70</a>	import from Excel	
export		user data .....	<a href="#">39</a>
user data .....	<a href="#">39</a>	import system manager default CA certificate .....	<a href="#">186</a>
export to Excel		import user .....	<a href="#">40</a>
user data .....	<a href="#">39</a>	IM transcripts .....	<a href="#">101</a>
export users .....	<a href="#">42</a>	IM Transcripts Web Service .....	<a href="#">99</a>
export users in bulk through CLI .....	<a href="#">42</a>	IM Transcripts Web Service configuration .....	<a href="#">98</a>
external channel .....	<a href="#">111</a>	inactive client .....	<a href="#">111</a>
<b>F</b>			
federated domains .....	<a href="#">143</a>		
federated presence .....	<a href="#">136</a>		

inbound request ..... [180](#)  
inbound requests ..... [170](#), [301](#)  
inbound SIP request ..... [181](#)  
inclDomino ..... [97](#)  
incoming packets ..... [124](#)  
incoming to addresses ..... [124](#)  
install exchange ..... [64](#)  
installing exchange collector ..... [64](#)  
installing exchange collector post installation ..... [66](#)  
integrating Domino Calendar with Presence Services  
    Checklist ..... [75](#)  
integrating exchange collector with presence services ..... [60](#)  
intermediate configuration view ..... [17](#)  
IP ..... [310](#)  
ip address ..... [58](#), [59](#)  
IP address ..... [111](#), [235](#), [252](#)  
IP address and FQDN change ..... [261](#)  
IP address change ..... [253](#)  
IP addresses ..... [123](#), [124](#)  
IPS logger ..... [99](#), [107](#), [310](#)  
IPv4 ..... [100](#), [108](#), [310](#)  
IPv6 ..... [100](#), [108](#), [310](#)  
iscovery protocol ..... [124](#)

**J**

jabber ..... [18](#)  
Jabber ID ..... [124](#)  
jdbc ..... [101](#)  
JID ..... [124](#), [237](#)  
Jlog ..... [108](#), [311](#)  
JSM ..... [99](#), [107](#), [110](#), [112](#), [114](#), [115](#), [310](#)  
JSMCP ..... [110](#)  
jsmID ..... [318](#)

**K**

keepalives ..... [109](#), [312](#)  
known issues ..... [319](#)

**L**

license renewal ..... [33](#)  
license status ..... [249](#)  
licensing ..... [33](#)  
line arguments ..... [100](#)  
local presence domain  
    Presence Services server ..... [154](#), [155](#)  
log ..... [109](#), [312](#)  
logging level ..... [72](#)  
lync ..... [198](#), [210](#)  
lync edge ..... [205](#)  
Lync federation  
    Session Manager ..... [206](#)  
Lync integration ..... [13](#)  
lync server ..... [205](#)

**M**

maximum memory ..... [309](#)  
maximum requests ..... [111](#)  
maximum size ..... [109](#)  
maximum size of threadpool ..... [109](#)  
max memory percentage ..... [309](#)  
MD5 checksum ..... [104](#)  
Microsoft Office Communications 2007 ..... [196](#), [209](#)  
Microsoft-RTC ..... [16](#)  
mod\_authz ..... [47](#), [48](#)  
mod\_idmap ..... [47](#), [48](#)  
mod\_pep ..... [48](#)  
mod\_simple ..... [47](#), [48](#)  
mod\_winfo ..... [48](#)  
modifying a reverse pointer ..... [258](#)  
modifying CA certificate to edge server root certificate ..... [256](#)  
modifying OCS Edge IM service provider ..... [257](#)  
modifying presence access levels ..... [273](#)  
modifying the SRV record for a new hostname ..... [258](#)  
monit ..... [247](#), [249](#)  
MS Edge Server ..... [198](#)  
MS exchange collector parameters ..... [63](#)  
multi-domain support  
    Lync federation ..... [169](#), [223](#)  
multiple domain ..... [13](#)  
multiuser chat ..... [129](#)  
    multiuser ..... [129](#)

**N**

netmask ..... [252](#)  
netstat ..... [315](#)  
network login ..... [276](#)  
network mask ..... [261](#)  
network mask change ..... [261](#)  
network parameters ..... [250](#)  
new command processor ..... [107](#)  
New Host (A)  
    Session Manager ..... [208](#)  
new hostname ..... [258](#)  
new SIP transport ..... [183](#)  
nms ..... [238](#)  
non-System Platform ..... [261](#)  
non-System Platform deployments ..... [259](#), [260](#)  
number of clients ..... [108](#)

