Avaya Aura® Presence Services Snap-in Reference

Release 7.0.1
Issue 3
December 2016

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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 one 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 each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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 is the software contained within the list of Heritage Nortel Products located at https://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 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

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products 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 products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

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, its licensors, its suppliers, 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 is a registered 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.

Contents

Chapter 1: Introduction

Purpose

This document describes tested Presence Services characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements. This document also contains Presence Services installation, configuration, initial administration, and basic maintenance checklist and procedures.

This document is intended for people who need to install, configure, and administer the Presence Services snap-in. This document contains specific information about this snap-in. For an overview of the Avaya Breeze™, see the *Avaya Breeze™ Overview and Specification*. For general information about Avaya Breeze™ snap-in deployment, see *Quick start to Deploying Avaya Breeze™ Snap-ins*.

Change history

Issue	Date	Summary of changes
3.0	December 2016	Added information about Domino Collector integration.
2.0	May 2016	Added information about the following features: • XMPP federation • Federation between two Presence Services clusters on the same System Manager • Instant Message Broadcast Tool • Lync Interdomain federation • Lync Intradomain federation • Interoperability with Avaya Multimedia Messaging • Roster size enforcement • Inter-Domain Presence and IM • Creating or importing a Presence Services session • Geographic Redundancy • Migrating from Presence Services 6.2.x to Presence Services 7.0.x

Table continues…

Issue	Date	Summary of changes
		• Federation with Cisco Jabber • Presence Services Software Inventory web service • Certificate Management • User and device administration Added information about the following alarms: • Lost Connectivity to remote Geographic Redundancy cluster • Clear Lost Connectivity to remote Geographic Redundancy cluster • Presence Services Geographic Redundancy misconfigured • Clear Presence Services Geographic Redundancy misconfigured • Cluster Health Check failed • Clear Cluster Health Check failed Added information about the following CLI commands: • smgrPresenceUserAccessControl • presHealthCheck • presStatus • presClients • presCollectMetrics • presGraphMetrics

Chapter 2: Presence Services snap-in description

Presence Services overview

Avaya Aura® Presence Services provides the presence of a user through the presence states. For example, busy, away, or Do Not Disturb. The presence is an indication of the availability of a user and the readiness to communicate across services, such as telephony, instant messaging (IM), and video.

The presentity is the visibility of a user on a shared communication network. The users who are a part of the presentity group have access to the presence status of another user. A watcher is a user who monitors the presentity of another user. The watcher must subscribe to Presence Services to receive presence updates for a presentity.

Presence Services supports collecting presence information from diverse sources. This information is aggregated for a user and then made available to the presence-aware applications. These applications use Local Presence Service (LPS) to subscribe to Presence Services. When an application subscribes to Presence Services, the application receives presence change notifications that contain the aggregated presence for a user and the communication resources available to the user. Using this information, the application can provide a visual indication about the presence of the user.

Presence Services supports:

- The presence aggregation service that collects the presence information from Avaya and third-party sources and distributes the presence information to the Avaya tools.
- The aggregation of presence information from a variety of Avaya endpoints, including one-X® clients.
- The Extensible Messaging and Presence Protocol (XMPP).

Presence Services is compatible with the client software from Microsoft®, IBM® Domino®, and open source. Presence Services uses the following collectors to enable the users to use the core Presence Services capabilities with other presence sources:

- AES Collector: To collect telephony presence information from nonpresence-capable devices such as H323, DCP, and SIP endpoints administered as OPTIM extensions.
- Exchange Collector: To collect the calendar and out-of-office information from Exchange mailboxes.
- Domino Collector: To collect the calendar and out-of-office information from Domino mailboxes.

Local Presence Service

Presence-aware applications can use Local Presence Service (LPS) to subscribe to Presence Services. LPS runs co-resident on the application server. 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.

PS connector

PS connector is an Avaya Breeze™ snap-in service used by other Avaya Breeze™ applications. When PS connector is enabled, other application running on the same Avaya Breeze™ cluster can get or set the presence status of a provisioned user using PS connector. PS connector service runs on separate Avaya Breeze™ cluster from where Presence Services runs.

Presence Services architecture

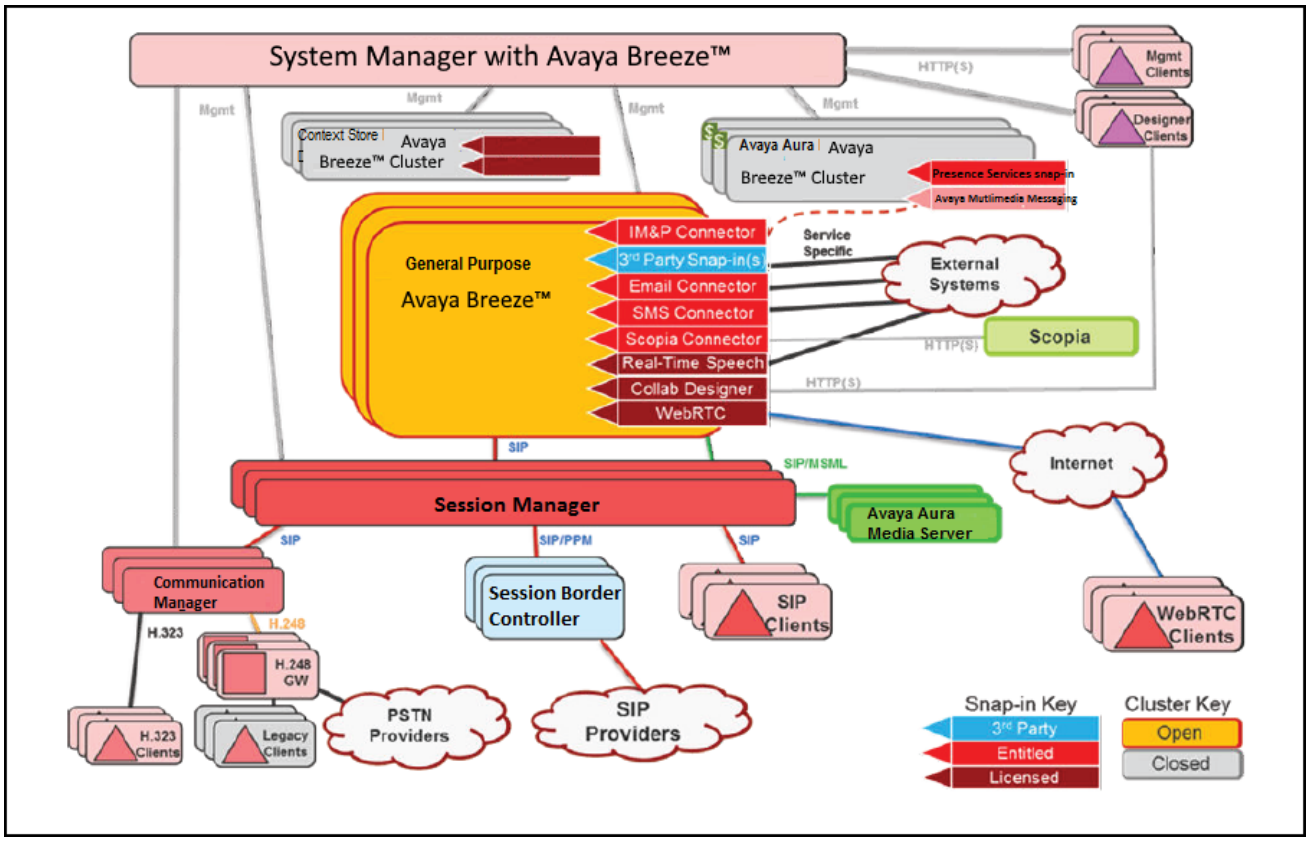


Figure 1: Avaya Breeze™ architecture

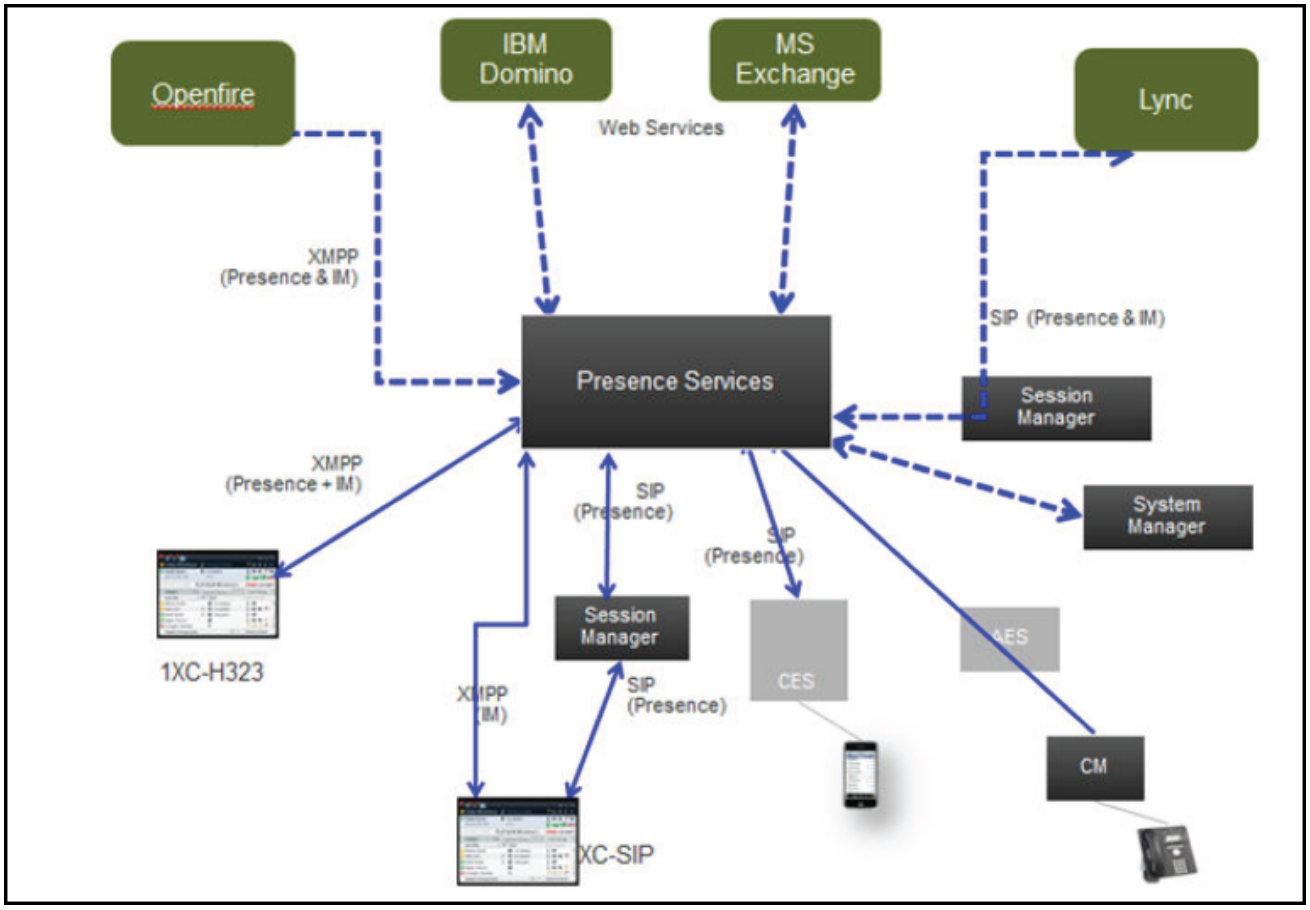


Figure 2: Presence Services snap-in architecture

What's new in Presence Services

This chapter provides an overview of the new and enhanced features of Presence Services Release 7.0.1.

Support for XMPP federation with Openfire

Presence Services Release 7.0.1 supports federation of a Presence Services Release 7.0.1 system with Openfire.

Support for XMPP federation between Presence Services 7.0.1 and Presence Services 6.2.6

Presence Services Release 7.0.1 supports federation of a Presence Services Release 7.0.1 system with a Presence Services Release 6.2.6 system.

Presence domain sharing

Presence Services Release 7.0.1 supports deployment of Presence Services solution that shares the same addressing domain.

Support for Geographic Redundancy

Presence Services Release 7.0.1 supports Geographic Redundancy. This feature enables Presence Services solution to be deployed with both High Availability and clustered solutions in different geographic regions.

Support for Cisco Jabber Federation

Presence Services Release 7.0.1 supports federation with Cisco Jabber enabling the exchange of presence and IM information between users. This feature will only be compatible with Aura endpoints that support true federation.

Upgrade scripts for XCP controller data

Presence Services Release 7.0.1 enables the administrator to maintain the XCP controller data when migrating/upgrading from Presence Services Release 6.2.x to Presence Services Release 7.0.x without the need to manually configure the configuration settings in Presence Services Release 7.0.x.

Support for Note Aggregation

Presence Services Release 7.0.1 provides a mechanism to aggregate the availability description that is sent to endpoints to be delivered along with presence of the user.

Support for forwarding IM traffic to Avaya Multimedia Messaging

Presence Services Release 7.0.1 provides an option to forward all IM traffic to Avaya Multimedia Messaging if an Avaya Multimedia Messaging is deployed as part of the solution.

Support for Common Server

Presence Services Release 7.0.1 supports Common Server Release 3.0.

Support for Interoperability among clients

Presence Services Release 7.0.1 will be compatible with existing Avaya endpoints that are used with Presence Services Release 6.2.x and 7.0. Presence/IM capable devices:

- 96X0 SIP (XMPP IM not supported)
- 96X1 SIP
- OneXC SIP
- OneXC H323
- Avaya Communicator
- Summit (XMPP IM not supported)
- One-X Agent

Non Presence/IM capable devices:

- 96X0 H323
- 96X1 H323

Supported migration paths

The supported migration paths for Presence Services Release 7.0.1 are:

Release	Requirement
5.2.x	Upgrade to 6.x and then upgrade to 7.0.1.
6.0.x	Direct upgrade to 7.0.1.
6.1.x	Direct upgrade to 7.0.1.
6.2.x	Direct upgrade to 7.0.1.
7.0.0.0.x	Direct upgrade to 7.0.1.
7.0.0.1.x	Direct upgrade to 7.0.1.

Key features of Presence Services

- Supports a presence model that uses rules in an algorithm to arrive at an aggregated presence for a user.
- Supports protocols, such 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 7.0, Avaya one-X® Communicator Release 6.2, Avaya Communicator for Windows, and Avaya Communicator for iPad support this Presence Services feature.

Feature comparison

The following table summarizes the operational and functional changes in the Presence Services releases.

Feature	6.0	6.1	6.2	7.0.x
Access Control Lists	N	N	Y	Y
Exchange Collector	N	N	Y	Y
XMPP federation	N	N	Y	Y
Simple Authentication and Security Layer	N	N	Y	Y
Inter-Tenant Communication Control	N	N	Y	Y
Avaya common servers	N	N	Y	Y
Virtualized Environment	N	N	Y	Y

Chapter 3: Interoperability

Avaya Product requirements

Avaya product	Minimum supported version
Avaya Aura® System Manager	7.0
Avaya Breeze™	3.1
Avaya Aura® Session Manager	7.0
Avaya Aura® Communication Manager	6.3.6
Avaya Aura® Application Enablement Services	7.0
Avaya one-X® Client Enablement Services	6.2.4

Chapter 4: Licensing

Licensing

Presence Services snap-in does not require a license to work.

Chapter 5: Deployment

Planning

Cluster considerations

Presence Services can be deployed as a single-server cluster or a multi-server cluster:

- For High Availability, a multi-server cluster must be deployed. For information about administering High Availability, see “Administering Presence Services System service attributes”.
- The number of required servers depends on the number of presence-enabled users that will be hosted by this cluster. For more information, see *Capacity and scalability specification*.
- The service attribute **Number of users** is used to optimize performance of the cluster. Changing this value requires a restart of the entire cluster, resulting in a service outage. When the cluster is initially deployed, it is recommended that this service attribute be administered with the planned number of users that will eventually be hosted by this cluster.

  For example, if the cluster is initially deployed with 20,000 users, but is planned to grow to 40,000 users, then this service attribute should be administered with 40,000 at the time of initial deployment.

  For information about administering the number of users, see “Configuring System service attributes”.
- Avaya Breeze™ Release 3.1 supports five profiles, each with different allocations of CPU, memory and disk space. During Avaya Breeze™ deployment, an Avaya Breeze™ 3.1 profile must be selected. For more information, see *Deployment of Avaya Breeze™*. If Presence Services is the only snap-in deployed on the cluster, select the Avaya Breeze™ 3.1 profile based on the number of users that will be hosted by this cluster. After deploying the Avaya Breeze™ profile, you must update the disk space allocated to each VM through vCenter or vSphere. There is no need to perform this step if you are using SDM to deploy the OVA.

  The following table summarizes the system resources required for each of the 4 different profiles.

Number of users	Breeze Profile	Number of vCPUs	CPU Reservation (Mhz)	Memory (GB)	Disk Space (GB)
1 to 1000	2	4	9600	8	80
1001 to 2400	3	6	14400	10	80
2401 to 5000	4	8	19200	16	150
5001 to 16000	5	12	28800	27	300

You must check the VM resource allocation through vCenter or VSphere after the Avaya Breeze™ OVA has been deployed. There is no need to perform this step if you are using SDM to deploy the OVA.

Key customer configuration information

Record the information in the following worksheet. These values need to be entered when deploying Presence Services.

Table 1: Key customer configuration information

No.	Requirement	Value
1	Location of Avaya Breeze™ OVA	
2	Avaya Breeze™ Virtual Machine name	
3	Avaya Breeze™ Profile type	
4	Avaya Breeze™ Virtual Machine hostname	
5	Avaya Breeze™ Management Module IP address	
6	Network mask for Avaya Breeze™ management network interface	
7	Default gateway IP address	
8	DNS domain	
9	Primary DNS server IP address	
10	Secondary DNS server IP address (optional)	
11	HTTP Proxy (optional)	
12	Primary NTP server IP address	
13	Secondary NTP server IP address (optional)	
14	Login ID for customer account	
15	Password for customer account	
16	System Manager IP address	
17	System Manager enrollment password	

Table continues…

No.	Requirement	Value
18	Avaya Breeze™ SIP Entity name	
19	Avaya Breeze™ Security Module IP address	
20	Session Manager SIP Entity name	
21	Avaya Breeze™ Cluster name	
22	Avaya Breeze™ Cluster IP address	
23	Location of the Presence Services SVAR	
24	Presence Services Cluster SIP Entity name	
25	Presence Services Cluster FQDN	
26	Name of Entity Link between Avaya Breeze™ and Session Manager	
27	Name of Entity Link between Presence Services Cluster SIP Entity and Session Manager	

Presence Services single-server deployment

Checklist for deploying a single-server Presence Services cluster

Prerequisites:

You must have the following before deploying Presence Services:

- VMware ESXi installed on a server with a host IP address assigned. For the recommended VMware ESXi version, see *Deploying Avaya Breeze*™ or use Avaya Virtualization Platform.
- Session Manager requires a Listen Port with the Listen Port as 5061, Protocol as TLS, and Default Domain as the login domain of endpoint devices. Without this, PPM will fail for SIP endpoints. For more information, see *Administering Avaya Aura® Session Manager*.

Note:

Ensure that you select the **Endpoints** check box for the Listen Port.

In the following checklist, *s* refers to the number of deployed Session Managers.

Table 2: Checklist for deploying a single-server Presence Services cluster

No.	Task	Reference	✔
1	Administer DNS A record to resolve Avaya Breeze™ hostname	—	

Table continues…

No.	Task	Reference	✔
	to Avaya Breeze™ Management IP address.		
2	Administer DNS A record to resolve System Manager hostname to IP address.	—	
3	Administer DNS A record to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address.	—	
4	Deploy Avaya Breeze™ 3.1 on host server.	Deploying Avaya Breeze™ on page 22	
5	Confirm that Avaya Breeze™ successfully replicates with System Manager.	Confirming that Avaya Breeze successfully replicates with System Manager on page 24	
6	Administer Avaya Breeze™ SIP Entity.	Administering Avaya Breeze SIP Entity on page 24	
7	Administer *s* Entity Links between Avaya Breeze™ and Session Managers.	Administering Entity Link between Avaya Breeze and Session Manager on page 25	
8	Administer Presence Services Cluster SIP Entity.	Administering Presence Services Cluster SIP Entity on page 26	
9	Administer *s* Entity Links between Presence Services Cluster SIP Entity and Session Managers.	Administering Entity Link between Presence Services Cluster SIP Entity and Session Manager on page 26	
10	Administer Avaya Breeze™ server.	Administering Avaya Breeze server on page 27	
11	Administer Avaya Breeze™ cluster and assign Avaya Breeze™ server.	Administering Avaya Breeze cluster on page 27	
12	Administer Presence Services on Avaya Breeze™ Managed Element.	Administering Presence Services on Avaya Breeze Managed Element on page 28	
13	Administer System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address.	Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze Security Module IP address on page 29	
14	Administer Avaya Breeze™ alarming.	For information, see *Deploying Avaya Breeze™*.	
15	Load Presence Services snap-in.	Loading Presence Services snap-in on page 29	
16	Install Presence Services snap-in on Avaya Breeze™ cluster.	Installing Presence Services snap-in on page 30	
17	Administer Presence Services System service attributes.	Administering Presence Services System service attributes on page 30	
18	Restart Presence Services.	Restarting Presence Services on page 164	

Table continues…

No.	Task	Reference	✔
19	Verify that Presence Services snap-in is ready to support Presence and IM.	Verifying that Presence Services snap-in is ready to support Presence and IM on page 224	

Deployment of Avaya Breeze™

You can deploy Avaya Breeze™ using one of the following ways:

- VMware vSphere Client
- Solution Deployment Manager
- VMware vCenter

The following procedure describes the deployment of Avaya Breeze™ on VMware vSphere Client, using ESXi 5.5 and Avaya Breeze™ 3.1.0.0. For information about deploying Avaya Breeze™ using Solution Deployment Manager or VMware vCenter, see *Deploying Avaya Breeze™*.

Deploying Avaya Breeze™ using VMware vSphere Client

Before you begin

- Install VMware vSphere client on the desktop.
- Verify that System Manager Enrollment Password is not expired. You can verify this setting by logging into System Manager web console, and navigating to **Services** > **Security** > **Certificates** > **Enrollment Password**.
- It is recommended that an Avaya Breeze™ license be installed on System Manager prior to deploying Avaya Breeze™. Else, the server will immediately be in License Error Mode.

For more information, see *Deploying Avaya Breeze™*.

Procedure

1. Log in to the ESXi host server using VMware vSphere Client.
2. In the Inventory list, select the ESXi host.
3. Click **File** > **Deploy OVF Template**.

   The system displays the Source window.
4. Click **Browse**, and select the Avaya Breeze™ OVA.

   See “Table 1: Key customer configuration information”, row 1.
5. Click **Next**.

   The system displays the OVF Template Details window.
6. Verify that the details displayed match the version of the Avaya Breeze™ that you are expecting to deploy.
   - If the details do not match, you may have chosen the wrong OVA. Click **Back** and select the correct OVA.
   - If the details do match, click **Next**.

The system displays the End User License Agreement page.

7. If you accept the End User License Agreement click **Accept**, and click **Next**.

   The system displays the Name and Location page.

8. Enter a name for the Avaya Breeze™ Virtual Machine (VM), and click **Next**.

   See “Table 1: Key customer configuration information”, row 2.

   The system displays the Deployment Configuration page.

9. Select the configuration profile that best fits the deployment, then click **Next**.

   See “Table 1: Key customer configuration information”, row 3.

   The system displays the Disk Format page.

10. Select the disk provisioning format you want, then click **Next**.

    Thick Provision Eager Zeroed is recommended for an Avaya Breeze™ installation that will support Presence Services.

    The system displays the Network Mapping page.

11. Refer toAvaya Breeze™ documentation for information on Network Mapping, and click **Next**.
12. On the Ready to Complete page, verify the options listed.
13. Click **Finish**.

    The OVA will take several minutes to deploy.

14. Once deployment is completed, within the VMware vSphere Client, the new VM will now appear in the Inventory List under the ESX host. Select the VM.
15. Right-click and select **Power** > **Power On**.
16. With the VM still selected, right-click and select **Open Console**.

    This pops up a console window showing the VM booting. You can use Ctrl + Alt to exit the window at any time.

17. During the boot, you will see the End User License Agreement. Scroll down through this document using the spacebar. At the bottom, enter `yes` if you agree to the terms.

    The VM continues to boot.

18. Towards the end of the boot sequence you are prompted to configure the VM. Enter `y` to proceed.
19. Enter the following details:

    - Hostname: See “Table 1: Key customer configuration information”, row 4
    - IP address: See “Table 1: Key customer configuration information”, row 5
    - Netmask: See “Table 1: Key customer configuration information”, row 6
    - Gateway IP address: See “Table 1: Key customer configuration information”, row 7
    - DNS domain: See “Table 1: Key customer configuration information”, row 8

- Primary DNS server IP address: See “Table 1: Key customer configuration information”, row 9
- (Optional) Secondary DNS server IP address: See “Table 1: Key customer configuration information”, row 10
- (Optional) When the system prompts, **Would you like to configure an HTTP proxy?**, enter `y` or `n` depending on the network configuration.

  If you enter `y`, enter the HTTP proxy FQDN or the HTTP proxy IP address. See “Table 1: Key customer configuration information”, row 11.
- Avaya Timezone Selection
- Date
- Time
- When the system prompts, **Would you like to disable NTP?**, enter `no`.
- IP/FQDN of Primary NTP Server: See “Table 1: Key customer configuration information”, row 12
- (Optional) IP/FQDN of Secondary NTP Server: See “Table 1: Key customer configuration information”, row 13
- Login ID to use for the customer account: See “Table 1: Key customer configuration information”, row 14
- Password for Customer Login: See “Table 1: Key customer configuration information”, row 15
- IP Address of the System Manager: “Table 1: Key customer configuration information”, row 16
- Enrollment Password: See “Table 1: Key customer configuration information”, row 17

Confirming that Avaya Breeze™ successfully replicates with System Manager

Procedure

1. On the System Manager web console, navigate to **Services** > **Replication**.
2. In **Replica Group** column, click **CollaborationEnvironment_3.1**.
3. In **Replica Node Host Name** column, locate your newly-deployed Avaya Breeze™.
4. After 2 – 15 minutes, verify that the status of the **Synchronization Status** field is green/ Synchronized. If not, see *Repairing replication between Avaya Breeze™ and System Manager*.

Administering Avaya Breeze™ SIP Entity

About this task

Administer Avaya Breeze™ as a SIP Entity so that you can configure Session Manager to route traffic through Avaya Breeze™.

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of your SIP Entity.

   See “Table 1: Key customer configuration information”, row 18.
4. In the **FQDN or IP Address** field, type the IP address of Avaya Breeze™ Security Module.

   See “Table 1: Key customer configuration information”, row 19.
5. In the **Type** field, select **Avaya Breeze™**.
6. From the **SIP Link Monitoring** drop-down menu, select **Link Monitoring Enabled**.
7. Click **Commit**.

   For information about other fields, see *Deploying Avaya Breeze™*.

Administering Entity Link between Avaya Breeze™ and Session Manager

About this task

Create an Entity Link to connect Session Manager to Avaya Breeze™. You must administer separate Entity Links for Avaya Breeze™ servers in order to open SIP listeners on the designated ports.

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** field, type a name for the Avaya Breeze™ SIP Entity Link.

   See “Table 1: Key customer configuration information”, row 26.
4. In the **SIP Entity 1** field, select the Session Manager instance.

   See “Table 1: Key customer configuration information”, row 20.
5. In the **SIP Entity 2** field, select the Avaya Breeze™ SIP Entity that you created in “Administering Avaya Breeze™ SIP Entity”.

   See “Table 1: Key customer configuration information”, row 18.
6. In the **Protocol** field, enter `TLS`.
7. In the **Connection policy** field, enter `trusted`.
8. The system automatically enters **5061** in both the **Port** fields. Do not change these fields.
9. Click **Commit**.

Administering Presence Services Cluster SIP Entity

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter a name for the Presence Services Cluster SIP Entity.

   See “Table 1: Key customer configuration information”, row 24.
4. In the **FQDN or IP Address** field, enter the Presence Services Cluster FQDN.

   See “Table 1: Key customer configuration information”, row 25.
5. In the **Type** field, select **Presence Services**.
6. From the **SIP Link Monitoring** menu, select **Link Monitoring Enabled**.
7. Click **Commit**.

Administering Entity Link between Presence Services Cluster SIP Entity and Session Manager

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing** > **Entity Links**.
2. In the **Name** field, enter a name for Entity Link.

   See “Table 1: Key customer configuration information”, row 27.
3. In the **SIP Entity 1** field, select the Session Manager instance.

   See “Table 1: Key customer configuration information”, row 20.
4. In the **Protocol** field, select **TLS**.
5. In the **Port** field, type `5062`.

   Note:

   Note that this port number cannot be the same as the port number administered in “Administering Entity Link between Avaya Breeze™ and Session Manager”.
6. In the **SIP Entity 2** field, select the Presence Services Cluster SIP Entity.

   See “Table 1: Key customer configuration information”, row 24.
7. In the **Port** field, type `5061`.
8. In the **Connection Policy** field, select **trusted**.
9. Click **Commit**.

Administering Avaya Breeze™ server

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Avaya Breeze™** > **Server Administration**.
2. Click **New**.
3. In the **SIP Entity** field, select the SIP entity that you created in “Administering Avaya Breeze™ SIP Entity”.

   See “Table 1: Key customer configuration information”, row 18.
4. Ensure that the value in the **UCID Network Node ID** field is unique across the solution deployment so that it does not conflict with other UCID-generating entities like Avaya Aura® Communication Manager or Avaya Aura® Experience Portal.

   For more information about UCID, see *Deploying Avaya Breeze™*.
5. In the **Management Network Interface FQDN or IP Address** field, type the IP address of the Avaya Breeze™ Management Network Interface.

   See “Table 1: Key customer configuration information”, row 5.
6. In the **Security Module Network Mask** field, type the network mask used for the SIP (Security Module) network.
7. In the **Security Module Default Gateway** field, type the default gateway used for the SIP (Security Module) network.

   See “Table 1: Key customer configuration information”, row 7.

   For information about **Call Control PHB** and **VLAN ID** fields, see *Deploying Avaya Breeze™*.
8. Click **Commit**.

   A new Managed Element instance of type Avaya Breeze™ is automatically created at **Services** > **Inventory** > **Manage Elements**.

   Note:

   The Commit fails if the Avaya Breeze™ license file on WebLM does not have the sufficient capacity to allow addition of another Avaya Breeze™ server.

Administering Avaya Breeze™ cluster

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Click **New**.
3. In the **Cluster Profile** field, select **Core Platform**.
4. In the **Cluster Name** field, enter a name for the cluster.

   See “Table 1: Key customer configuration information”, row 21.

5. In the **Cluster IP** field, assign an IP address to the cluster.

   See “Table 1: Key customer configuration information”, row 22.

6. Select the **Enable Cluster Database** check box.
7. Select the **Enable Database Auto Switchover** check box.
8. **(Optional)** Use the **Grid password** field to secure the grid data exchanged between nodes in the cluster.

   To use the secure grid:

   - Select the **Use secure grid** check box.
   - Enter a password in the **Grid password** field.

   This field also applies to Geographic Redundancy. The secure grid setting and password must be the same on both Geo-Redundant clusters.

9. Click the **Server** tab.
10. In Unassigned Servers, click **+** to the left of the Avaya Breeze™ instance created in “Administering Avaya Breeze™ server”.

    The Avaya Breeze™ instance appears in the Assigned servers list.

11. Click **Commit**.
12. Select the cluster instance and in the **Cluster instance** field, select **Accept New Service**.

Administering Presence Services on Avaya Breeze™ Managed Element

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Inventory**.
2. Click **Manage Elements**.
3. Click **New**.
4. In the **Type** field, select **Presence Services**.
5. In the **Select type of Presence Server to add:** section, select **Presence Services on Avaya Breeze**.
6. Click **Continue**.
7. In the **Presence Services SIP Entity** field, select the Presence Services Cluster SIP Entity created in “Administering Presence Services Cluster SIP Entity”.

   See “Table 1: Key customer configuration information”, row 24.

8. In the **Primary Avaya Breeze Cluster** field, select the Avaya Breeze™ cluster created in “Administering Avaya Breeze™ SIP Entity”.

   See “Table 1: Key customer configuration information”, row 21.

   The system populates the **Avaya Breeze Cluster IP Address** field.

9. Leave the **GEO Redundant Avaya Breeze Cluster** field blank when deployed in non-GR mode.

   If deployed in GR mode, see “Presence Services geographically redundant deployment”.

10. Click **Commit**.

Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address

Procedure

1. Navigate to **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. Click **New**.

   The system displays a New Local Host Name Resolution Name Entries window.

3. In the **Host Name (FQDN)** field, enter the Presence Services Cluster FQDN.

   See “Table 1: Key customer configuration information”, row 25.

4. In the **IP Address** field, enter the Avaya Breeze™ Security Module IP address.

   See “Table 1: Key customer configuration information”, row 19.

5. In the **Port** field, enter `5061`.
6. For the remaining fields, accept the default values.
7. Click **Commit**.

Loading Presence Services snap-in

Before you begin

Note the location of the Presence Services SVAR file.

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Service Management**.
3. Select the snap-in that you want to load, and click **Load**.
4. On the Load Service page, click **Browse** and browse to your snap-in file location.

   See “Table 1: Key customer configuration information”, row 23.

5. Click **Open**.
6. Click **Load**.

   The system displays an Accept End User License Agreement page.

7. If you accept the End User License Agreement, click **Accept**.

Installing Presence Services snap-in

Procedure

1. On System Manager, in **Elements**, click **Avaya Breeze™**.
2. In the left navigation pane, click **Service Management**.
3. Select the Presence Services snap-in that you loaded during “Loading Presence Services snap-in”.
4. Click **Install**.

   The system display the list of Avaya Breeze™ clusters.
5. Select the Avaya Breeze™ cluster that you created during “Administering Avaya Breeze™ Cluster”.
6. Click **Commit**.
7. Installation may take several minutes to complete. To see the status of the snap-in installation, click the **Refresh Table** icon located in the upper-left corner of the **All Services** list.

Administering Presence Services System service attributes

About this task

The following service attributes within the System group are important to optimize performance of the cluster:

- High Availability
- Number of users

High Availability can only be enabled on a multi-server deployment.

For a description of the Number of users service attribute, see “Planning”.

Note:

A Presence Services restart must be performed after changing either of these service attributes

Procedure

1. On the System Manager dashboard, navigate to **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the Service Globals or the Service Clusters tab.
3. Within the **Service** menu, select **PresenceServices**.
4. Navigate to the **System** group.
5. To enable High Availability on the cluster, within the **High Availability** row:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter `True`.
   c. Click **Commit**.

High Availability is disabled by default.

6. To set the number of users planned for this cluster, within the **Number of Users** row:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter a value between `500` and `250000` that represents the total number of users that will eventually be supported on this cluster.
   c. Click **Commit**.

   The default number of users is 1000.

   You can perform the Presence Services administration changes now or after restarting the Presence Services cluster. For information about the administration procedures, see “Administration”.

   In addition to these two service attributes, other Presence Services administration changes might be needed. Most changes do not need a Presence Services restart, but some do. If changing any service attributes that require a Presence Services restart, it is recommended that these changes also be made now. Other changes can be performed later. For information about administration procedures, see "Service Attributes".

Presence Services multi-server deployment

A multi-server deployment requires the following IP addresses, where *m* is the number of physical servers, and *n* is the number of Presence Services instances in the cluster.

- *m* VMware ESXi host IP addresses
- *n* Avaya Breeze™ Management Module IP addresses
- *n* Avaya Breeze™ Security Module IP addresses
- OneAvaya Breeze™ Cluster IP address

For example, a cluster with five physical servers, each hosting one instance of Presence Services, requires 16 IP addresses and one Presence Services Cluster FQDN.

Checklist for deploying a multi-server Presence Services cluster

Prerequisites:

You must have the following before deploying Presence Services:

- For each server in the cluster, VMware ESXi is installed on the server with a host IP address assigned. For the recommended VMware ESXi version, see *Deploying Avaya Breeze™*.
- VMware vSphere client installed to access the ESXi server. For the recommended VMware vSphere version, see the VMware documentation.

- Session Manager requires a Listen Port with the Listen Port as 5061, Protocol as TLS, and Default Domain as the login domain of endpoint devices. Without this, PPM will fail for SIP endpoints. For more information, see *Administering Avaya Aura® Session Manager*.

Note:

Ensure that you select the **Endpoints** check box for the Listen Port.

In the following checklist:

- *n* refers to the number of Presence Services instances in the cluster.
- *s* refers to the number of deployed Session Managers.

Table 3: Checklist for deploying a multi-server Presence Services cluster

No.	Task	Reference	✔
1	Administer *n* DNS A records to resolve Avaya Breeze™ hostname to Avaya Breeze™ Management IP address.	—	
2	Administer one DNS A record to resolve System Manager hostname to IP address.	—	
3	Administer *n* DNS A records to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address.	—	
4	Deploy *n* Avaya Breeze™ 3.1 instances on *m* host servers.	Deployment of Avaya Breeze on page 22	
5	Confirm that *n* Avaya Breeze™s successfully replicate with System Manager.	Confirming that Avaya Breeze successfully replicates with System Manager on page 24	
6	Administer *n* Avaya Breeze™ SIP Entities.	Administering Avaya Breeze SIP Entity on page 24	
7	Administer *n***s* Entity Links between Avaya Breeze™ and Session Manager.	Administering Entity Link between Avaya Breeze and Session Manager on page 25	
8	Administer one Presence Services Cluster SIP Entity.	Administering Presence Services Cluster SIP Entity on page 26	
9	Administer *s* Entity Links between Presence Services Cluster SIP Entity and Session Managers.	Administering Entity Link between Presence Services Cluster SIP Entity and Session Manager on page 26	
10	Administer *n* Avaya Breeze™ servers.	Administering Avaya Breeze server on page 27	

Table continues…

No.	Task	Reference	✔
11	Administer one Avaya Breeze™ cluster and assign *n* Avaya Breeze™ servers.	Administering Avaya Breeze cluster on page 27	
12	Administer one Presence Services on Avaya Breeze™ Managed Element.	Administering Presence Services on Avaya Breeze Managed Element on page 28	
13	Administer *n* System Manager LHNR entries to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address.	Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze Security Module IP address on page 29	
14	Administer Avaya Breeze™ alarming.	For information, see *Deploying Avaya Breeze™*.	
15	Load Presence Services snap-in.	Loading Presence Services snap-in on page 29	
16	Install Presence Services snap-in on Avaya Breeze™ cluster.	Installing Presence Services snap-in on page 30	
17	Administer Presence Services System service attributes.	Administering Presence Services System service attributes on page 30	
18	Restart Presence Services.	Restarting Presence Services on page 164	
19	Verify that Presence Services snap-in is ready to support Presence and IM.	Verifying that Presence Services snap-in is ready to support Presence and IM on page 224	

Presence Services geographically redundant deployment

Presence Services support Geographic Redundancy (GR), which is essentially a disaster recovery mechanism. It provides a way for enterprises to build a highly resilient Presence and IM solution by partitioning their data centers in two distant physical sites. The data is replicated between the two sites through geo-replication which provides additional redundancy in case a data center fails or there is some other event that makes the continuation of normal functions impossible.

Presence Services Geographic Redundancy solution is based on active-active deployment model. Both the data centers provide services during normal operations. The users are partitioned between the two data centers, typically in accordance with the location. During normal operations, each data center provides services to the local users. On a wide area network (WAN), geo-location can help improve network performance so that users halfway across the planet can access the same services at local-area network (LAN) speeds. When disaster occurs and one of the data center goes down, the users of that data center migrates to the other data center to receive service and continue to be operational.

Checklist for deploying a geographically redundant Presence Services clusters

A geographically redundant Presence Services solution requires deployment of two multi-server Presence Services Clusters, physically located in different data centers or sites.

Prerequisites

You must have the following before deploying Presence Services:

1. A Geographic Redundancy enabled Avaya Aura deployment must exist:
   a. System Manager must be deployed in a geographic-redundant mode. See *Administering Avaya Aura® System Manager*.
   b. Session Managers must be deployed in both data centers and should be GR-aware. See *Administering Avaya Aura® Session Manager*.
   c. Communication Manager must be deployed in both data centers and should be GR-aware. See *Administering Avaya Aura® Communication Manager*.
   d. Other components, such as Application Enablement Services should be deployed accordingly. See respective documentation.
2. Both data centers must have separate DNS servers.

Considerations

1. Geographic redundancy for Presence Services is only supported on High Available deployments.
2. Each data center should have enough capacity to service the complete set of users, that is local users and the users from the other data center to ensure continued service to all after one of the data center is not functional.

   Note:

   Number of Users attribute must be configured with combined number of users in both data center and must have same value on both clusters.
3. Configuration of Presence Cluster in both data centers should be identical. That is, the Clusters must have same set of service attributes. See “Administering Presence Services System service attributes”.
4. For all solution components to detect the GR event, ensure that the data access to the damaged data center (DC) is completely disabled.

In the following checklist:

- DC-1 refers to data center 1.
- DC-2 refers to data center 2.
- *n* refers to the number of servers in each Presence Services clusters.

Table 4: Checklist for deploying a geographically redundant Presence Services cluster

No.	Task	Reference	✔
1	Administer one multi-server Presence cluster in DC-1.	Presence Services multi-server deployment on page 31	
2	Administer one multi-server Presence cluster in DC-2.	Presence Services multi-server deployment on page 31	
3	Administer additional n DNS A records on DC-1 to resolve Presence Services Cluster FQDN of DC-2 to Avaya Breeze™ Security Module IP address of DC-1.	—	
4	Administer additional n DNS A records on DC-2 to resolve Presence Services Cluster FQDN of DC-1 to Avaya Breeze™ Security Module IP address of DC-2.	—	
5	Administer additional n System Manager LHNR entries to resolve Presence Services Cluster FQDN of DC-1 to Avaya Breeze™ Security Module IP addresses of DC-2.	Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze Security Module IP address of remote data centers on page 36	
6	Administer additional n System Manager LHNR entries to resolve Presence Services Cluster FQDN of DC-2 to Avaya Breeze™ Security Module IP addresses of DC-1.	Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze Security Module IP address of remote data centers on page 36	
7	Administer DC-2 as Geo Redundant Cluster of DC-1.	Administering Geographic Redundant Avaya Breeze Cluster to an existing Managed Element on page 37	
8	Administer DC-1 as Geo Redundant Cluster of DC-2.	Administering Geographic Redundant Avaya Breeze Cluster to an existing Managed Element on page 37	
9	Enable High Availability on both Presence Clusters.	Administering Presence Services System service attributes on page 30	
10	Restart Presence Services on both Presence Clusters.	Restarting Presence Services on page 164	
11	Verify that Presence Services snap-in is ready to support Presence and IM.	Verifying that Presence Services snap-in is ready to support Presence and IM on page 224	
12	Administering Aura users for Geographic Redundancy.	Administering Avaya Aura user for Geographic Redundancy on page 37	
13	Administering devices for Geographic Redundancy.	Administration of Avaya Aura devices for Geographic Redundancy on page 38	

Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address of remote data centers

About this task

For messages to be routed correctly and in accordance with geo-location of servers, appropriate LHNR records need to be created on System Manager. For Geographic Redundant deployment, each cluster FQDN has all the IP addresses of Avaya Breeze™ nodes in both data centers. However, the priority of the IP Address mapping to the local data center is higher than the priority of the IP address in the remote data center.

Procedure

1. Navigate to **Elements** > **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. Click **New**.

   The system displays a New Local Host Name Resolution Name Entries window.
3. In the **Host Name (FQDN)** field, enter the Presence Services Cluster FQDN of local data center.
4. In the **IP Address** field, enter the Avaya Breeze™ Security Module IP address of the server from remote data center.
5. In the **Port** field, enter `5061`.
6. In the **Priority** field, enter a higher number (lower priority) compared to the same FQDN mapping to local Avaya Breeze™ Security Module IP address.
7. For the remaining fields, accept the default values.
8. Click **Commit**.

   Note:

   For Session Managers to load balance traffic efficiently, ensure that all high priority LHNR records have same value *X* and all low priority LHNR records have same value *Y*, where *Y* > *X*.

Example

- There are two data centers (Presence Services Avaya Breeze™ clusters) in New York & Hong Kong.
- Each cluster has twoAvaya Breeze™ servers.
- Security module IP address of server in New York are `10.136.1.11` and `10.136.1.21`.
- Security module IP address of server in Hong Kong are `10.136.2.31` and `10.136.2.41`.
- Cluster FQDN of New York cluster is `nyps.avaya.com`.
- Cluster FQDN of Hong Kong cluster is `hkps.avaya.com`.

Then, create eight LHNR records as shown in the table below.

Table 5: Sample LHNR records in a GR deployment

Host Name (FQDN)	IP Address	Port	Priority	Weight	Transport
nyps.avaya.com	10.136.1.11	5061	100	100	TLS
nyps.avaya.com	10.136.1.21	5061	100	100	TLS
nyps.avaya.com	10.136.2.31	5061	200	100	TLS
nyps.avaya.com	10.136.2.41	5061	200	100	TLS
hkps.avaya.com	10.136.2.31	5061	100	100	TLS
hkps.avaya.com	10.136.2.41	5061	100	100	TLS
hkps.avaya.com	10.136.1.11	5061	200	100	TLS
hkps.avaya.com	10.136.1.21	5061	200	100	TLS

Administering Geographic Redundant Avaya Breeze™ Cluster to an existing Managed Element

Before you begin

A Managed Element of type Presence Services representing the Presence Services Cluster must exist on System Manager.

Procedure

1. On the System Manager Web console, navigate to **Home** > **Services** > **Inventory**.
2. Click **Manage Elements**.
3. Select the Presence Services Managed Element representing the local data center, and click **Edit**.
4. In the **GEO Redundant Avaya Breeze Cluster** dropdown, select the remote Avaya Breeze™ Cluster.
5. Click **Commit**.

Administering Avaya Aura user for Geographic Redundancy

About this task

Please refer to “User and device administration” section for general information on administering endpoints.

Procedure

1. Assign a Presence Profile to the user.

For more information, see “Assigning Presence Profile to a user on System Manager”.

2. For a SIP user, assign a Session Manager Profile with the following values:
   - **Primary SM**: Session Manager local to the user’s data center.
   - **Secondary SM**: Session Manager in the other data center.

Administration of Avaya Aura devices for Geographic Redundancy

See “User and device administration” for general information on administering endpoints. In a Geographic Redundant deployment, ensure that endpoint is configured with two DNS servers, where the preferred server is the local DNS and secondary server is the remote DNS.

For example, an Avaya Communicator on Windows client in New York should use the NY-DNS server as Preferred DNS Server and the HK-DNS server as Alternate DNS Server, whereas another client in Hong Kong should use HK-DNS as Preferred DNS Server and NY-DNS as Alternate DNS Server.

Presence Services uninstallation and deletion

Uninstalling a snap-in service

About this task

When you uninstall the Presence Services snap-in, Presence Services service attributes are not removed. For more information, see “Service Attributes”.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management**.
3. On the Service Management page, select the check box for the Presence Services snap-in.
4. Click **Uninstall**.
5. On the Confirm uninstall service page, perform the following steps:
   a. Select the cluster.
   b. Select the **Do you want to force the uninstall?** check box to force the uninstall.
   c. Click **Commit**.

Next steps

To verify that the snap-in service is uninstalled, perform the following steps:

1. On the Server Administration page, verify that the **Service Install Status** field shows **Uninstalling**.
2. On the Service Management page, verify that the **State** field shows **Loaded**.

   Note:

   If the snap-in is installed on any other clusters, the **State** field will still show **Installed**.
3. On the Cluster Administration page, verify that the Service Status page does not display the uninstalled service.

Deleting a snap-in service

About this task

After all versions of the Presence Services snap-in have been deleted, Presence Services service attributes are removed. For more information, see “Service Attributes”.

Before you begin

Ensure that the snap-in service is uninstalled.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management**.
3. On the Service Management page, perform the following steps:
   a. Select the Presence Services snap-in, and click **Delete**.
   b. Select the **Please Confirm** check box to confirm the deletion.
   c. Click **Delete**.

Next steps

Verify that the Service Management page does not display the deleted service.

Chapter 6: Migration and upgrades

Migrating from Presence Services 6.2.x to Presence Services 7.0.x

Before you begin

1. Upgrade System Manager to Release 7.0.1 or later. For more information, see *Upgrading Avaya Aura® System Manager to Release 7.0.1*.
2. Upgrade Session Manager to Release 7.0.1 or later. For more information, see *Upgrading Avaya Aura® Session Manager*.
3. Back up Presence Services 6.2.x data. For more information, see *Deploying Avaya Aura® Presence Services*, Release 6.2.x.
4. Download the `PresenceServices-Migration-Bundle.zip` file from PLDS.