**O**

OCS ..... [15](#), [49](#), [58](#), [59](#), [165](#), [167](#), [197](#)  
OCS configuration ..... [256](#)  
OCS Connection Manager ..... [58](#)  
OCS Gateway ..... [170](#), [174](#), [196](#), [211](#), [212](#), [301](#)  
OCS Gateway routing rule ..... [181](#)  
OCS SIP ..... [57](#), [201](#)  
OCS worksheet ..... [173](#), [300](#)  
Office Communications Server ..... [184](#)

## Index

One-X Client Enablement Services .....	<a href="#">285</a>	Presence Services admin status check .....	<a href="#">35</a>
one-x Communicator .....	<a href="#">49</a>	Presence Services FQDN change .....	<a href="#">260</a>
OOD Refer .....	<a href="#">43</a>	presence services ip address .....	<a href="#">58, 59</a>
OpenPort .....	<a href="#">118, 147, 164</a>	presence services IP address .....	<a href="#">252</a>
open port .....	<a href="#">125</a>	Presence Services IP address change .....	<a href="#">260</a>
other applications .....	<a href="#">16</a>	Presence Services license renewal .....	<a href="#">33</a>
other Avaya applications .....	<a href="#">16</a>	presentities .....	<a href="#">128</a>
outbound .....	<a href="#">310</a>	presentity .....	<a href="#">14, 127</a>
outbound connection .....	<a href="#">124</a>	Presentity .....	<a href="#">135</a>
outbound request .....	<a href="#">180</a>	presstatus .....	<a href="#">35, 36</a>
outbound requests .....	<a href="#">170, 301</a>	presuseracls .....	<a href="#">267</a>
outbound SIP request .....	<a href="#">180, 181</a>	primary DNS .....	<a href="#">251</a>
outgoing .....	<a href="#">123</a>	product ID .....	<a href="#">241</a>
outgoing connection attempt rules .....	<a href="#">122</a>	protocol .....	<a href="#">125</a>
overview .....	<a href="#">14, 141</a>	providing access to a Domino user .....	<a href="#">87</a>
overview MS exchange .....	<a href="#">60</a>	proxy .....	<a href="#">310</a>
<b>P</b>		proxy port .....	<a href="#">310</a>
packets .....	<a href="#">100, 108, 109, 311, 312</a>	proxy transport .....	<a href="#">310</a>
parameters .....		PS hostname .....	<a href="#">254</a>
Domino Collector .....	<a href="#">97</a>	PS logs .....	<a href="#">235</a>
parameters for MS exchange collector .....	<a href="#">61</a>	PTR .....	<a href="#">195</a>
Password .....	<a href="#">99, 107, 310</a>	<b>Q</b>	
PC3 presentity .....	<a href="#">140</a>	query .....	
PEM .....	<a href="#">199, 210</a>	inbound list .....	<a href="#">126</a>
performance tuning .....	<a href="#">70</a>	outbound list .....	<a href="#">126</a>
pidf .....	<a href="#">313</a>	quick reference .....	<a href="#">227</a>
PLDS .....	<a href="#">33</a>	<b>R</b>	
polling .....	<a href="#">115</a>	R2R .....	<a href="#">315</a>
connection .....	<a href="#">114</a>	sample configuration .....	<a href="#">316</a>
port .....	<a href="#">110, 122</a>	realm .....	<a href="#">308, 315</a>
Port .....	<a href="#">99, 107, 111, 310</a>	realm of the global configuration .....	<a href="#">308</a>
prescert .....	<a href="#">233</a>	reconfiguring OCS .....	<a href="#">256</a>
prescert tool .....	<a href="#">227, 232</a>	reconfiguring the LPS client .....	<a href="#">255</a>
presence access levels .....	<a href="#">273</a>	reconfiguring the SIP Tester client .....	<a href="#">255</a>
System Manager .....	<a href="#">273</a>	reference configuration .....	<a href="#">57</a>
Presence access levels .....	<a href="#">271, 273, 274</a>	related documentation .....	<a href="#">10</a>
Presence ACL .....		remote access .....	<a href="#">198, 210</a>
field descriptions .....	<a href="#">274</a>	remote host .....	<a href="#">182, 214</a>
Presence and instant messaging .....	<a href="#">278</a>	removing .....	
presence commands .....	<a href="#">265</a>	Presence Service component .....	<a href="#">49</a>
Presence commands .....	<a href="#">227</a>	renewing your Presence Services license .....	<a href="#">34</a>
Presence communication address .....	<a href="#">26</a>	requests .....	<a href="#">111</a>
Presence Communication Profile Migrating tool .....	<a href="#">30</a>	resolve hostname .....	<a href="#">246</a>
presence components .....	<a href="#">49</a>	resource list .....	<a href="#">128</a>
presence domain .....	<a href="#">254</a>	restarting .....	
presence FQDN .....	<a href="#">58, 59</a>	the system .....	<a href="#">19</a>
presence model .....	<a href="#">13</a>	restore .....	<a href="#">227, 230</a>
presence profile .....		restore.sh .....	<a href="#">229</a>
bulk export and import .....	<a href="#">29</a>	reverse pointer .....	<a href="#">195, 258</a>
Presence Profile .....	<a href="#">27</a>	Session Manager .....	<a href="#">208</a>
presence publisher .....	<a href="#">288, 289</a>	rich Presence .....	<a href="#">225</a>
Presence server .....	<a href="#">22</a>	root user .....	<a href="#">110</a>
presence server ip address .....	<a href="#">58, 59</a>	Router .....	<a href="#">99, 107, 309</a>
presence services .....	<a href="#">23</a>		
Presence Services .....	<a href="#">21</a>		

router outbound connection information parameters ..... [125](#)  
 Router-to-Router ..... [161](#), [315](#)  
 routing policies ..... [219](#)  
 routing regular expressions ..... [218](#)  
 runlevel ..... [100](#), [108](#), [311](#)

## S

S2S ..... [116–118](#), [122](#), [125](#), [163](#)  
 S2S command processor ..... [121–125](#)  
 S2S command processor address ..... [124](#)  
 S2S Connection Manager ..... [117](#)  
 S2SCP ..... [117](#), [125](#), [126](#)  
 sasl authentication ..... [104](#)  
 SCEP ..... [232](#), [233](#)  
 SDNS ..... [17](#)  
 search domain ..... [259](#)  
 seconds ..... [124](#)  
 Server-to-Server Connection Manager ..... [144](#)  
 Server-to-Server port ..... [153](#)  
 Server-to-Server Port  
   Openfire server ..... [154](#)  
 service d ..... [124](#)  
 Session Manager ..... [43](#)  
 session manager entity link ..... [246](#)  
 Session Manager Security Module IP address ..... [43](#)  
 signing the Domino Calendar web service database ..... [77](#)  
 SIP ..... [59](#), [194](#), [207](#), [309](#), [310](#), [313](#), [314](#)  
   host ..... [313](#)  
   publishes ..... [313](#)  
 SIP Bulk Subscription Server ..... [15](#)  
 SIP client ..... [47](#)  
 SIP edge ..... [59](#)  
 SIP Enablement Server ..... [16](#)  
 SIP entities ..... [216](#)  
 SIP entity ..... [45](#)  
 SIP gateways ..... [309](#)  
 SIP host ..... [309](#)  
 SIP Presence Server ..... [15](#)  
 SIP proxy ..... [308](#), [310](#), [312](#)  
 SIP Proxy ..... [58](#), [182](#), [214](#)  
 SIP proxy routing rules ..... [308](#)  
 SIP request ..... [180](#)  
 SIP routing domain ..... [25](#)  
 SIP SIMPLE ..... [13](#)  
 SIP stack ..... [309](#)  
 SIP stack configuration parameters ..... [176](#), [213](#)  
 SIP subscription ..... [313](#)  
 SIP TLS transport ..... [175](#)  
 SIP trace ..... [205](#)  
 SMTP ..... [108](#)  
 SNMP ..... [108](#), [238–240](#), [311](#)  
 SNMP Configuration ..... [108](#), [311](#)  
 sockets ..... [108](#)  
 soliciting confirmation ..... [272](#)  
 solution template properties ..... [291](#)  
 SPchangeParam.log ..... [259](#)

spiritAgent ..... [238](#), [239](#)  
 SRV ..... [194](#), [207](#)  
 SSL ..... [115](#)  
 staging directory ..... [229](#)  
 stanza addressing ..... [129](#)  
 stanza optimiser ..... [129](#)  
 stanza optimizer  
   advanced configuration view ..... [129](#)  
 start command ..... [100](#)  
 starting the server ..... [200](#)  
 status check ..... [35](#)  
 status description ..... [38](#)  
 status of presence service server on system manager ..... [23](#)  
 stderr ..... [100](#), [109](#), [311](#)  
 stopping the server ..... [200](#)  
 subscripts ..... [229](#)  
 support ..... [12](#)  
 swversion.sh tool ..... [227](#)  
 System Default ..... [273](#)  
 System Manager ..... [21](#), [51](#)  
 System Manager hostname ..... [246](#)