Procedure

1. Create migration data files for each node of the 6.2.x cluster:
   a. Copy psMigration6.2.x.sh to the Presence Services Release 6.2.x server.
   b. To ensure that the script is executable, run `chmod 775 psMigration6.2.x.sh`.
   c. Run the script: `./psMigration6.2.x.sh`.
   d. Copy the migration output file to a safe location off the Presence Server.

   You will need this migration output file on the Avaya Breeze™ server in Step 6d.

   Note:

   This script has to be run on all nodes if you have a cluster. If you have a cluster make sure you rename each migration output file with a unique name.
2. If you want the option to revert to Presence Services 6.2.x configuration, take a backup of the System Manager data.

   For more information, see *Administering Avaya Aura® System Manager*.
3. Deploy Avaya Breeze™ and Presence Services snap-in.

   For more information, see “Chapter 4: Deployment”.
4. Add or assign some users to the Presence Services snap-in on Avaya Breeze™ cluster to verify the cluster is working.
5. Run the Presence Communication Profile migration utility on System Manager.

In Presence Services 6.2.x, the **System** drop down menu of the User's Presence Communication Profile in System Manager lists each node in the Cluster. In Presence Services 7.0.x, the drop down menu lists just the Cluster. The individual nodes are not listed. To change the **System** setting for all users, use the migration script included in `PresenceServices-Migration-Bundle.zip`.

For detailed instructions, refer to the help file included in the `PresenceServices-Migration-Bundle.zip`.

After executing the migration script, Presence Services 6.2.x will be interrupted.

6. Run the Presence Services 7.0 migration utility on Avaya Breeze™:
   - If the Presence Services 6.2.x system had users with more than 100 buddies, increase the Presence Services snap-in service attribute **Roster Limit Maximum Number of Contacts** to an appropriate value before running this step.

     By default, the maximum number of contacts per user is 100 for Presence Services on Avaya Breeze™.
   - If the Presence Services 6.2.x system had any users who are watched by more than 100 federated users, increase the Presence Services snap-in service attribute **Roster Limit: Maximum Number of External Watchers** to an appropriate value before running this step.

     By default, the maximum number of federated users who can watch a user is 100 for Presence Services on Avaya Breeze™.

   a. Copy the file(s) created in Step 1b to the same Avaya Breeze™ location as used in Step 6.
   b. Log in to the Avaya Breeze™ server and execute the `psMigration7` script.

      For example, `psMigration7 /tmp/psMigrationData6.2.x.tgz`.

      For a Presence Service 6.2.x cluster, the script must be run with each file created in Step 1c. You may run this script on any Presence Services 7.0.x node for each file created from your Presence Services 6.2.x cluster.
   c. Select the appropriate option when prompted to import external XMPP watchers and manual presence states like Out Of Office.

      If you do not import manual presence states, all user manual states will be lost. External XMPP watchers are federated XMPP users who are watching Avaya Aura presence users. If you do not import these XMPP watchers, the federated watcher must manually add the contacts again to receive the contact's presence updates.
7. Configure Presence Services attributes that are not automatically migrated.
8. Review the output summary from Step 6d, some service attributes may require manual updates.
9. Stop the Presence Service cluster.

   Wait for the operation to complete before proceeding to the next step.
10. Start the Presence Service cluster.

Upgrading from Presence Services 7.x to a newer version

Before you begin

Ensure that you have installed the correct version of Avaya Breeze™ servers. For more information about the supported versions, refer to Release Notes.

Procedure

1. Download the newer version from PLDS.
2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
3. Select the cluster you want to update.
4. Click **Cluster State** > **Deny New Service**.
5. Click **Service Management**.
6. Click **Load**, and browse to the new Presence Services-7.x.x.x.x.svar file.
7. Click **Load**.
8. Select the existing 7.x Presence Services service.
9. Click **Uninstall**.
10. Select the cluster that you want to update, select the check box to force the uninstall.
11. Click **Commit**.
12. Select the new loaded Presence Services service.
13. Click Install.
14. Select the cluster that you want to update.
15. Click **Commit**.
16. Select the Presence Services service that you uninstalled.
17. Click Delete.
18. Navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
19. Select the cluster you updated.
20. Click **Cluster State** > **Accept New Service**.

Checklist for upgrading a Geographic Redundant deployment

If you are upgrading Presence Services deployed in Geographic Redundant mode, choose to do either of the following:

- Upgrade both data centers at once.

  This upgrade option is service impacting and Presence Services are not available during the duration of the upgrade. Use the instructions provided in release notes to upgrade both data centers at the same time.

- Upgrade one data center at a time

  This upgrade option provides ability to do in-service upgrades, that is the Presence Services is available to the users of both the data centers while one of the data center is upgrading.

  Warning:

  Upgrading a data center may impact Avaya Aura® services other than Presence Services. Upgrades should be scheduled during a maintenance window to avoid any service disruptions.

In the following checklist, the two data centers are referred as DC-1 & DC-2

Table 6: Checklist for performing in-service upgrade in a geographic redundant deployment

No.	Task	Reference	✔
1	Disable access to DC-1.	Disabling access to a data center on page 43	
2	Perform DC-1 upgrade	Upgrading from Presence Services 7.x to a newer version on page 42	
3	Enable access to DC-1.	Enabling access to a data center on page 46	
4	Disable access to DC-2	Disabling access to a data center on page 43	
5	Perform DC-2 upgrade	Upgrading from Presence Services 7.x to a newer version on page 42	
6	Enable access to DC-2	Enabling access to a data center on page 46	

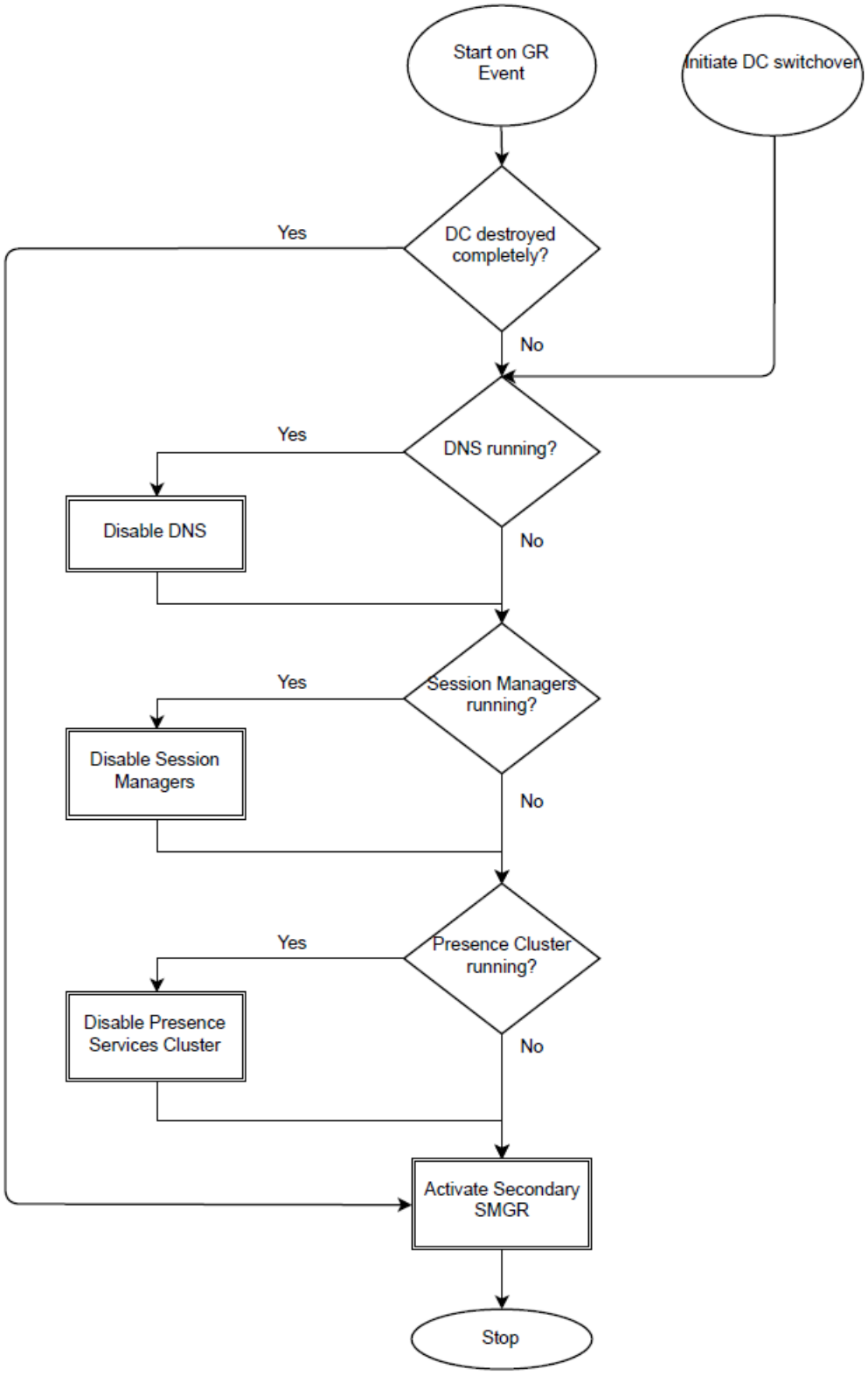
Disabling access to a data center

About this task

The administrator must disable access to a data center undergoing an upgrade / failure / switchover. This ensures that the users serviced from this data center migrate to the other data center

successfully. It is recommended that the whole data center is disabled by disconnecting it from the network or similar mechanisms. If it’s not possible to do so, follow the procedure provided.

Procedure


Start on GR Event
Initiate DC switchover
DC destroyed completely?
Yes
No
DNS running?
Yes
Disable DNS
No
Session Managers running?
Yes
Disable Session Managers
No
Presence Cluster running?
Yes
Disable Presence Services Cluster
No
Activate Secondary SMGR
Stop

Disabling DNS

The actual procedure to disable DNS server depends on the type of DNS deployed in the network and the host operating system. The administrators need to ensure that the target DNS is no longer providing services and the clients configured with this DNS server start using their secondary DNS, that is the DNS of the other data center.

Disabling Session Manager

Procedure

1. On the System Manager web console, navigate to **Elements** > **Session Manager** > **Dashboard**.
2. Select all Session Manager located in the target data center set the **Service State** to **Deny New Service**.

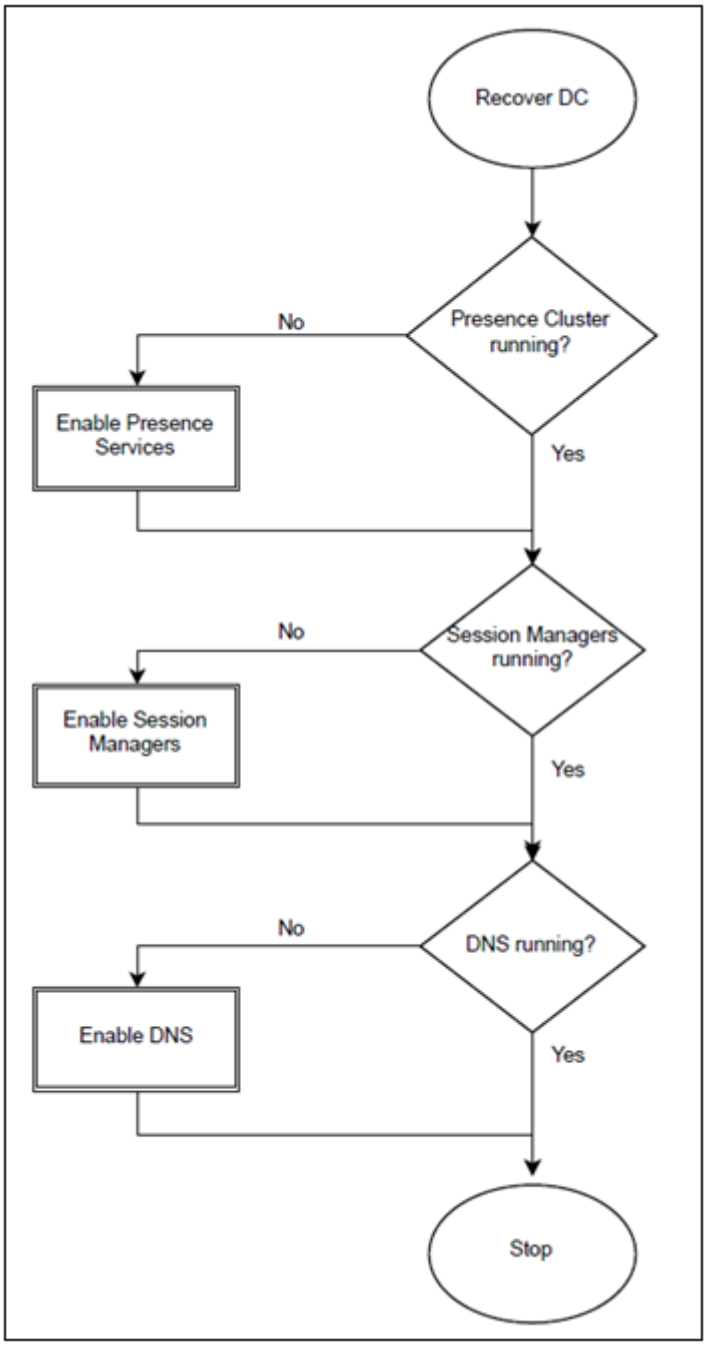
Disabling Avaya Breeze™ cluster running Presence Services

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the Presence Services cluster, and change the **Cluster State** to **Deny New Service**.
3. Uninstall Presence Services. For more information, see *Uninstalling a snap-in service*.

Enabling access to a data center

Procedure


Recover DC
Presence Cluster running?
No
Enable Presence Services
Yes
Session Managers running?
No
Enable Session Managers
Yes
DNS running?
No
Enable DNS
Yes
Stop

Enabling Avaya Breeze™ cluster running Presence Services

Before you begin

Ensure that the Avaya Breeze™ servers running the Presence Services are recovered / powered up.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the Presence Services cluster, and change the **Cluster State** to **Accept New Service**.

Enabling Session Manager

Before you begin

Ensure that the servers running Session Manager are recovered / powered up.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Session Manager** > **Dashboard**.
2. Select all Session Manager located in the data center undergoing upgrade and set the **Service State** to **Accept New Service**.

Enabling DNS

Before you begin

Ensure that the servers running DNS are recovered / powered up.

About this task

The actual procedure to enable DNS server depends on the type of DNS deployed on in the network and the host operating system.

Procedure

Ensure that after the data center is upgraded, the clients should be able to use their primary DNS in local data center.

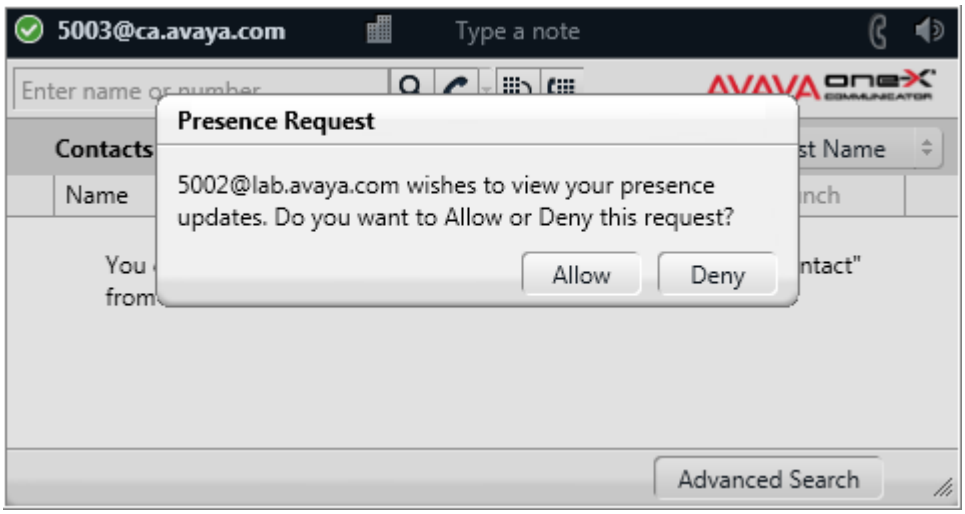
Chapter 7: Administration

Access control policy

Presence Services 7.0 uses the Avaya Breeze™ service attribute to set the global, cluster, or user access control policy. For more information, see “Configuring access control policy”.

System Manager ACL configuration at **Users** > **User Management** > **System Presence ACLs** used for Releases prior to Release 7.0 Presence Services deployments is not applicable to Presence Services Release 7.0 or later.

Access control determines whether a watcher can view a user presence. Following are the three policy levels: `ALLOW`, `BLOCK`, and `CONFIRM`. `ALLOW` makes a user presence public for all watchers. `BLOCK` makes a user presence private for all watchers. `CONFIRM` gives the user the choice to allow or block presence for a particular watcher through an authorization request as presented to the user by the presence client. For example, Avaya one-X® Communicator displays an authorization dialog box as shown in the figure below.



When changing an access control policy from `ALLOW` or `BLOCK` to `CONFIRM`, the presentity clients do not display access control authorization requests until after the presentity logs out and then in again. When changing the policy from `CONFIRM` to `ALLOW` or `BLOCK`, previous access control authorizations remain in force. To remove all previous access control decisions, use the access control script tool.

Note:

The default access control policy should not be set to `CONFIRM` if non-ACL-capable endpoints are deployed.

The access control policy is effective immediately. The new watcher requests will receive an authorization request on the presentity's Avaya one-X® Communicator client. The existing watchers will not receive any new presence updates until the presentity logs out and in again. Once the presentity logs in again, they will get an authorization request for anyone who was watching the presentity before, or has just requested to watch them. Immediate authorization requests are avoided on all existing presentities who are being watched as it will impact the network. For example, if there were 125,000 presence users, each having 25 contacts, there will be over 3 million authorization requests. Batching of requests is required, adding complexity and potential new problems.

Configuring access control policy

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **Access Control** section.
6. In the **Access Control Policy** field, select the **Override Default** check box.
7. In the **Effective Value** field, type `Allow`, `Block`, or `Confirm`.
8. Click **Commit**.

Collectors

AES Collector

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

The number of AES servers that AES Collector can use is not limited. If you want AES Collector to use an AES server, ensure that the AES server is added to the System Manager Inventory list. If you want to prevent AES Collector from using an AES server, remove the AES server from the System Manager Inventory list. The System Manager Inventory list is used by AES Collector to identify the pool of AES servers that it can acquire a user from.

AES Collector collects events for any user with AES Collection explicitly enabled in the Presence communication profile, or enabled through the AES system policy. The AES system policy is at **Elements** > **Presence** > **Configuration** > **Publish Presence with AES Collector – Default**. For more information, see “Assigning an Avaya Presence/IM communication address to a user”. AES Collector sequentially tries the AES servers configured in the System Manager Inventory until it acquires the user from that AES.

Configuring AES Collector

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the AES Collector attribute group.
6. In the **AES Collector Enabled** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type True.
7. In the **AES Server Username** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the user name that the AES collector will use when connecting to the AES server.
8. In the **AES Server Password** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the password that the AES collector will use when connecting to the AES server.
9. In the **Publish DND Status** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `true` to enable the AES collector to publish Do Not Disturb (DND) status. The default value is `false`, which disabled the feature.
10. In the **Away Timer (mins)** field:
    a. Select the **Override Default** check box.

b. In the **Effective Value** field, set the time to change the state to away after a call is disconnected. The default value if `0`, which disables the feature.

11. In the **Out of Office timer (mins)** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the time to change the state to out-of-office after a call is disconnected. The default value is `0`, which disables the feature.
12. Click **Commit**.

    If you change any of the following attributes, you must restart the AES Collector:

    - AES Server Username
    - AES Server Password
    - Publish DND Status
    - Away Timer (mins)
    - Out of Office timer (mins)

    To restart AES Collector, start and stop AES Collector using Step 6.
13. Install the root CA certificate.

    If the certificate on AES was signed by a certificate authority, install the root CA certificate from the authority. Else, install the AES self-signed certificate generated during the AES installation.

Installing the root CA certificate

About this task

For AES prior to Release 6.x, use the product certificate in the ZIP bundle. For AES Release 7.x or AES Release 6.x using 3rd party certificate, the CA signing the AES certificate needs to be imported into Avaya Breeze™.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the Avaya Breeze™ cluster.
3. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze Instances)**.
4. In the **Select Store Type to install trusted certificate** field, select **All**.
5. Click **Choose File** and browse to the certificate file.
6. Click **Retrieve Certificate**.
7. Click **Commit**.

Configuration of AES Collector in a Geographic Redundant deployment

To configure AES Collector on Presence Services deployed in Geographic Redundant mode, AES Collector must be configured on Avaya Breeze™ clusters in both data centers. See “Configuring AES Collector” to configure AES Collector on each cluster.

During normal operations, a user enabled for presence collection through AES Collector is managed by the home data center as configured in Presence Profile. When the data center is not operational, the remote data center automatically takes over the collection of presence information of the user.

Exchange Collector

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 availability 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 Calendar and Out of Office Assistant records from the Exchange server by using MS Exchange Web Service (EWS) and converts these records into presence events. Exchange Collector only collects for Aura users that are configured with a Microsoft Exchange communication address in their communication profile.

Presence Services 7.0 supports the following versions of MS Exchange Server:

- 2007
- 2010
- 2010 Service Packs
- 2013

Exchange Collector connects to the Microsoft Exchange server securely using TLS. This connection requires that a Microsoft Exchange server certificate be installed into the Avaya Breeze™ cluster where Exchange Collector is enabled. Typically, the CA certificate should be used as CA certificate is used to sign the certificates for all the Microsoft Exchange servers in the network if there is more than one. Otherwise, a certificate for each Microsoft Exchange server must be imported into the cluster. For information about exporting certificates from Microsoft Exchange Server, refer to the Microsoft documentation.

Note:

MS Exchange 2010 requires impersonation. However, for MS Exchange 2013, you must run the command **`Add-MailboxPermission -Identity username@domain -user psadmin -AccessRights FullAccess -InheritanceType all`** for all used mailboxes, instead of configuring impersonation. Before you run the command, create or import the Presence Services session. For more information, see “Creating or importing a Presence Services session”.

Creating or importing a Presence Services session

Procedure

1. To create a Presence Services session, run the following in the powershell on the Exchange server:

   ```
   $Session = New-PSSession -ConfigurationName Microsoft.Exchange -
   ConnectionUri connection URI -Authentication Kerberos -Credential
   $UserCredential
   ```

   connection URI is a string provided in the following format: `http://FQDN of the exchange server/PowerShell/`. For example, if your exchange FQDN is `MyExchangeServer.company.com` then *connection URI* is: `http://MyExchangeServer.company.com/PowerShell/`

2. To import a Presence Services session, run the following in the powershell on the Exchange server:

   ```
   Import-PSSession $Session
   ```

Configuring Exchange Collector

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the Exchange Collector attribute group.
6. In the **Exchange Collector Enabled** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type True.

      Exchange Collector collects and publishes Presence information on behalf of clients that do not support a native Presence implementation.
7. In the **Exchange Server URI** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the URI of the Exchange server.
8. In the **Exchange Server Username** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the user name that the Exchange collector must use when connecting to the Exchange server.

9. In the **Exchange Server Password** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the password that the Exchange collector must use when connecting to the Exchange server.
10. In the **Exchange Calendar Information Polling Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the calendar information collection interval in minutes.
11. In the **Exchange Calendar Request Rate** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the maximum calendar request per minute rate for the collector to send to the server.
12. In the **Exchange Out-Of-Office Information Polling Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the Out-Of-Office information collection interval in minutes.
13. In the **Exchange Out-Of-Office Request Rate** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the Out-Of-Office request per minute rate for the collector to send to the server.
14. In the **Exchange Publishing Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the collector publish interval in minutes.
15. Click **Commit**.

    If you change any of the following attributes, you must restart Exchange Collector:

    - Exchange Server URI
    - Exchange Server Username
    - Exchange Server Password
    - Exchange Calendar Information Polling Period
    - Exchange Calendar Request Rate
    - Exchange Out-Of-Office Information Polling Period
    - Exchange Out-Of-Office Request Rate
    - Exchange Publishing Period

    To restart Exchange Collector, start and stop Exchange Collector using Step 6.

Configuration of Exchange Collector in a Geographic Redundant deployment

To configure Exchange Collector on Presence Services deployed in Geographic Redundant mode, Exchange Collector must be configured on Avaya Breeze™ clusters in both data centers. See “Configuring Exchange Collector” to configure Exchange Collector on each cluster.

During normal operations, a user enabled for presence collection through Exchange Collector is managed by the home data center as configured in Presence Profile. When the data center is not operational, the remote data center automatically takes over the collection of presence information of the user.

Domino Collector

Domino Collector is a Presence Services component that provides integration with an IBM® Domino enterprise deployment. Domino Collector collects and publishes the calendar and out-of-office information for Domino mailboxes. The Domino server manages Domino mailboxes. The Domino Calendar web service, which is included with Presence Services, must be installed on the Domino server. The Domino Calendar web service processes the calendar and out-of-office web service and retrieves calendar and out-of-office information. The results are sent back to the collector.

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 presence events.
- Collects for Aura users configured with `LotusNotes` communication address in their communication profile.

Presence Services supports Domino Server 9.0.1.

Configuring Domino Collector

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the Domino Collector attribute group.
6. In the **Domino Collector Enabled** field:
   a. Select the **Override Default** check box.

b. In the **Effective Value** field, type True.

7. In the **Domino Server Web Service URI** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the URI of the Domino web server.
8. In the **Domino Server Username** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the user name that the Domino collector must use when connecting to the Domino server.
9. In the **Domino Server Password** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, set the password that the Domino collector must use when connecting to the Domino server.
10. In the **Domino Calendar Information Polling Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the calendar information collection interval in minutes.
11. In the **Domino Calendar Request Rate** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the calendar request per minute rate for the collector to send to the server.
12. In the **Domino Out-Of-Office Information Polling Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the Out-Of-Office information collection interval in minutes.
13. In the **Domino Out-Of-Office Request Rate** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the Out-Of-Office request per minute rate for the collector to send to the server.
14. In the **Domino Publishing Period** field:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, set the interval in minutes.
15. Click **Commit**.

    If you change any of the following attributes, you must restart Domino Collector:

    - Domino Server Web Service URI
    - Domino Server Username

- Domino Server Password
- Domino Calendar Information Polling Period
- Domino Calendar Request Rate
- Domino Out-Of-Office Information Polling Period
- Domino Out-Of-Office Request Rate
- Domino Publishing Period

To restart Domino Collector, start and stop Domino Collector using Step 6.

Configuration of Domino Collector in a Geographic Redundant deployment

To configure Domino Collector on Presence Services deployed in Geographic Redundant mode, Domino Collector must be configured on Avaya Breeze™ clusters in both data centers. See “Configuring Domino Collector” to configure Domino Collector on each cluster.

During normal operations, a user enabled for presence collection through Domino Collector is managed by the home data center as configured in Presence Profile. When the data center is not operational, the remote data center automatically takes over the collection of presence information of the user.

Domino Collector integration

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	Installing the Domino Calendar web service database on page 59	
3	Sign the Domino Calendar web service database.	Domino Server	Signing the Domino Calendar web service database on page 60	
4	Create a new Domino user for Domino Collector.	Domino Server	Creating a Domino user for Domino Collector to authenticate on page 62	
5	Provide access to the Domino user.	Domino Server	Providing reader access to the	

Table continues…

No.	Task	Server	Link	✔
			Domino user for Domino Collector to authenticate on page 70	
6	Add Lotus Notes handle to the Domino user.	Presence Services	Adding Lotus Notes handle to a System Manager user on page 74	
7	Configure Domino Collector.	Presence Services	Domino Collector configuration on page 75	

Installing the Domino Calendar web service database

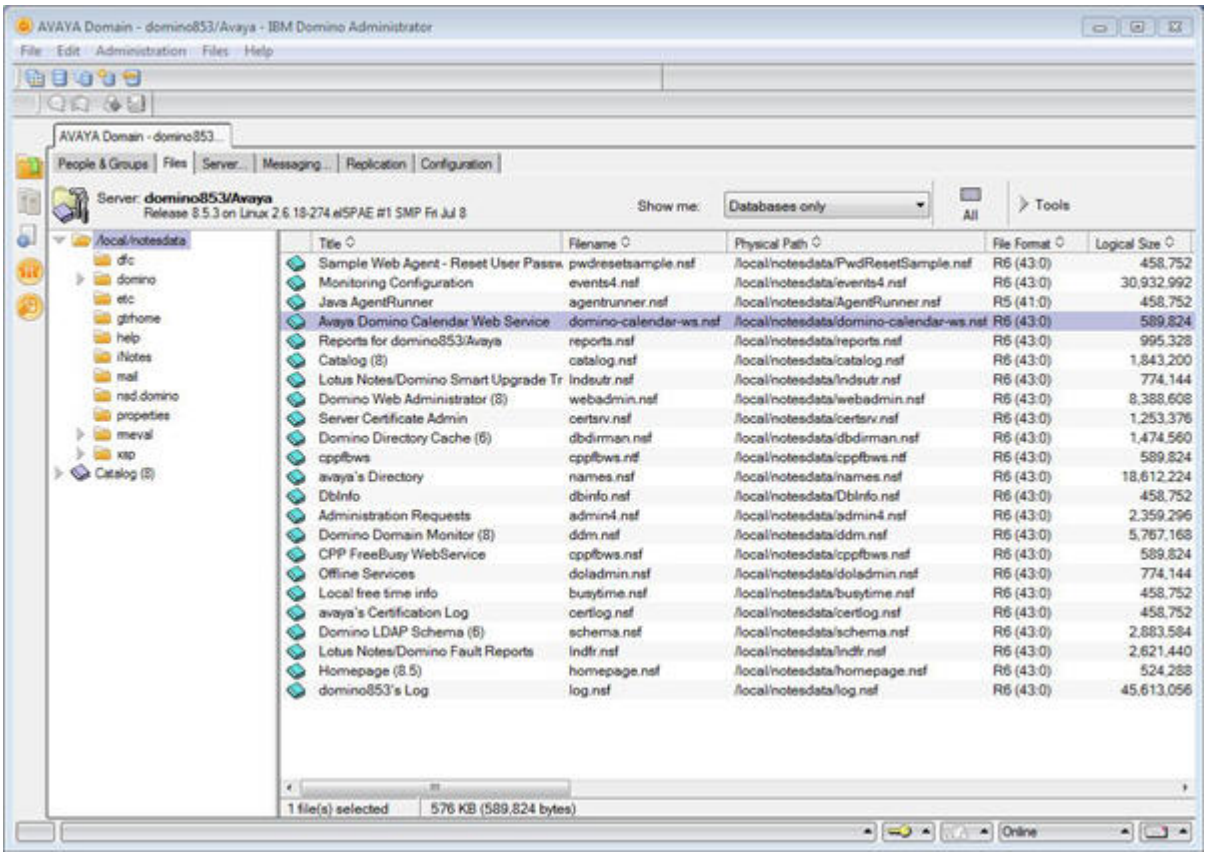
Procedure

1. Extract the Domino Calendar web service file, `domino-calendar-ws.nsf`, from the `PresenceServices-Bundle` 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.

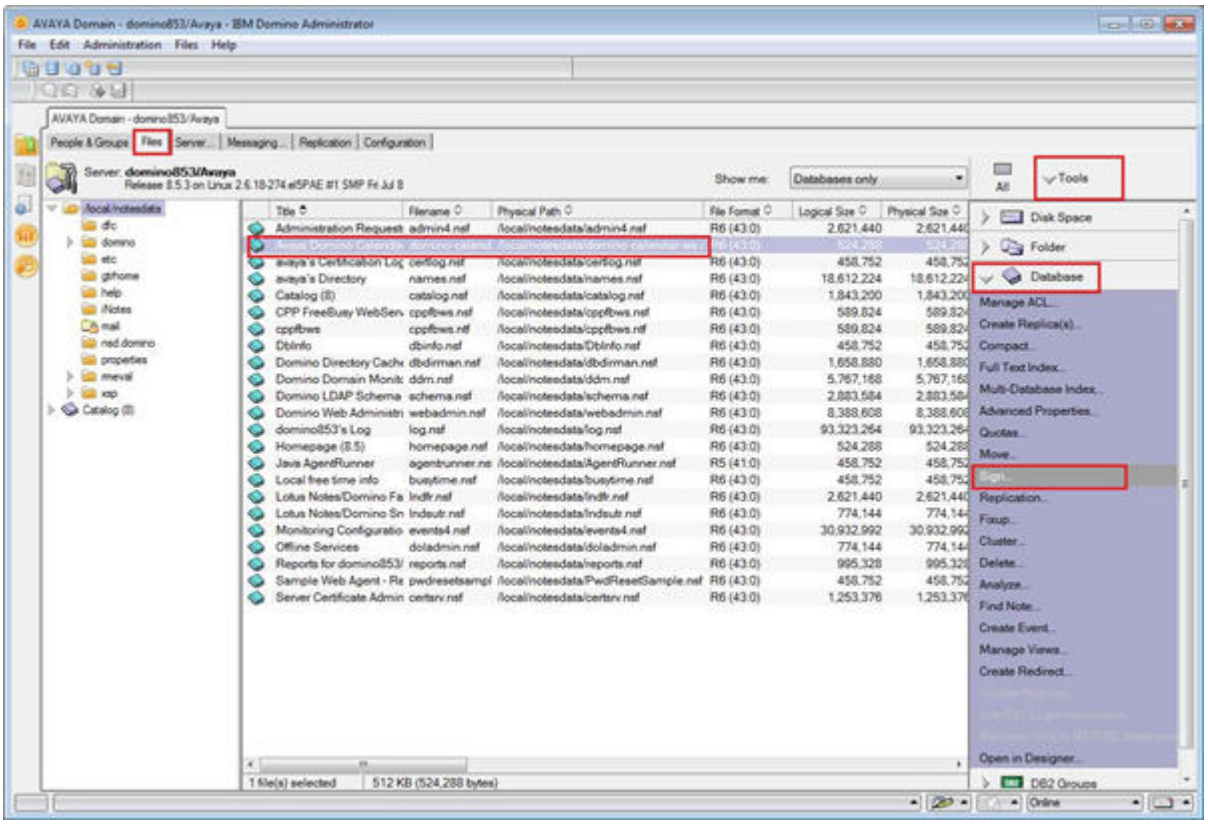


Signing the Domino Calendar web service database

Procedure

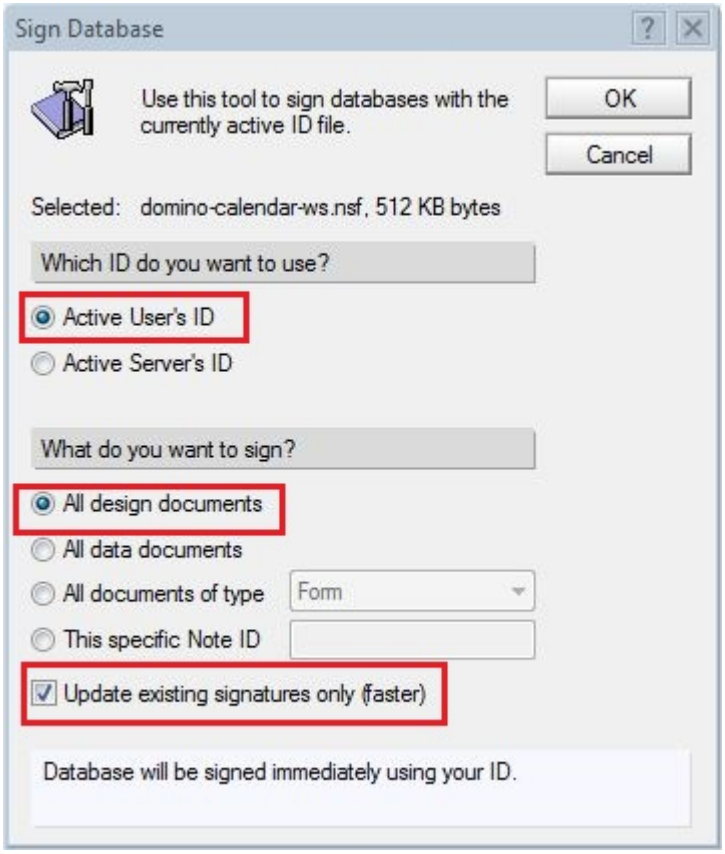
1. Log in to the Domino Administrator client with the administrator credentials.
2. Click the Domino server.
3. Click **Files**.

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**.

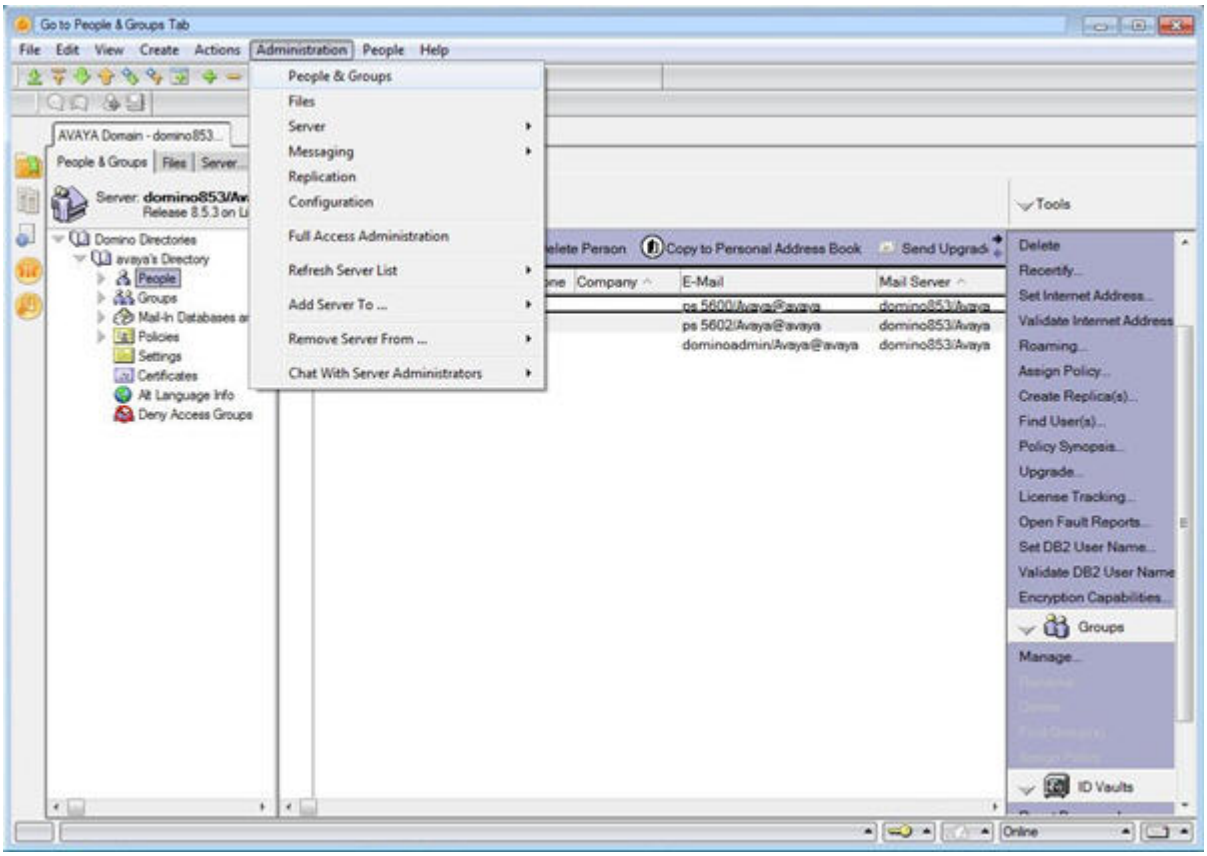
    The system displays the **1 database processed - 0 errors** message.

Creating a Domino user for Domino Collector to authenticate

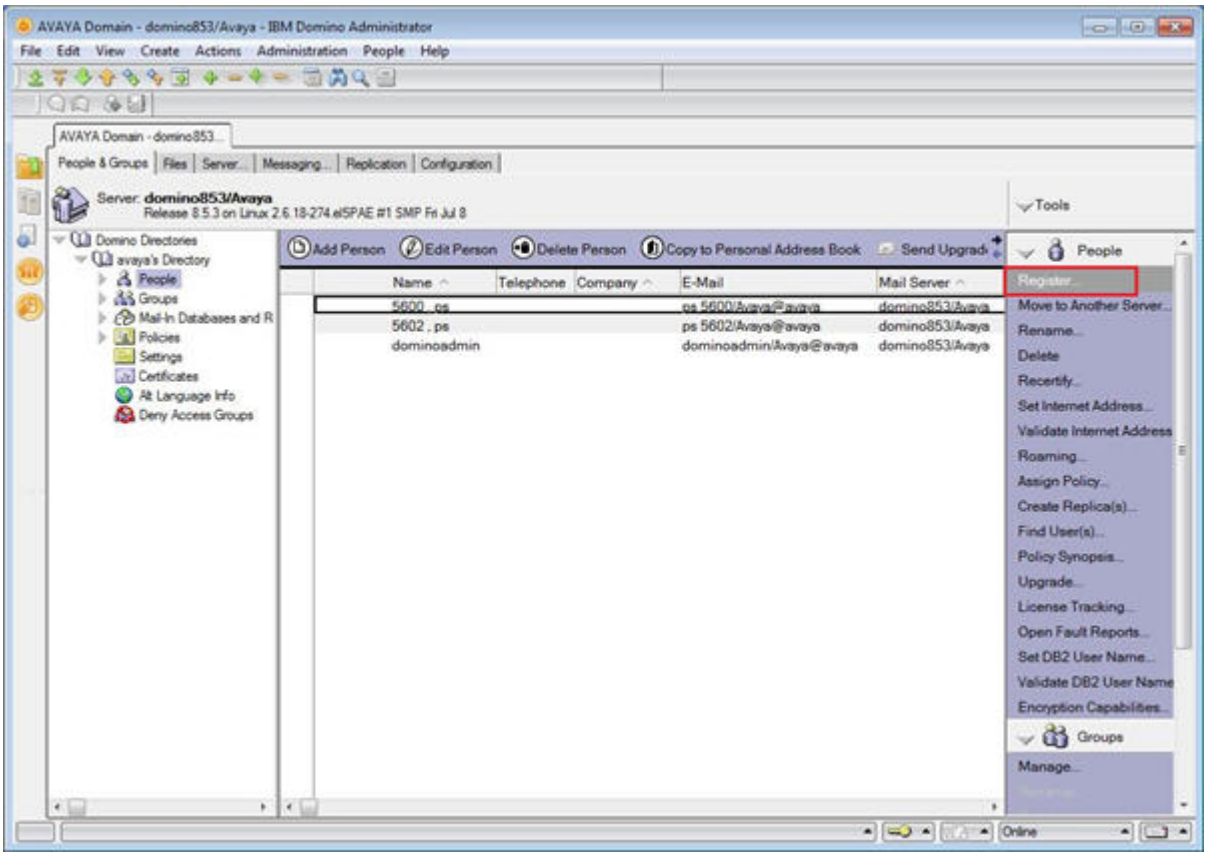
Procedure

1. Log in to the Domino Administrator client.

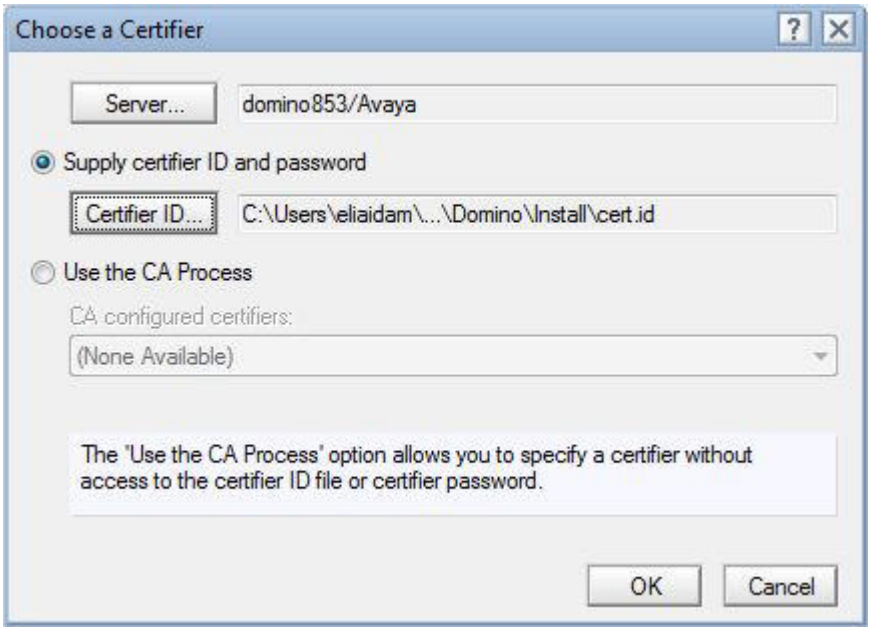
2. Click **Administration** > **People & Groups**.



3. Click **Register**.

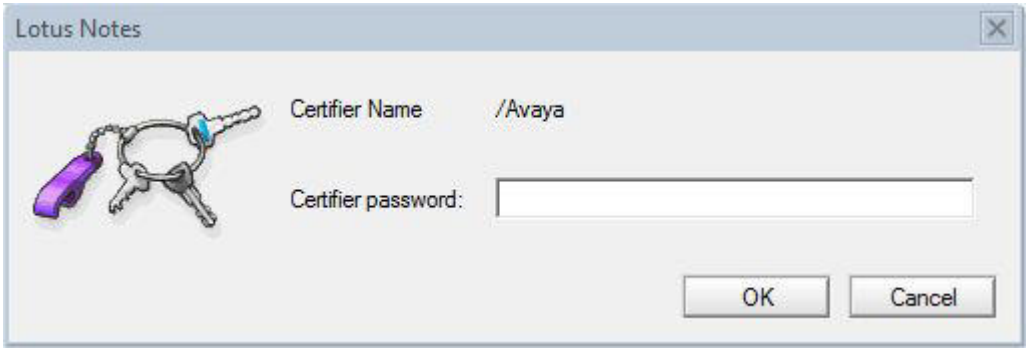


4. Click **Server**, and select the server.



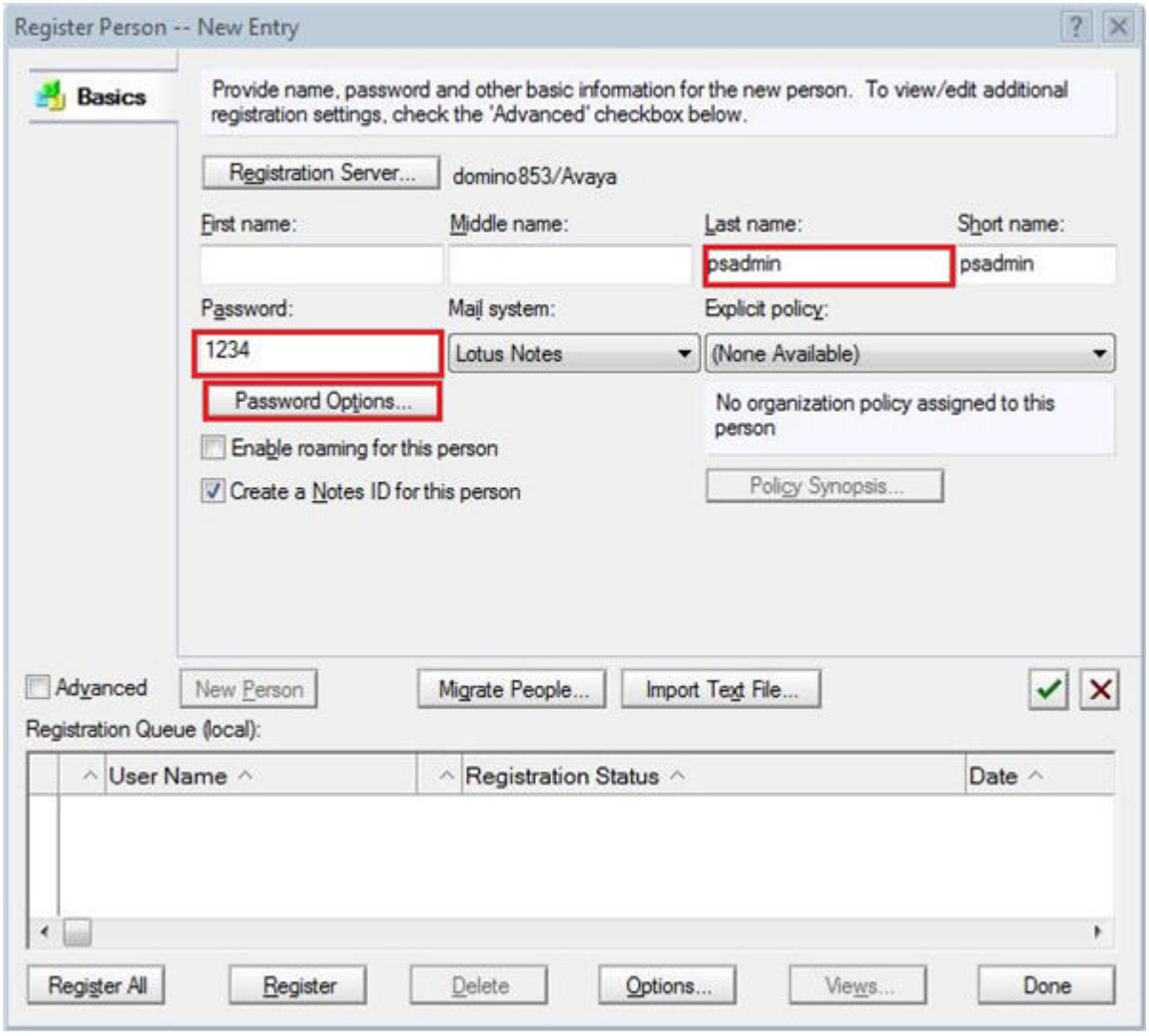
The system creates the `cert.id` file is created when the administrator launched the Domino client for the first time.