## T

TCP ..... [309](#), [312](#)  
 TestAlarm ..... [240](#)  
 test alarms ..... [253](#), [255](#)  
 testing DNS records from Microsoft Edge Server ..... [258](#)  
 The OCS Gateway ..... [15](#)  
 threadpool ..... [109](#)  
 time (minutes) endpoint is Away until being declared Out Of Office ..... [57](#)  
 time (minutes) endpoint is on-hook until being declared Away ..... [57](#)  
 timeout ..... [111](#)  
 timeout for response ..... [111](#)  
 timezone ..... [262](#)  
 TLS ..... [308](#), [309](#), [313](#)  
 TLS certificate  
   Session Manager ..... [214](#)  
   verify ..... [215](#)  
 tool ..... [265](#)  
 traffic ..... [112](#)  
 training ..... [11](#)  
 trust configuration ..... [211](#)

## U

UA ..... [308](#)  
 UDP ..... [309](#)  
 unresolvable hostname ..... [125](#)  
 update ..... [227](#)  
 update certificates ..... [265](#)  
 update entity link ..... [246](#)  
 update log level ..... [237](#)  
 update log level tool ..... [236](#)  
 updating client configuration ..... [247](#)

## Index

URL .....	<a href="#">101</a>	checklist .....	<a href="#">143</a>
User ACL .....	<a href="#">273</a>	XMPP federation architecture .....	<a href="#">141</a>
User Agent .....	<a href="#">49</a>	XMPP server .....	<a href="#">49</a>
user configuration .....	<a href="#">135</a> , <a href="#">222</a>	XMPP Server .....	<a href="#">16</a>
System Manager .....	<a href="#">24</a>		
user default .....	<a href="#">269</a>		
User Default .....	<a href="#">273</a>		
user default acl policy .....	<a href="#">269</a>		
user-default-policy-domain.sh .....	<a href="#">139</a>		
user handles .....	<a href="#">53</a> , <a href="#">57</a> , <a href="#">201</a>		
user provisioning .....	<a href="#">318</a>		
using			
command line mode .....	<a href="#">36</a>		
using the Interactive Mode .....	<a href="#">35</a>		
<b>V</b>			
verify default gateway .....	<a href="#">251</a>		
verify domain search list .....	<a href="#">252</a>		
verify hostname .....	<a href="#">44</a>		
verifying DNS setup .....	<a href="#">156</a>		
verifying exchange server connection status .....	<a href="#">69</a>		
verifying primary DNS .....	<a href="#">251</a>		
verify netmask changes .....	<a href="#">252</a>		
verify Presence Services IP .....	<a href="#">253</a>		
videos .....	<a href="#">11</a>		
viewing monit using a CLI .....	<a href="#">249</a>		
VoIP .....	<a href="#">165</a> , <a href="#">167</a>		
<b>W</b>			
Watcher .....	<a href="#">135</a>		
watchers.sh .....	<a href="#">237</a>		
Web Command Processor .....	<a href="#">112</a>		
WebLM .....	<a href="#">33</a>		
web service .....	<a href="#">99</a> , <a href="#">100</a>		
whitelisting .....	<a href="#">119</a> , <a href="#">120</a>		
hosts			
IP address .....	<a href="#">119</a>		
windows 2008 server .....	<a href="#">201</a>		
<b>X</b>			
XCP .....	<a href="#">17</a> , <a href="#">98</a> , <a href="#">110</a> , <a href="#">112</a> , <a href="#">116–118</a> , <a href="#">313</a>		
XCP configuration .....	<a href="#">61</a>		
XCP Controller .....	<a href="#">18</a> , <a href="#">49</a> , <a href="#">285</a>		
XCP server .....	<a href="#">101</a> , <a href="#">110</a> , <a href="#">114</a>		
XCP system .....	<a href="#">118</a>		
XEP .....	<a href="#">112</a> , <a href="#">125</a>		
XEP-0030 .....	<a href="#">124</a>		
XEP-0033 .....	<a href="#">129</a>		
XML			
import user .....	<a href="#">40</a>		
XMPP .....	<a href="#">13</a> , <a href="#">15</a> , <a href="#">110</a> , <a href="#">112</a> , <a href="#">114</a> , <a href="#">117</a> , <a href="#">125</a> , <a href="#">237</a>		
XMPP clients .....	<a href="#">32</a>		
XMPP federation .....	<a href="#">141</a>		