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

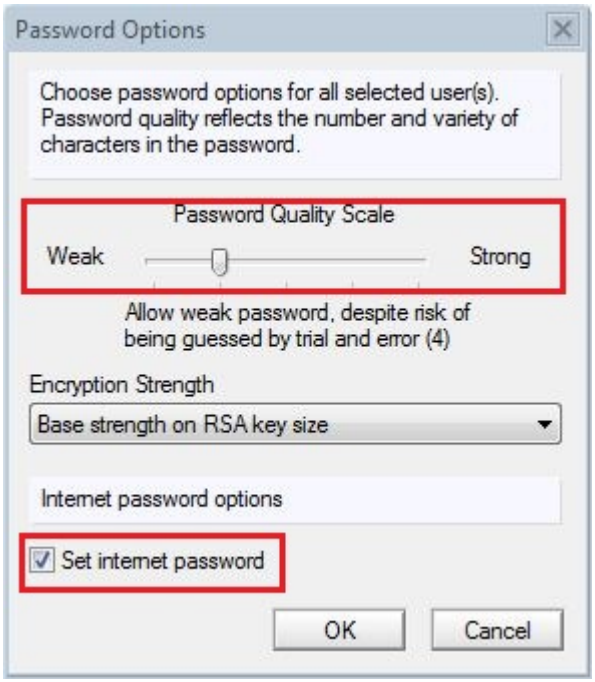


8. In the **Last name** field, type the last name.

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

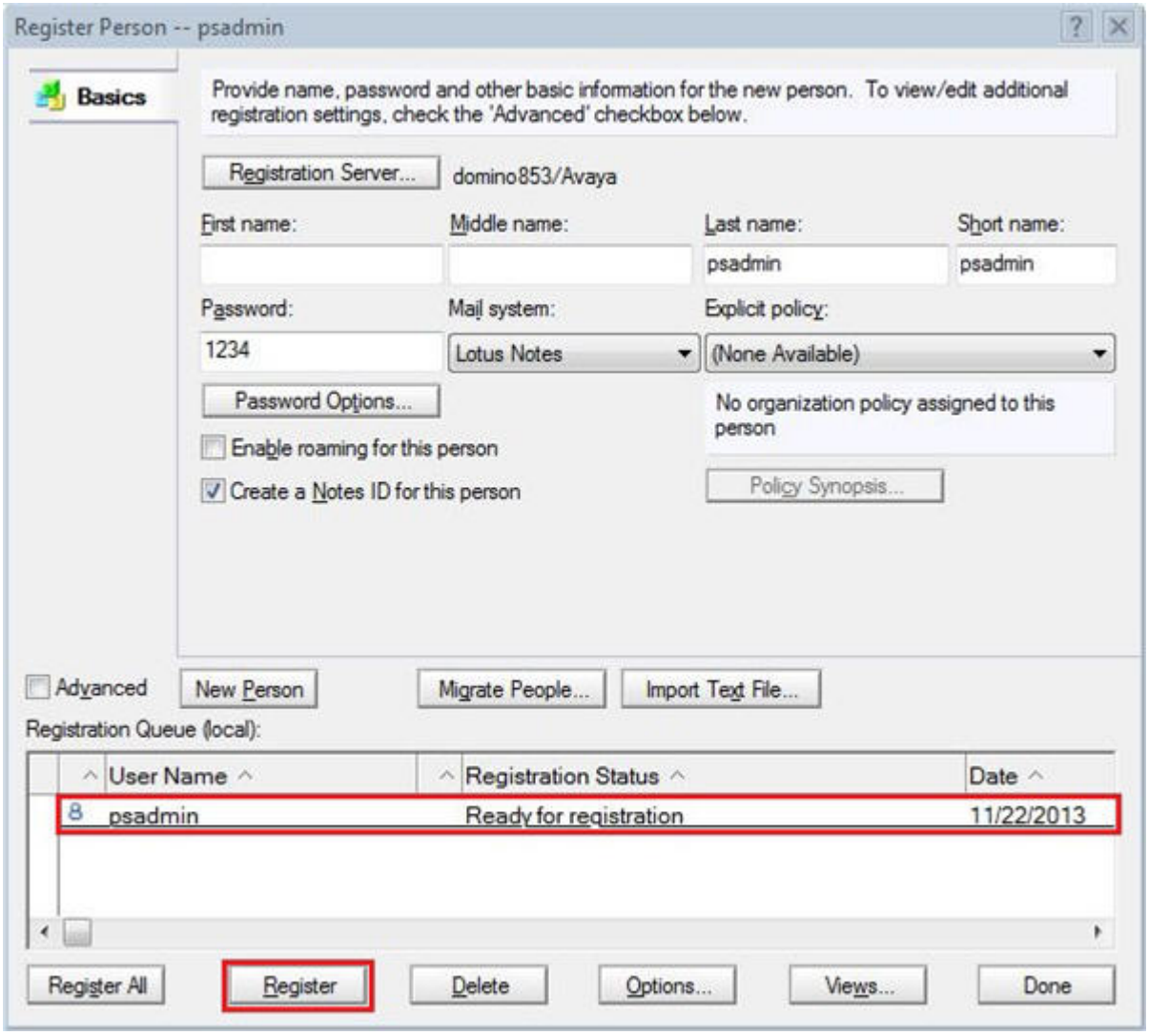


10. On the **Password Options** page:
    a. Select the value of **Password Quality Scale**.
    b. Select the **Set internet password** check box.
    c. Click **OK**.



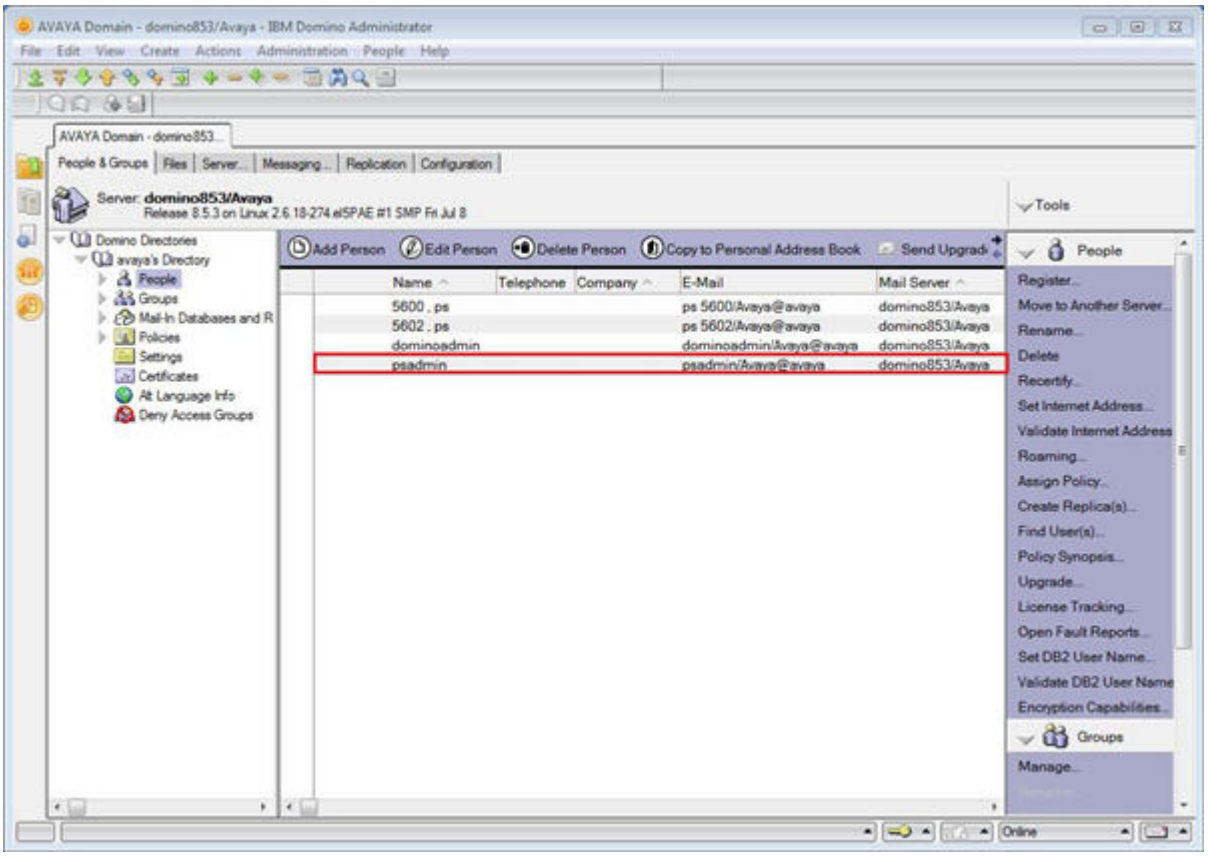
11. Select the green check mark box.

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



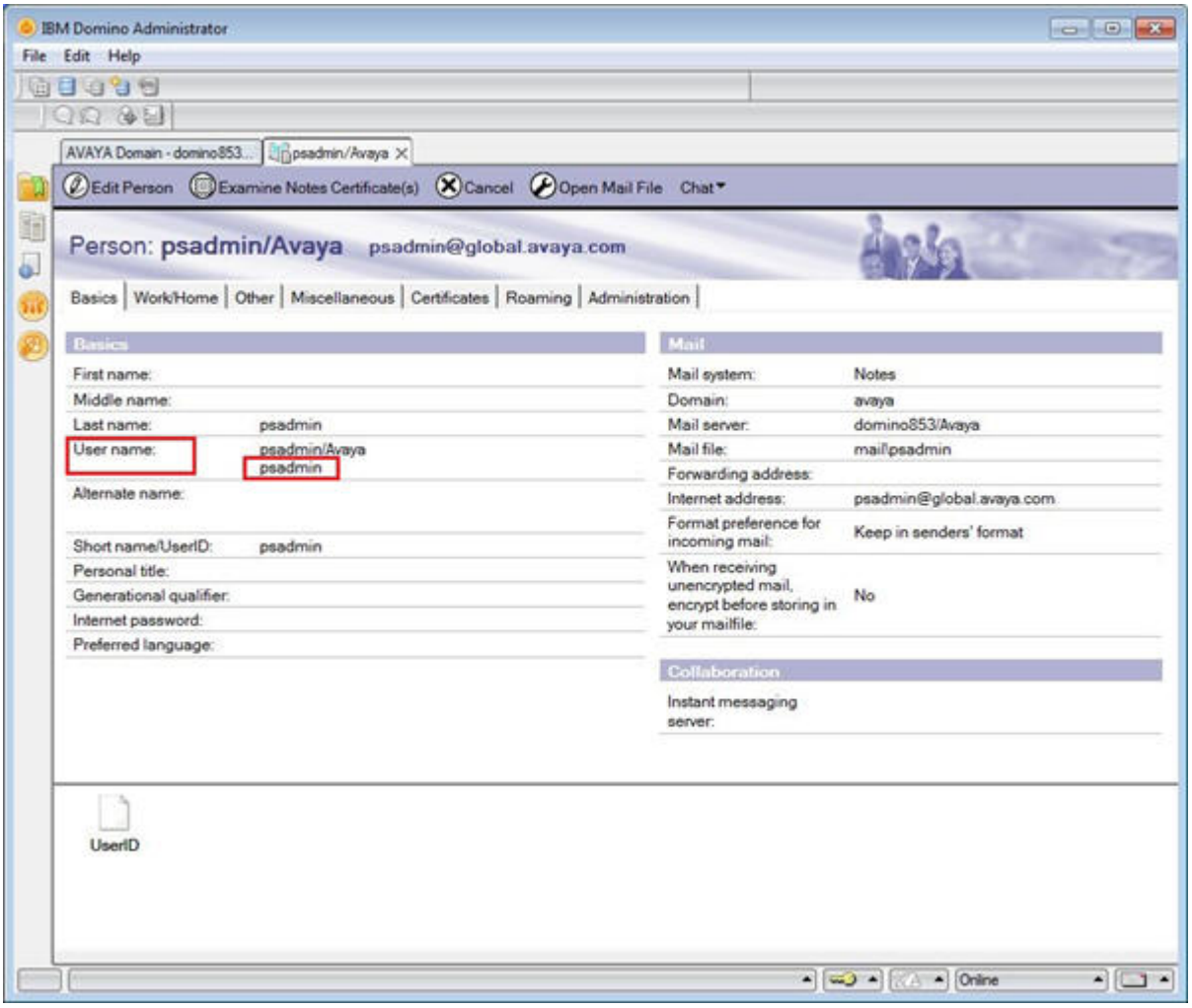
13. Click **OK**.
14. Click **Done**.

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

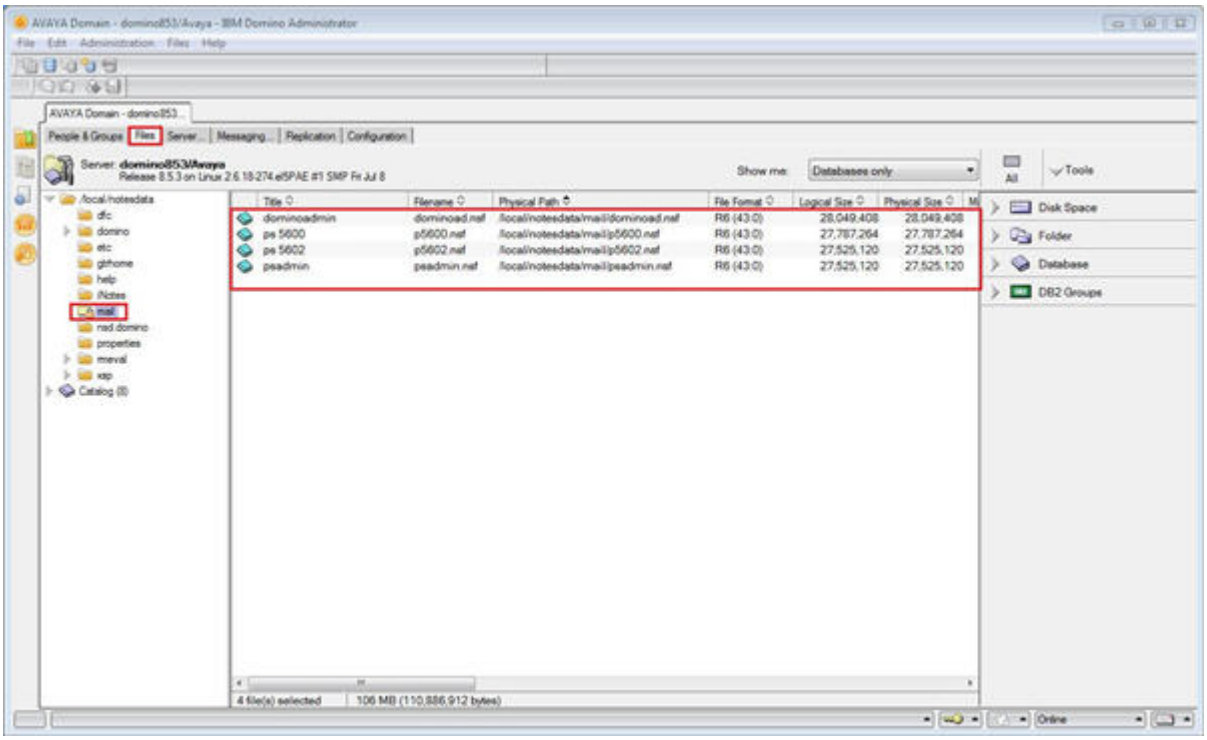
About this task

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.

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

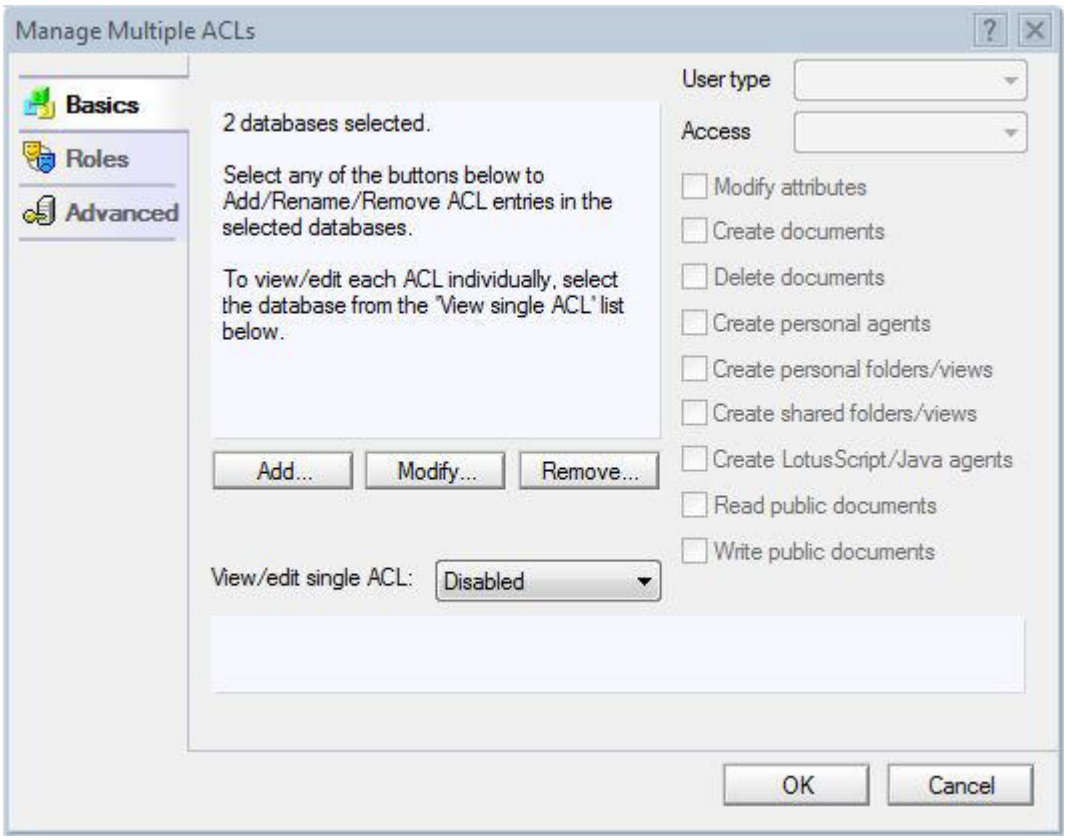


3. Select all mail files for which calendar and out-of-office information are being collected.

Note:

To collect calendar and out-of-office information for any new users, the administrator must navigate to this page and select the new mail file.

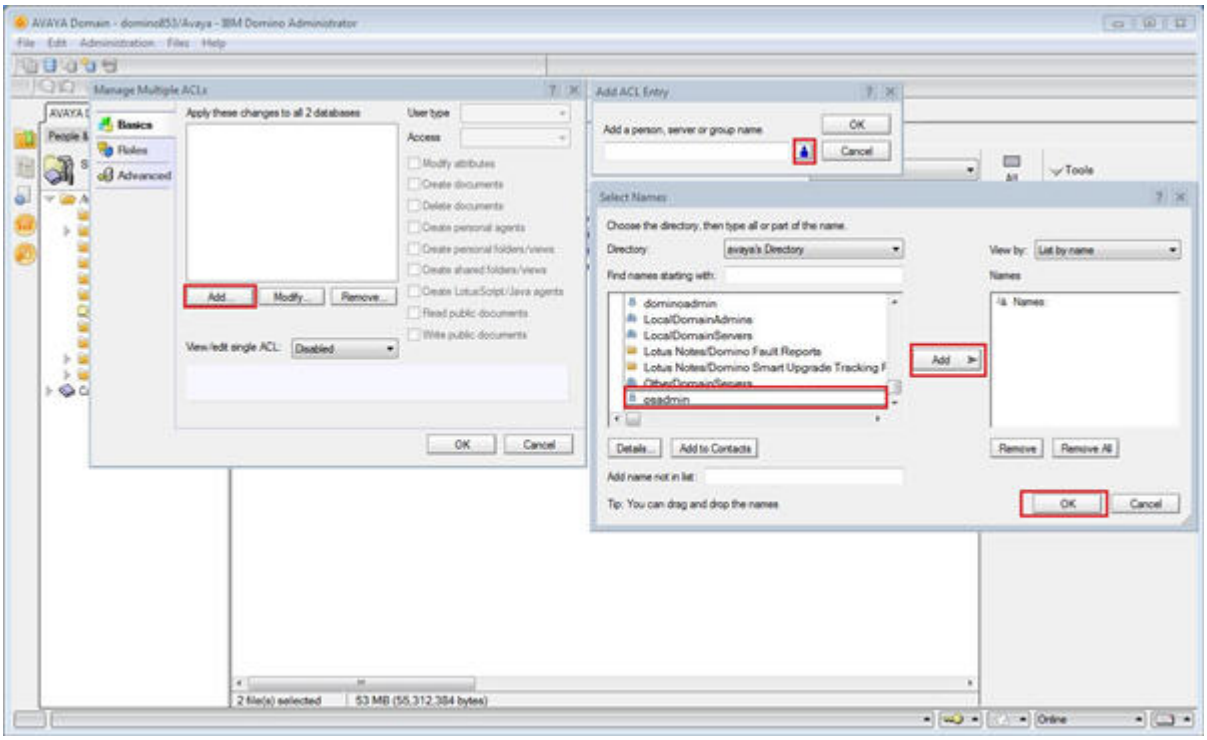
4. Right-click the selected files, and click **Access Control** > **Manage**.



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

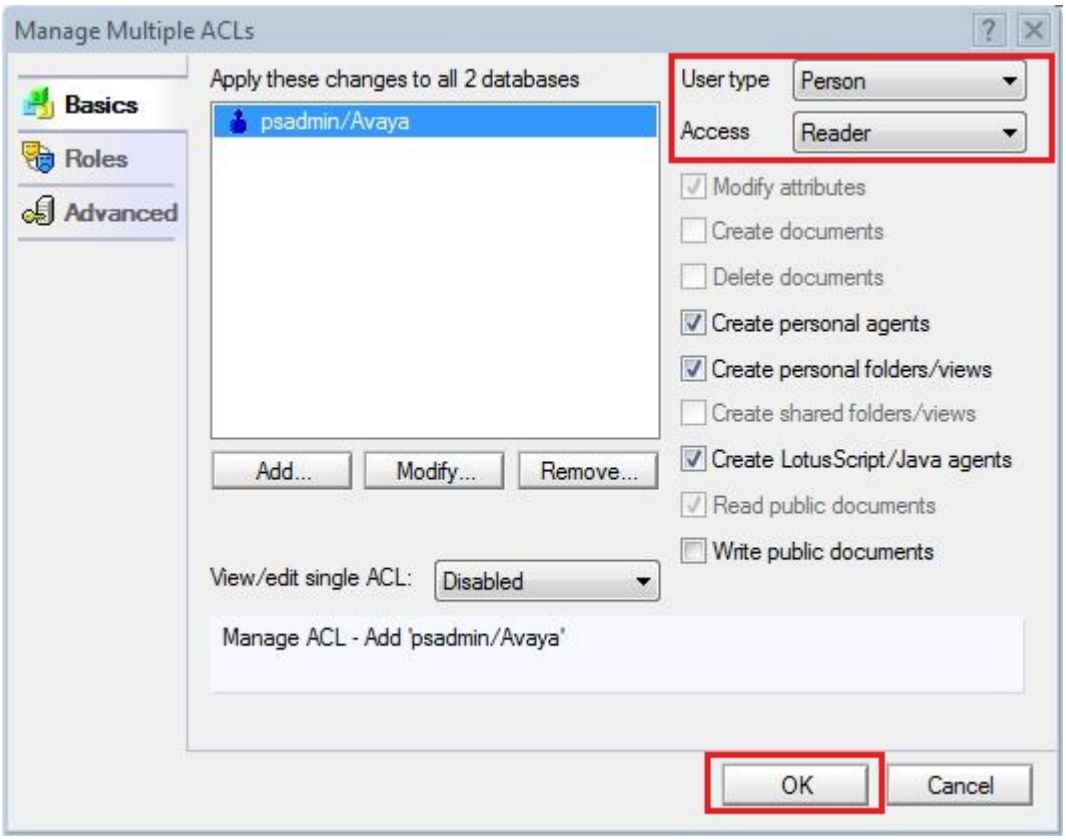
   In the example, `psadmin` is the Domino user.
7. Click **Add**.

8. Click **OK**.



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

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



11. Click **OK**.
12. Click **OK**.

Adding Lotus Notes handle to a System Manager user

Procedure

1. Log in to the System Manager web console as an administrator.
2. Click **User Management** > **Manage Users**.
3. Select the 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 **Lotus Notes**.
7. 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

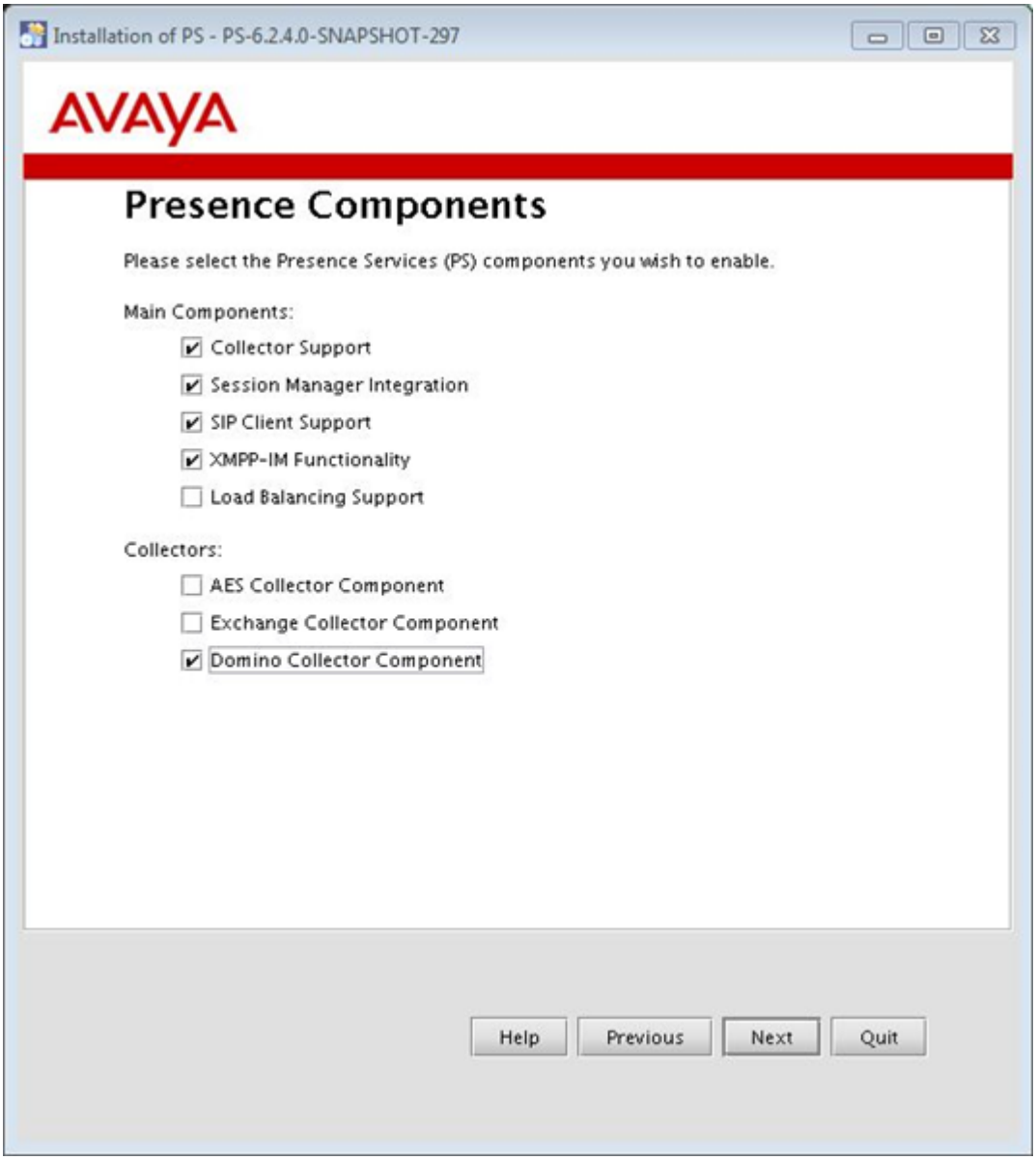
Configuring Domino Collector during the Presence Services graphical installation

About this task

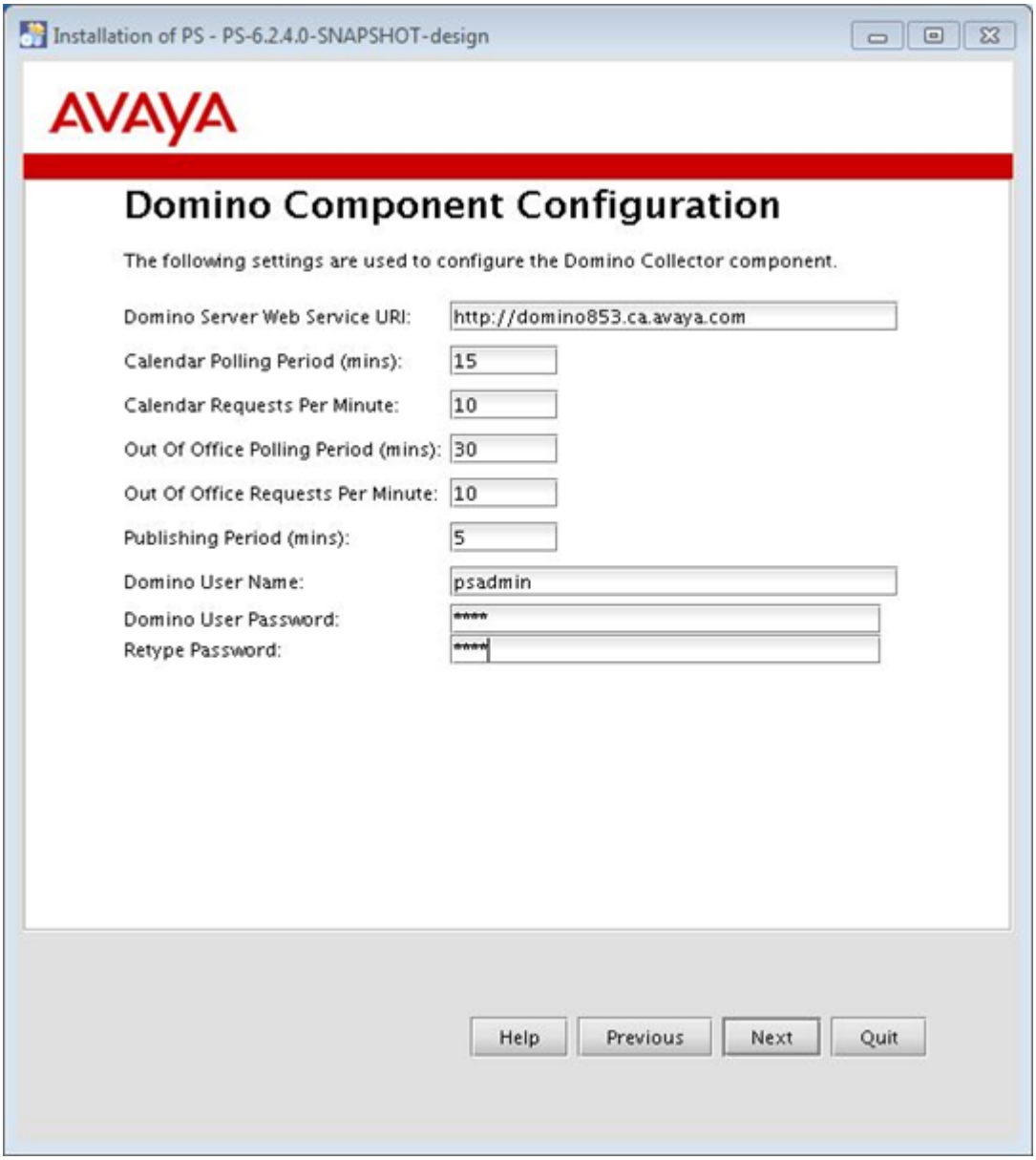
You must perform this procedure during the Presence Services installation.

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.



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

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

Domino Collector Configuration field descriptions

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

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*.

Domino Collector configuration parameters

Name	Description	Default value
inclDomino	Specifies whether to install Domino Collector or not.	`false`

Table continues…

Name	Description	Default value
	To allow the installation of Domino Collector, set this field to `true`. To prevent the installation of Domino Collector, set this field to `false`.	
DOMINO_SERVER_URI	Specifies the URI of the Domino server. For example, `http:// < domino-server-fqdn >`. 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
DOMINO_CALENDAR_POLLING_PERIOD	Specifies how frequently Domino Collector polls the Domino server to get calendar information for users.	`15` minutes
DOMINO_CALENDAR_REQUEST_RATE	Specifies how many Calendar Information requests are sent to the Domino server every minute.	`10`
DOMINO_OOTO_POLLING_PERIOD	Specifies how frequently Domino Collector polls the Domino server to get Out-of-Office information for users.	`30` minutes
DOMINO_OOTO_REQUEST_RATE	Specifies how many Out-of-Office requests are sent to the Domino server every minute.	`10`
DOMINO_PUBLISHING_PERIOD	Specifies how frequently Domino Collector sends the latest Domino presence tuple information to the XCP core for publishing.	`5` minutes
DOMINO_USERNAME	Specifies the user name of a Domino user who has the required permissions to read mail files for the requested users.	blank
DOMINO_USER_PASSWORD	Specifies the password of the Domino user.	blank

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.

Federation

Presence Services allows presence and IM exchange between Avaya Aura® users that are hosted by a Presence Services cluster. Through federation, Presence Services allows presence and IM exchange between Avaya Aura® users, and users that are hosted by a third-party server. Federation can also be used to allow presence and IM exchange between Avaya Aura® users in different Presence Services clusters.

Presence Services federation is certified with the following servers:

- Another Avaya Aura® Presence Services cluster prior to Release 7.0 using XMPP
- Another Avaya Aura® Presence Services cluster Release 7.0 or later using SIP
- Cisco Jabber using XMPP
- Ignite Realtime Openfire using XMPP
- Microsoft Lync using SIP

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

Lync federation

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 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 Lync client, 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 Lync federation 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 usingAvaya Aura® clients.

Additionally, an Enterprise user can obtain the overall presence availability of their Aura colleagues by adding the presence handle of an Avaya Aura® user to their buddy list. The MOC/Lync client displays the presence against the contact address of an Avaya Aura® user.

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 Lync federation when Inter-Tenant Communication Control is enabled on System Manager.

When you enable Lync federation 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 using the MOC/Lync client can see an overall availability of an Avaya Aura® user, by adding the presence handle of an Aura user to their buddy list.

Lync federation is supported in two ways for a given user, True federation and Hybrid federation.

In both cases, the user is defined in the Lync system. A True federation user is not defined in System Manager. A Hybrid federation user is defined in System Manager and is presence enabled. To enable an Aura user as a Hybrid Lync federation user, you must add the Microsoft SIP user handle to the Aura user in System Manager. For more information, see “Adding Microsoft SIP user handles to System Manager”.

Lync federation supports both Interdomain (different domains) and Intradomain (shared domain). The configuration of these federations are different so there is a separate checklist for each.

Note:

Lync Intradomain Federation does not support Hybrid users.

Note:

For correct user routing from Session Manager to the Presence Services cluster, all Avaya Presence/IM handles must be lowercase. Using uppercase characters might result in the inability for Session Manager to route presence and/or IM to an Avaya user from the other system, resulting in loss of presence updates or proper exchanging of IM's. Check if there are any Avaya users on System Manager with Avaya Presence/IM handles in uppercase characters and, if so, edit the handle to lowercase characters.

Adding Microsoft SIP user handles to System Manager

Procedure

1. Log in to the System Manager web console as an administrator.
2. Navigate to **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, in the **Communication Address** section, click **New**.
6. From the **Type** drop-down list box, select **Microsoft 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 `lyncdomain.com`.
8. Click **Add**.

Checklist for configuring Lync Interdomain federation

Table 7: Checklist for configuring Lync Interdomain federation

No.	Task	Link	✔
DNS Administration			
1	Add a DNS SRV record for the Lync gateway.	Adding a DNS SRV record for the Lync gateway on page 84	
2	Add New Host (A).	Adding New Host (A) on page 85	
3	Add a new reverse pointer.	Adding a new reverse pointer on page 85	
Lync server			
4	Generate and import certificate for Lync.	Generating a Web server certificate with server and client authentication on page 86	
5	Import the System Manager CA root certificate into the Lync Edge Trust store.	Importing the System Manager default CA certificate into the Lync Edge Trust Store on page 91	

Table continues…

No.	Task	Link	✔
6	Add Presence Services as an IM service provider for Lync.	Adding Lync gateway as an IM service provider for Lync on page 92	
7	Enable a Lync user for remote access and federation.	Enabling a Lync user for remote access and federation on page 93	
8	Restart the Edge server service after completing changes to DNS.	Restarting the Edge server service after completing changes to DNS on page 94	
9	Download the root certificate of the CA that has signed the certificate used on the External Interface of the Edge server.	Downloading the CA that signed the certificate for the External Interface of the Edge server on page 94	
Presence Services configuration			
10	Configure Lync Interdomain federation.	Configuring Lync Interdomain federation on page 95	
Session Manager configuration			
11	Update the Session Manager TLS certificate.	Updating the Session Manager TLS certificate on page 96	
12	Verify the updated Session Manager TLS certificate.	Verifying the updated Session Manager TLS certificate on page 96	
13	Add the host information on Session Manager.	Adding host information on Session Manager on page 97	
14	Add the SIP entities and the entity link representing Lync edge server.	Adding SIP Entities and Entity link representing Lync edge server on page 97	
15	Add the routing regular expressions.	Adding the routing regular expressions on page 99	
16	Add the routing policies.	Adding the routing policies on page 99	
17	Add or update the existing Communication Manager application.	Adding or updating the existing Communication Manager application on page 100	

Adding a DNS SRV record for the Lync 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.

Note:

In multiple Session Manager setup, repeat this procedure for each Session Manager.

Adding New Host (A)

Procedure

1. Log in to the Lync 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.

Note:

In multiple Session Manager setup, repeat this procedure for each Session Manager.

Adding a new reverse pointer

Procedure

1. On the Lync 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**.

Note:

In multiple Session Manager setup, repeat this procedure for each Session Manager.

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.

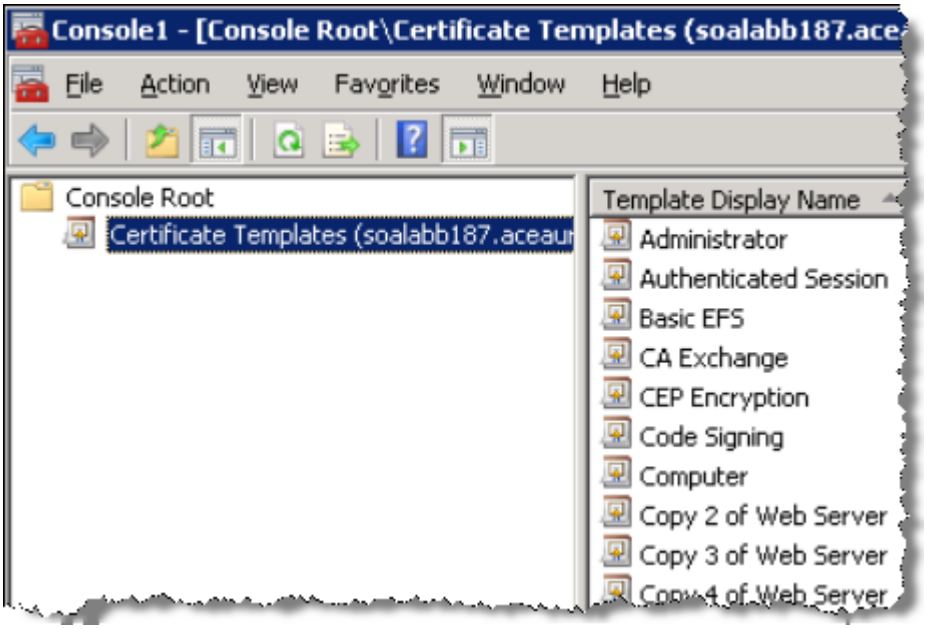
To create a certificate for external interface using Microsoft Certificate Authority (CA) in a Windows 2008 Enterprise Edition Server running a standalone Microsoft Enterprise CA:

Note:

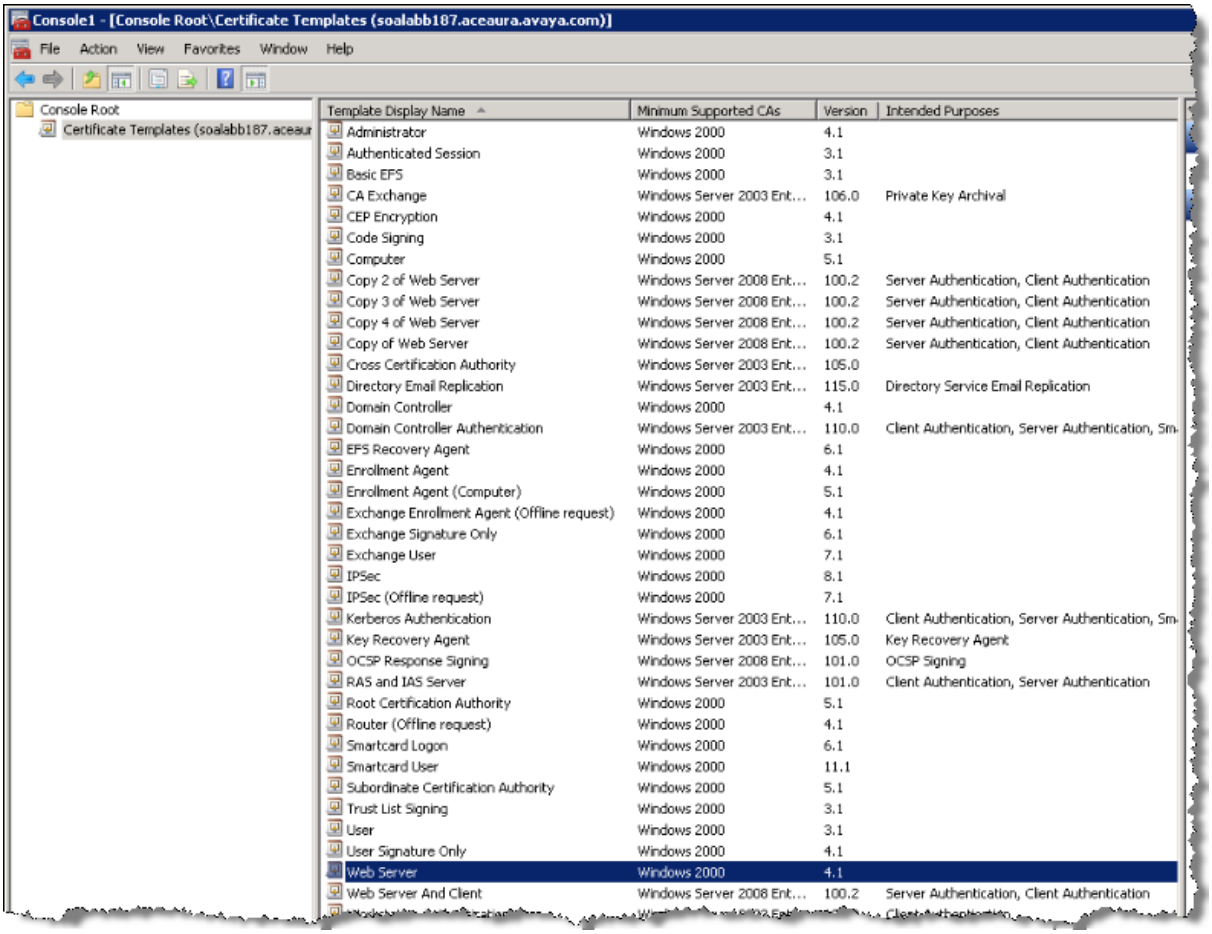
The procedure may vary depending on the configuration and setup of your Microsoft CA.

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**.

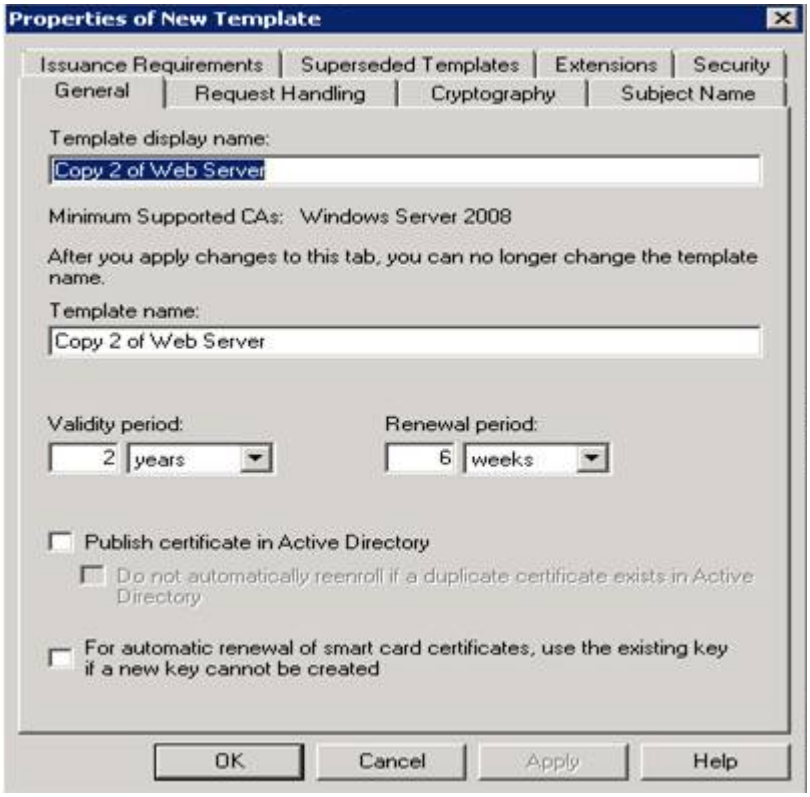


The system displays the Duplicate Template dialog box.

3. On the Duplicate Template dialog box, select the **Windows Server 2008, Enterprise Edition** option.

The system displays the Properties of New Template dialog box.

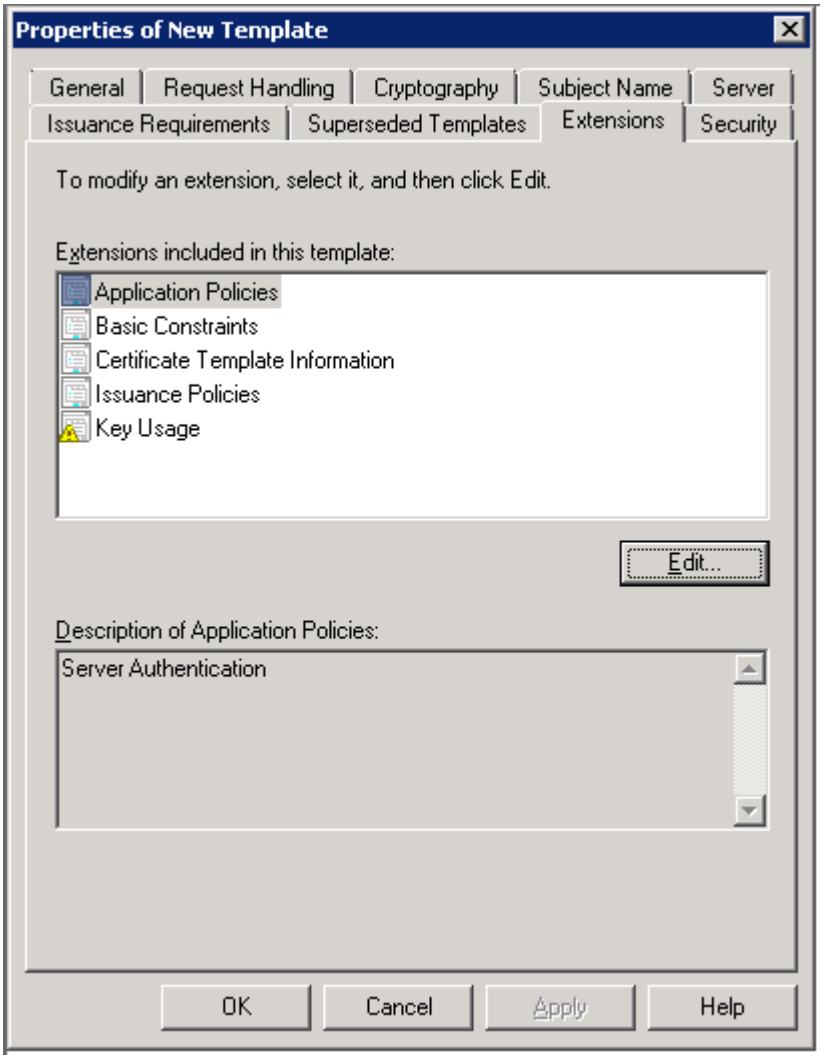
4. In the Properties of New Template dialog box, on the **General** tab, in the **Template display name** and **Template name** field, enter a display name for the template.



Note:

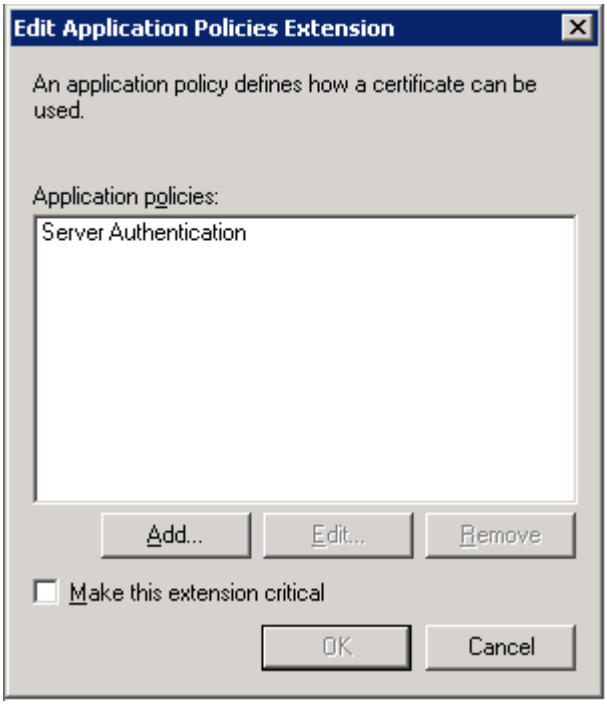
You must use the default entry for the Template name field.

5. On the **Extensions** tab, under the **Extensions included in this template** list, select **Application Policies**, and then click **Edit**.



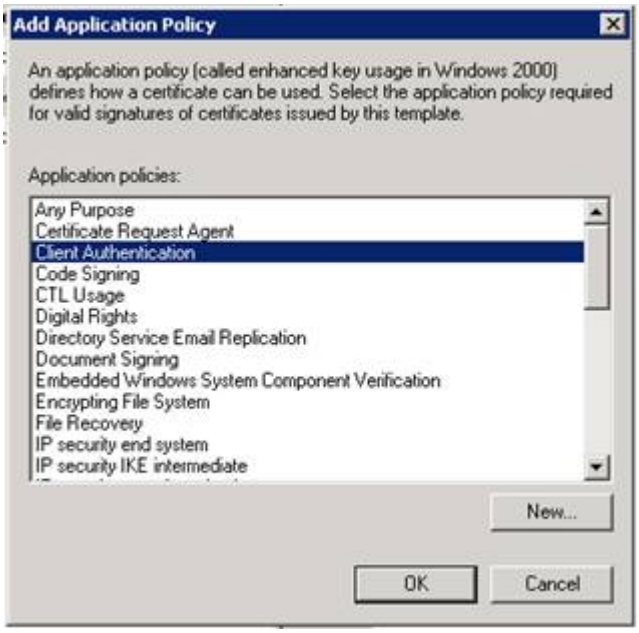
The system displays the Edit Application Policies Extension dialog box.

6. On the Edit Application Policies Extension dialog box, click **Add**.



The system displays the Add Application Policy dialog box.

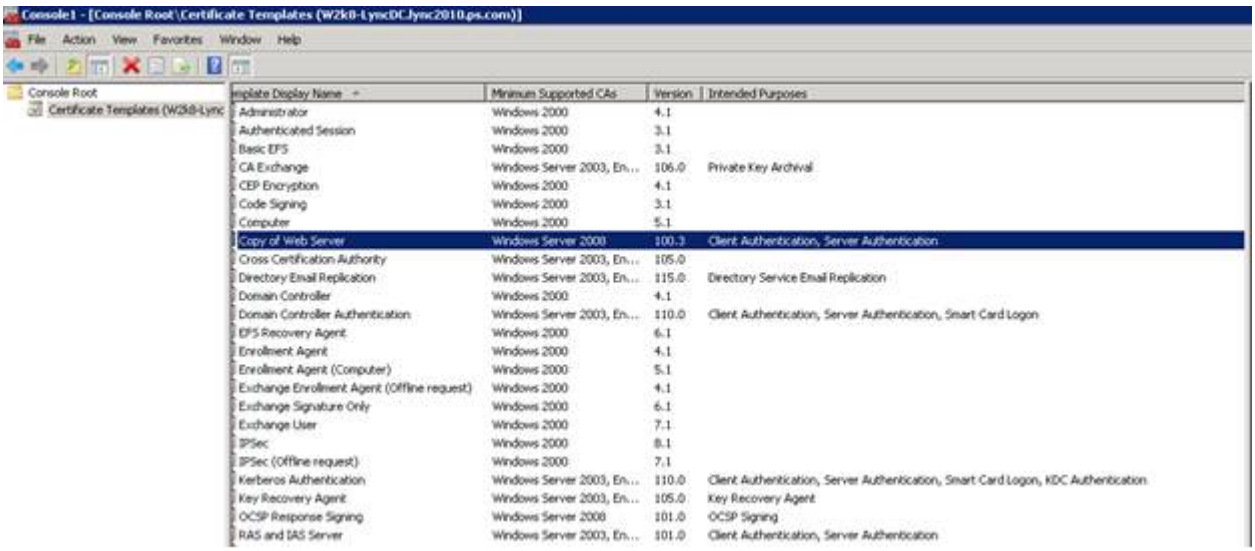
7. On the Add Application Policy dialog box, from the Application policies list, select **Client Authentication**, and then click **OK**.



8. Click **Apply**, and then click **OK**.

Next steps

1. Verify the newly added duplicate Web server certificate in the Certificate Templates list.



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, on the System Manager web console, navigate to **Security** > **Certificates** > **Authority**. Click **View Certificate**. The serial number and expiry date is shown in the window.

       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 System Manager 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.

Adding Lync gateway as an IM service provider for Lync

Procedure

1. On the Lync Front End Server, click **Start** > **All Programs** > **Microsoft Lync Server 2013** > **Micrsoft 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 2013, 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 Access, click the **SIP Federation Providers** tab.
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 the **External Access Policy** tab.
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 the **Access Edge Configuration** tab.
14. Click **Edit** > **Show details**.

    The system displays the Edit Access Edge Configuration screen.
15. Ensure that you select the following:
    - **Enable federation and public IM connectivity**
    - **Enable partner domain discovery**
    - **Enable remote user access**
    - **Enable anonymous user access to conferences**
16. To save the changes, click **Commit**.

    Note:

    In multiple Session Manager setup, repeat this procedure for each Session Manager.

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.

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 Lync Server Access Edge service.
3. Right-click **Lync Server Access Edge** service and select **Start** > **Start all stopped Services**.

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.

    Note:

    In multiple Session Manager setup, repeat this procedure for each Session Manager.

Configuring Lync Interdomain federation

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. In the **Lync Federation: Lync Federation Enabled** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type True.
6. In the **Lync Federation: Lync Domain Name List** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the list of federated Lync domain names.
7. Click **Commit**.

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.

   Note:

   In multiple Session Manager setup, repeat this procedure for each Session Manager.

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**.

   Note:

   In multiple Session Manager setup, repeat this procedure for each Session Manager.

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.

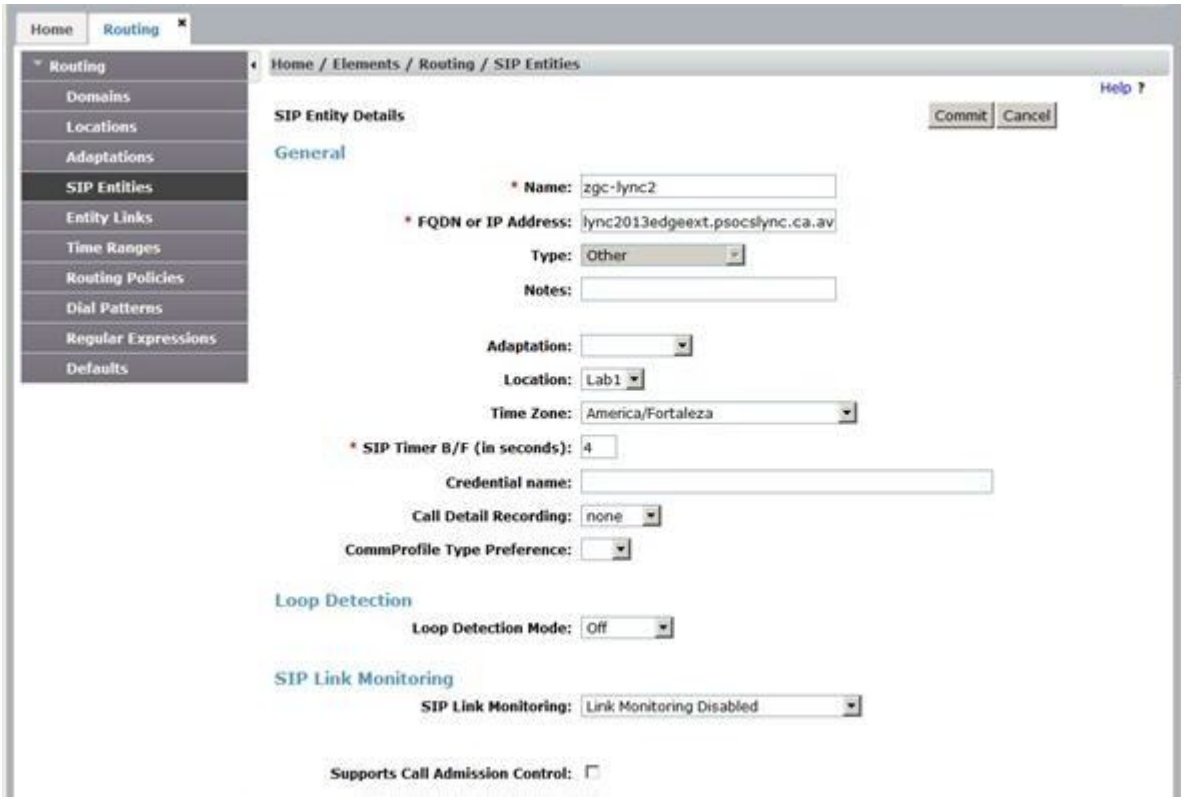
   For example, **lync2013.ca.avaya.com** and the Lync edge external FQDN with the same edge external IP address. Use the 5061 port for TLS transport.
4. Click **Commit** to save the changes.

Adding SIP Entities and Entity link representing Lync edge server

Procedure

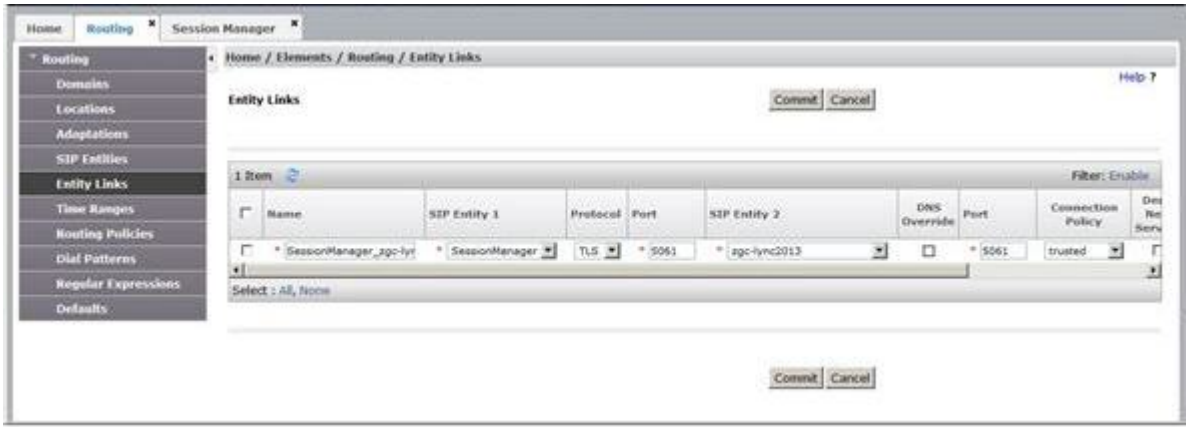
1. Log in to the System Manager web console.
2. Click **Routing** > **SIP Entities** > **New**.
3. Add a new Entity entry for the Lync edge server with the following values:
   - **Name**: Enter a name for the Lync edge server.
   - **FQDN or IP Address**: Enter the Lync edge server external interface FQDN.
   - **Type**: Select **Other**.
   - **SIP Link Monitoring**: Select **Link Monitoring Disabled**.

   Use default values for the other fields.



4. Add 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.

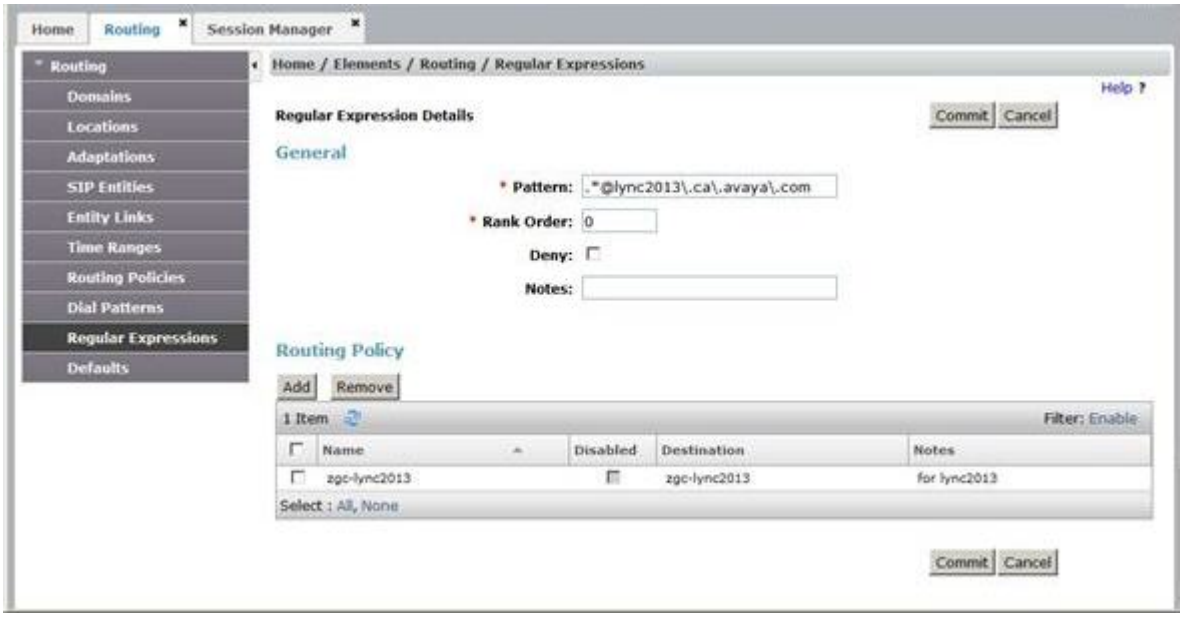
Note:

In multi Session Manager setup, select only one Session Manager for this configuration. The selected Session Manager must be the same as Session Manager specified in "Adding Lync gateway as an IM service provider for Lync" procedure.

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

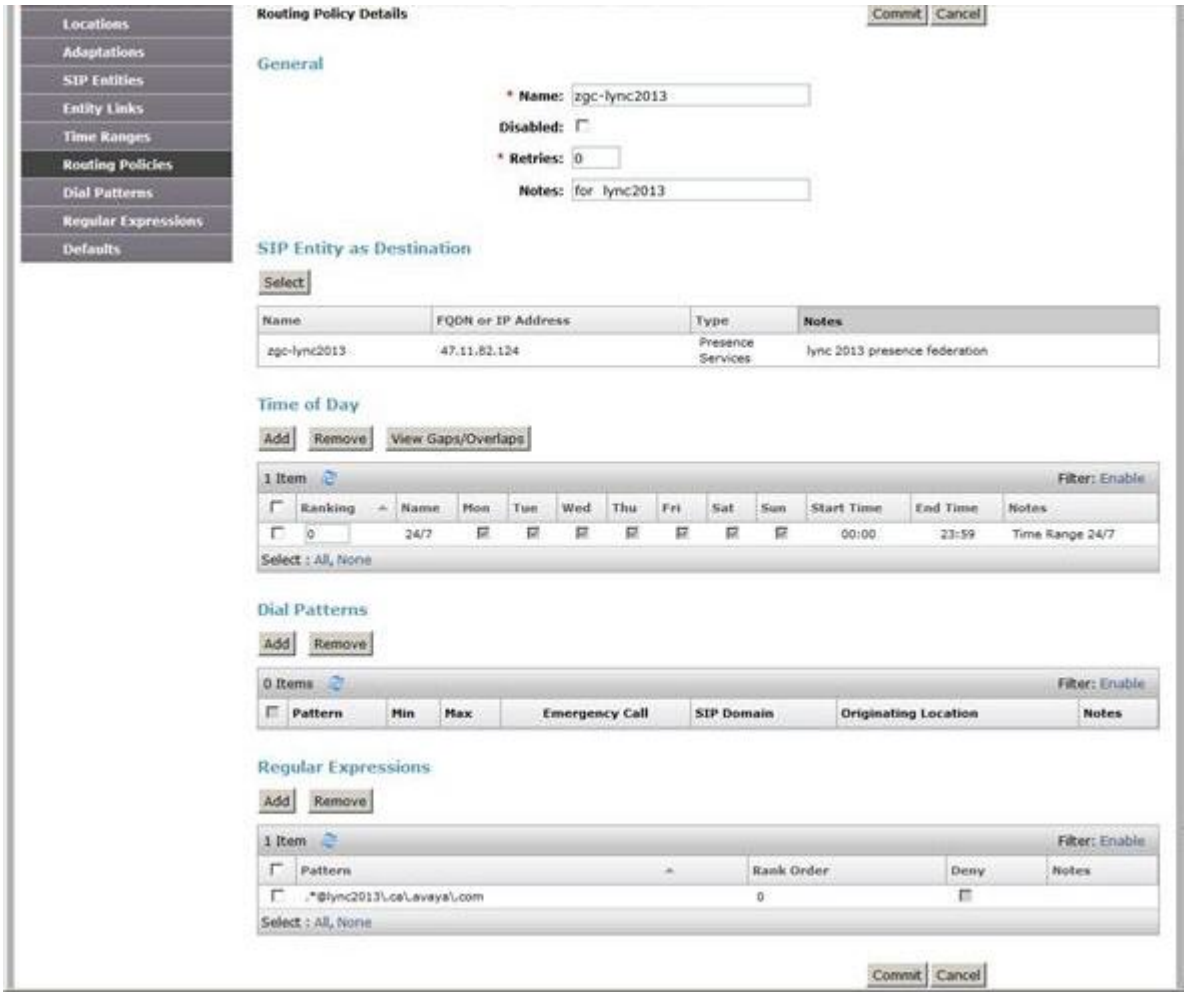
The routing policy must be configured so that the SIP messages are routed to Lync edge server and Presence Services servers.

Create one policy for the Lync edge server and create a policy for each Presence Services server if there are multiple Presence Services servers in the Presence Services 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.
6. Click **Select** to add the expression to the policy.



7. Click **Commit** to save the change.
8. Use the above steps to create the policy for each Presence Services server.

Adding or updating the existing Communication Manager application

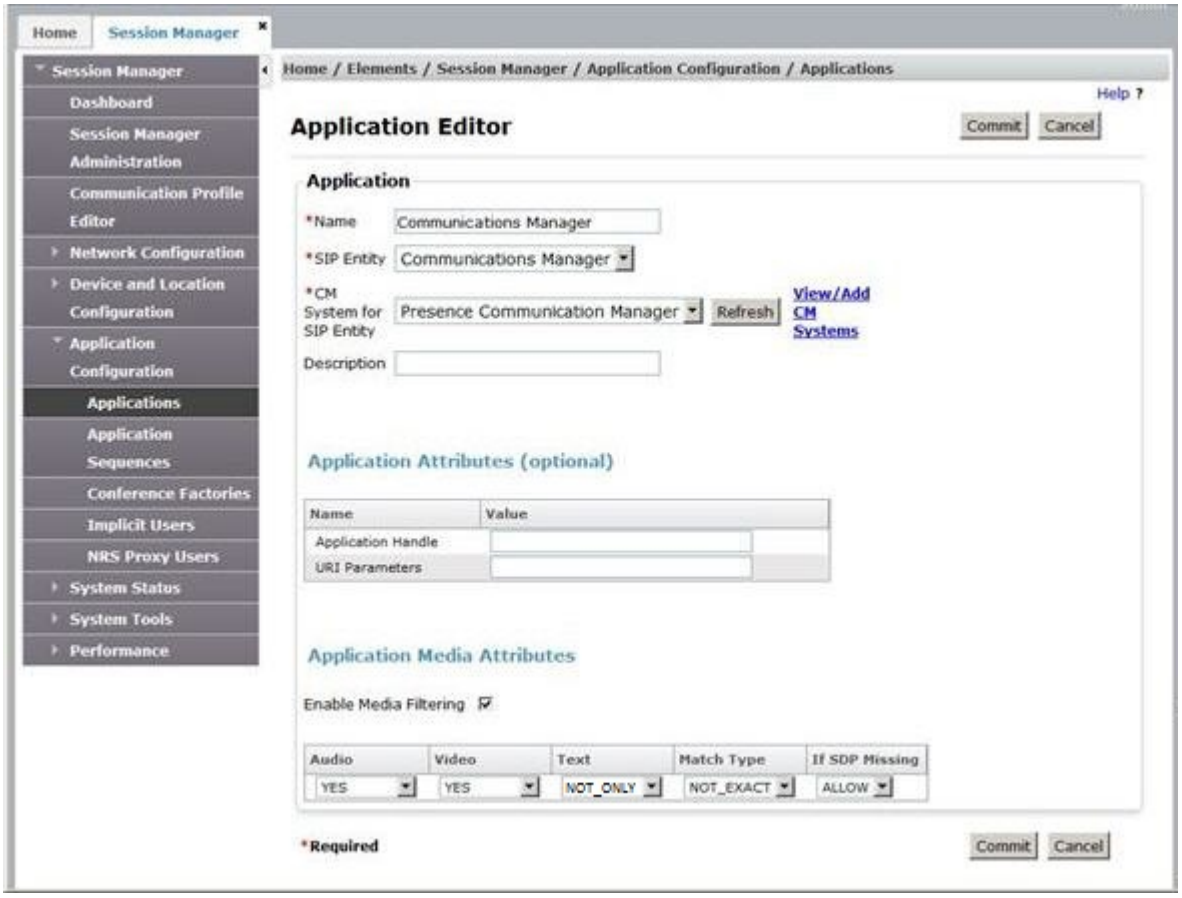
About this task

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

1. 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.

Lync federation with multiple Session Manager deployment

Lync Federation works with one Session Manager at a time. In High Availability (HA) and Geographic Redundant (GR) configurations, a manual step is required to change which Session Manager provides federation functionality to Lync. This manual step is required whenever the configured Session Manager fails.

The manual step is applicable for Lync federation in:

- Multiple Session Managers configuration (HA) with single Avaya Breeze™ cluster environment.
- Geographic Redundancy configuration (GR) with two or more Session Managers environment.

Prerequisites for reconfiguring Session Manager connectivity to Lync federation

- Administer SIP Entity or Entity Links or Managed Elements between Presence Servers and the Session Manager. See *Presence Service multi-server deployment* or *Presence Service geographically redundant deployment*.
- Administer Entity Links between Session Managers. For more information, see *Administering Avaya Aura® Session Manager*.
- Administer each Session Manager. See *Lync federation*.

Checklist for reconfiguring Session Manager Connectivity to Lync interdomain federation

No.	Task	Reference	✔
1	Modify the SIP Entity link representing Lync Edge Server		
2	Modify the Lync Server Public Provider		

Modifying the SIP Entity link representing Lync Edge Server

Procedure

1. On the System Manager web console, click **Elements** > **Routing**.
2. Click **SIP Entities**.
3. Select the **SIP Entity** that representing the connection to Lync Edge Server and click **Edit**.
4. In the **Entity Link** section on **SIP Entity**, select the available Session Manager.
5. Click **Commit**.

Example

Next steps

Modifying the Lync Server Public Provider

Procedure

1. On the **Microsoft Edge Server**, click **Start** > **Administrative Tools** > **Services**.
2. Locate the **Lync Server Access Edge** service.

3. Right-click the **Lync Server Access Edge** service and select **Stop**.
4. On the **Lync Front End Server** click **Start** > **All Programs** > **Microsoft Lync Server 2013** > **Microsoft Lync Server control Panel**.
5. In **Federation** and **External Access**, click **SIP Federation Providers** tab.
6. Select the Public provider that associated with the failed Session Manager.
7. Click **Edit** > **Delete** > **OK**.
8. Click **New** > **Public Provider**.
9. Ensure that you select the **Enable communications with this provider** check box.
10. In **Provider Name**, specify the domain name that the Presence server uses as the Presence/IM domain, this domain name should be the same as the deleted Public Provider.
11. In **Access Edge service (FQDN)** field, specify the replacement Session Manager Server FQDN.
12. In **Default Verification Level**, ensure that you select **Allow users to communicate with every one using this provider**.
13. To save the changes, click **Commit**.
14. On the **Microsoft Edge Server**, Start the **Lync Server Access Edge Service**.

Lync Intradomain federation

Lync Intradomain federation enables presence and IM to be shared between Aura users and Lync users in the same domain. Lync Intradomain federation is not supported for Hybrid users.

Note:

For correct user routing from Session Manager to the Presence Services cluster, all Avaya Presence/IM handles must be lowercase. Using uppercase characters might result in the inability for Session Manager to route presence and/or IM to an Avaya user from the other system, resulting in loss of presence updates or proper exchanging of IM's. Check if there are any Avaya users on System Manager with Avaya Presence/IM handles in uppercase characters and, if so, edit the handle to lowercase characters.

Checklist for configuring Lync Intradomain federation

Table 8: Checklist for configuring Lync Intradomain federation

No.	Task	Link	✔
1	Configure Avaya Multimedia Messaging SIP Proxy.	For more information, see *Deploying Avaya Multimedia Messaging*.	
2	Configure Lync Intradomain federation.	Configuring Lync Intradomain federation on page 104	

Configuring Lync Intradomain federation

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. In the **Lync Federation: Lync Federation Enabled** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type True.
6. In the **Lync Shared Domain List** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the list of shared federated Lync domain names.
7. Click **Commit**.

Checklist for reconfiguring Session Manager Connectivity to Lync intradomain federation

No.	Task	Description	✔
1	Modify the Avaya Multimedia Messaging SIP Adaptor representing Avaya Multimedia Messaging to Session Manager.		
2	Modify the SIP Entity link representing connection to Avaya Multimedia Messaging.		

Modifying the Avaya Multimedia Messaging SIP Adaptor representing Avaya Multimedia Messaging to Session Manager

Procedure

1. Log into Avaya Multimedia Messaging admin console.
2. Click **Server Connections** > **Federation Configuration**.
3. Select the Session Manager **SIP Adaptor**, and click **Edit**.
4. Change to the available Session Manager.

5. Click **Commit**.
6. Click **Confirm** restart service.

Modifying the SIP Entity link representing connection to Avaya Multimedia Messaging

Procedure

1. On the System Manager web console, click **Elements** > **Routing**.
2. Click **SIP Entities**.
3. Select the **SIP Entities** that representing the connection to Avaya Multimedia MessagingServer, and click **Edit**.
4. In the **Entity Link** section on the **SIP Entity**, select the available Session Manager.
5. Click **Commit**.
6. Repeat step 1 to 5 for the Avaya Multimedia Messaging **Relay SIP Entity**.

Inter-PS federation

Inter-PS federation allows exchange of Presence and IM between different Presence Services clusters.

You can configure federation between:

- Two Presence Services clusters on the same System Manager.
- Two Presence Services clusters on different System Managers.

Configuration of federation between two Presence Services clusters on the same System Manager

Presence Services to Presence Services federation between two clusters on the same System Manager works without explicit configuration. The two clusters may also share one or more domains. There are no domain limitations or requirements for federation to work.

To set up Inter-PS federation, you will need:

- Two Presence Services clusters on the same System Manager, that is, two Engagement Development Platform core clusters running Presence Services.
- Presence Communication profile set up correctly for users, that is, Aura presence users must be assigned correctly to the presence clusters. This setting is required for Presence/IM to work.

Assigning Avaya Presence/IM communication address to user on System Manager

About this task

An Avaya Presence/IM communication address is a unique presence identifier for a user. Servers, devices, and other users use this identifier to exchange IM and presence information with the user.

Before you begin

A user must already exist on System Manager at **Users** > **User Management**.

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management**

   The system displays the User Management page.
2. In the navigation pane, click **Manage Users**.
3. Select the user, and click **Edit**.

   The system displays the User Profile Edit page.
4. Click the **Communication Profile** tab.
5. Select the **Communication Profile** with the **Default** check box enabled.
6. In the **Communication Address** section, click **New**.
7. In the **Type** field, select **Avaya Presence/IM**.
8. In the **Fully Qualified Address** section:
   - In the first field, type the user part of the Avaya Presence/IM communication address.
   - In the second field, select the **Presence/IM routing** domain that was defined in “Configuring Presence/IM routing domain on System Manager”.
9. Click **Add**.
10. Click **Commit** to save the changes.

    Note:

    The Avaya Presence/IM communication address must be administered on the default Communication Profile.

Checklist for configuring federation between two Presence Services clusters on different System Managers

To set up Inter-PS federation, you will need:

- Two Presence Services clusters on different System Managers.
- Unique Presence domains for both the clusters.
- Presence Communication profile set up correctly for users, that is, Aura presence users must be assigned correctly to the presence clusters. This setting is required for Presence/IM to work.

Note:

For correct user routing from Session Manager to the Presence Services cluster, all Avaya Presence/IM handles must be lowercase. Using uppercase characters might result in the inability for Session Manager to route presence and/or IM to an Avaya user from the other system, resulting in loss of presence updates or proper exchanging of IM's. Check if there are any Avaya users with Avaya Presence/IM handles in uppercase characters on both System Managers and, if so, edit the handle to lowercase characters.

Table 9: Checklist for configuring federation between two Presence Services clusters on different System Managers

No.	Task	Reference	✔
1	Enable Inter-PS federation for both the Presence Services clusters.	Enabling Inter-PS federation on page 107	
2	Configure the Session Manager routing for both the System Managers.	Configuring the Session Manager routing on page 108	
3	Assign communication profile to users.	Assigning Avaya Presence/IM communication address to user on System Manager on page 105	
4	Downloading certificate from the first System Manager instance.	Downloading certificate from System Manager on page 108	
5	Adding certificate to Session Manager on the second System Manager instance.	Adding certificate to Session Manager on page 108	
6	Downloading certificate from the second System Manager instance.	Downloading certificate from System Manager on page 108	
7	Adding certificate to Session Manager on the first System Manager instance.	Adding certificate to Session Manager on page 108	

Enabling Inter-PS federation

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **Inter-PS Federation** section.
6. In the **Inter-PS Federation Enabled** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `True`.
7. In the **Inter-PS Domain Name List** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the list of federated Presence Services domain names.
8. Click **Commit**.

   Inter-PS federation must be enabled on both clusters for federation to work correctly.

Configuring the Session Manager routing

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing** > **SIP Entities** > **New**.
2. Add a new Entity entry for the Session Manager on the other System Manager with the following values:
   - **Name**: Enter a name for Session Manager.
   - **FQDN or IP Address**: Enter the asset IP address of Session Manager.
   - **Type**: Select **Other**.
3. Click **Commit**.
4. Click **Routing** > **Routing Policies** > **New**.
5. Create a routing policy with the following values:
   - **Name**: Enter a name for the routing policy.
   - **Retries**: Enter the number of retries.
   - **SIP Entity as Destination**: Select the SIP Entity created in Step 2.
6. Click **Commit**.
7. Click **Routing** > **Regular Expressions** > **New**.
8. Create regular expression with the following values:
   - **Pattern**: Add a pattern matching all users in the remote domain.

     For example, `.*@alpha\.ps\.avaya\.com`.
   - **Routing Policy**: Select the routing policy created in Step 5.
9. Click **Commit**.

   This procedure needs to be done on the other System Manager as well.

Downloading certificate from System Manager

Procedure

1. On the System Manager web console, navigate to **Services** > **Security**.
2. Click **Certificates** > **Authority**.
3. On the CA Functions page, click **Download PEM file**.
4. Save the downloaded file.

Adding certificate to Session Manager

Before you begin

Download the certificate from System Manager.

Procedure

1. Navigate to **Services** > **Inventory** > **Manage Elements**.

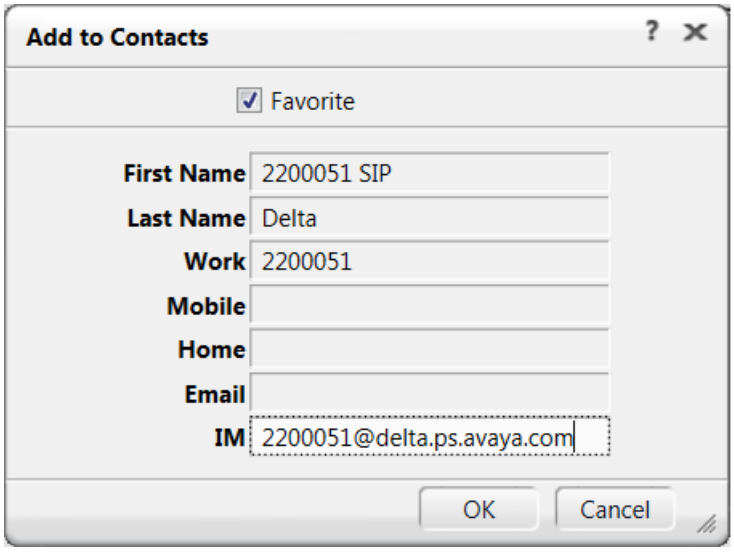
2. Select the Session Manager instance and click **More Actions** > **Configure Trusted Certificates**.
3. Click **Add**.
4. Select **Import from file** and import the PEM file downloaded in “Downloading certificate from System Manager”.
5. Click **Retrieve Certificate**.
6. Click **Commit**.

User or contact management from an Aura client

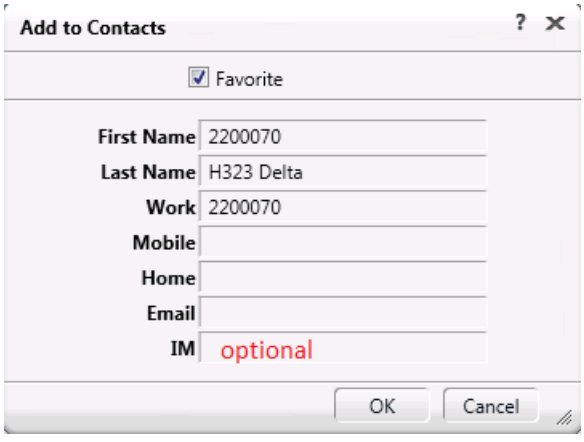
Presence Services clusters on the same System Manager

A federated contact is added like any other Aura contact. The watcher is unaware of the fact that the presentity is external from presence perspective.

H323 watcher of a federated presentity:



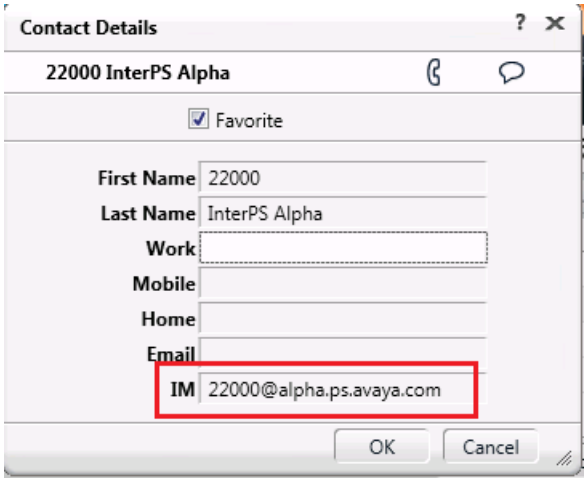
SIP watcher of a federated presentity:



Presence Services clusters on different System Managers

A federated contact is added like an external contact.

H323 or SIP watcher of a federated presentity:



Note:

In a multi Session Manager deployment, that is a System Manager having multiple Session Managers, configure SIP Entity Links among Session Managers so that all Session Managers can communicate. This requirement is mandatory if InterPS federation is enabled.

XMPP federation

Presence Services Release 7.0 and later uses XMPP to federate with the following types of remote deployments:

- Presence Services prior to Release 7.0
- Cisco Jabber
- Ignite Realtime Openfire

Ignite Realtime Openfire and Cisco Jabber only support a single local presence/IM domain and support federation on a single-server deployment.

Presence Services supports multiple local presence/IM domains and supports federation on a single-server or a multi-server cluster.

Federation between two deployments of Presence Services Release 7.0 or later is supported using SIP. For more information, see “Inter-PS federation”.

Key customer configuration information

Obtain the following information, and record it in the **Customer value** column of the table, before performing the tasks in the checklist. The task descriptions include screenshots using the values in

the **Sample value** column of “Table 7: Single-server Cluster Federated with Ignite Openfire example values”. The **Sample value** column is based on the following example:

- Presence Services Release 7.0 is deployed on a single-server cluster with two local presence/IM domains.
- Federated with Ignite Realtime Openfire in a single-server deployment with a single presence/IM domain.

Table 10: Single-server Cluster Federated with Ignite Openfire example values

No.	Requirement	Customer value	Sample value
1	Avaya Breeze™ Security Module IP addresses		`10.136.1.92`
2	Local Presence/IM domains		`presenceservices1.ps.avaya.com` `presenceservices2.ps.avaya.com`
3	S2S Port number		`5269`
4	Remote Presence/IM domains		`of.avaya.com`
5	Remote server IP addresses		`135.55.68.86`
6	Remote type		`Openfire`

Checklist for configuring XMPP federation

In the following checklists:

- *m* refers to the number of servers in the local Presence Services cluster.
- *n* refers to the number of local Presence/IM domains supported on the Presence Services cluster.
- *o* refers to the number of servers in the remote deployment.
- *p* refers to the number of remote Presence/IM domains.

Table 11: Checklist for configuring XMPP federation using TCP

No.	Task	Reference	✔
1	Administer *m* * *n* DNS SRV records to resolve `_xmpp-server` to Avaya Breeze™ Security Module IP address and S2S Port for local Presence/IM domain.	Administering DNS SRV records for local Presence Services domains on page 118	
2	Administer *o* * *p* DNS SRV records to resolve _xmpp-server to remote server IP address and S2S Port for remote Presence/IM domain.	Administering DNS SRV records for remote domains on page 119	

Table continues…

No.	Task	Reference	✔
3	Administer XMPP federation in unsecure mode (TCP).	Administering XMPP federation in unsecure mode (TCP) on page 116	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 114	
5	Administer Security Settings (TCP) in Openfire.	Administering Security Settings (TCP) on Openfire on page 114	
6	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 120	

Table 12: Checklist for configuring XMPP federation using TLS with self-signed

No.	Task	Reference	✔
1	Administer *m* * *n* DNS SRV records to resolve `_xmpp-server` to Avaya Breeze™ Security Module IP address and S2S Port for local Presence/IM domain.	Administering DNS SRV records for local Presence Services domains on page 118	
2	Administer *o* * *p* DNS SRV records to resolve _xmpp-server to remote server IP address and S2S Port for remote Presence/IM domain.	Administering DNS SRV records for remote domains on page 119	
3	Administer XMPP federation in secure mode (TLS).	Administering XMPP federation in secure mode (TLS) on page 117	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 114	
5	Administer Security Settings TLS on Openfire.	Administering Security Settings TLS on Openfire on page 114	
6	Administer Disable Certificate Verification in Openfire.	Administering Disable Certificate Verification on Openfire on page 115	
7	Export Openfire Certificate on Linux.	Exporting Openfire Certificate (Linux) on page 167	
8	Export Openfire Certificate on Windows.	Exporting Openfire Certificate (Windows) on page 168	
9	Import Certificate into Cluster Truststore.	Importing certificate into Cluster Truststore on page 168	
10	Import System Manager root CA certificate into Openfire Truststore on Windows.	Importing System Manager root CA certificate into Openfire Truststore (Windows) on page 169	

Table continues…

No.	Task	Reference	✔
11	Import System Manager root CA certificate into Openfire Truststore on Linux.	Importing System Manager root CA certificate into Openfire Truststore (Linux) on page 170	
12	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 120	

Table 13: Checklist for configuring XMPP federation using TLS with System Manager CA signed

No.	Task	Reference	✔
1	Administer *m* * *n* DNS SRV records to resolve `_xmpp-server` to Avaya Breeze™ Security Module IP address and S2S Port for local Presence/IM domain.	Administering DNS SRV records for local Presence Services domains on page 118	
2	Administer *o* * *p* DNS SRV records to resolve _xmpp-server to remote server IP address and S2S Port for remote Presence/IM domain.	Administering DNS SRV records for remote domains on page 119	
3	Administer XMPP federation in secure mode (TLS).	Administering XMPP federation in secure mode (TLS) on page 117	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 114	
5	Administering Security Settings TLS on Openfire.	Administering Security Settings TLS on Openfire on page 114	
6	Administer Disable Certificate Verification in Openfire.	Administering Disable Certificate Verification on Openfire on page 115	
7	Create Entity Profile on System Manager.	Creating Entity Profile on System Manager on page 171	
8	Generate a Certificate Signing Request (CSR) on Openfire.	Generating a certificate signing request on the Openfire server on page 172	
9	Sign the Openfire CSR on System Manager.	Signing the Openfire certificate signing request (CSR) on System Manager on page 172	
10	Install the System Manager CA and Signed Openfire Certificate on Openfire.	Installing the System Manager CA and Signed Openfire Certificate on Openfire on page 173	
11	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 120	

Administering Server to Server Settings on Openfire

About this task

This procedure uses the samples values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. On the Openfire server, navigate to **Server** > **Server Settings** > **Server to Server Settings**.
2. In **Service Enabled**, select **Enabled - Remote servers can exchange packets with this server on port 5269**.
3. Assign a port number.

   For example, `5269`.
4. Click **Save Settings**.
5. In **Idle Connections Settings**, select the **Never close idle connections** check box.

   This step is recommended.
6. Click **Save Settings**.
7. In **Allowed to Connect**, select the **Anyone - Any remote server is allowed to connect to this server. Use the table below to override the default settings** check box.

   This step is recommended.
8. Click **Save Settings**.

Administering Security Settings (TCP) on Openfire

Procedure

1. On the Openfire server, navigate to **Server** > **Server Settings** > **Security Settings**.
2. In **Server Connection Security**, configure the Openfire server to use TCP:
   a. In the **TCP** section, select the **Custom** check box.
   b. In the **Server Dialback** field, select **Available**.
   c. In the **TLS method** field, select **Not Available**.

   The **Accept self-signed certificates. Server dialback over TLS is now available** check box is not relevant when TCP is used.
3. Click **Save Settings**.

Administering Security Settings TLS on Openfire

Procedure

1. On the Openfire server, navigate to **Server** > **Server Settings** > **Security Settings**.
2. In **Server Connection Security**, configure the Openfire server to use TLS:
   a. Select **Required - Connections between servers always use secured connections**.

b. Select the **Accept self-signed certificates. Server dialback over TLS is now available** check box.

3. Click **Save Settings**.

Administering Disable Certificate Verification on Openfire

About this task

This procedure is required if the Presence Services certificate does not contain a subject alternative name (SAN) of the **OtherName** type and with an **XMPPaddr** identifier.

Procedure

1. On the Openfire server, navigate to **Server** > **Server Manager** > **System Properties** > **Add new property**.
2. In the **Property Name** field, add `xmpp.server.certificate.verify`.
3. In the **Property Value** field, add `false`.
4. Click **Save Property**.
5. Verify that the **xmpp.server.certificate.verify** entry appears in the list as `false`.
6. In the **Property Name** field, add `xmpp.server.certificate.verify.chain`,
7. In the **Property Value** field, add `false`.
8. Click **Save Property**.
9. Verify that the **xmpp.server.certificate.verify.chain** entry appears in the list as `false`.

Administering Enable Certificate Verification on Openfire

About this task

This procedure is required if the Presence Services certificate contains a subject alternative name (SAN) of the **OtherName** type and with an **XMPPaddr** identifier.

Procedure

1. On the Openfire server, navigate to **Server** > **Server Manager** > **System Properties** > **Add new property**.
2. In the **Property Name** field, add `xmpp.server.certificate.verify`.
3. In the **Property Value** field, add `true`.
4. Click **Save Property**.
5. Verify that the **xmpp.server.certificate.verify** entry appears in the list as `true`.
6. In the **Property Name** field, add `xmpp.server.certificate.verify.chain`,
7. In the **Property Value** field, add `true`.
8. Click **Save Property**.
9. Verify that the **xmpp.server.certificate.verify.chain** entry appears in the list as `true`.

Administering XMPP federation in unsecure mode (TCP)

About this task

To federate Presence Services with another XMPP server, an instance of an XMPP Federation *x* service attribute group must be administered, where *x* is a value from 1 to 4. In some conditions, one instance can be shared for more than one federated server. For more information about the XMPP attributes, see “Service Attributes”.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section. *x* refers to a value from 1 to 4.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Globals** or the **Service Clusters** tab.
3. Navigate to the **Component Enabled *x*** field within the XMPP Federation *x* group.
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `True`.

      XMPP Federation is disabled by default.
4. To disable the secure mode, change the value of the **Enable Secure Communications (TLS) *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `False`.

      Secure mode (TLS) is enabled by default.
5. To change the value of the **Federation Type *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type:
      - `Openfire` to federate with an Ignite Realtime Openfire server.
      - `Avaya` to federate with a pre-7.0 Presence Services server.
      - `Cisco` to federate with a Cisco Jabber server.

      `Openfire` is the default federation type.
6. Add the federated domain to the **XMPP Federation Domain List *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter one or more federated domains.

      In this example, type `of.avaya.com`.
7. Click **Commit**.

Administering XMPP federation in secure mode (TLS)

About this task

To federate Presence Services with another XMPP server, an instance of an XMPP Federation *x* service attribute group must be administered, where *x* is a value from 1 to 4. In some conditions, one instance can be shared for more than one federated server. For more information about the XMPP attributes, see “Service Attributes”.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section. *x* refers to a value from 1 to 4.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. Click the **Service Globals** or the **Service Clusters** tab.
3. Navigate to the **Component Enabled *x*** field within the XMPP Federation *x* group.
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `True`.

      XMPP Federation is disabled by default.
4. To disable the secure mode, change the value of the **Enable Secure Communications (TLS) *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `True`.

      Secure mode (TLS) is enabled by default.
5. To change the value of the **Federation Type *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type:
      - `Openfire` to federate with an Ignite Realtime Openfire server.
      - `Avaya` to federate with a pre-7.0 Presence Services server.
      - `Cisco` to federate with a Cisco Jabber server.

      `Openfire` is the default federation type.
6. Add the federated domain to the **XMPP Federation Domain List *x*** field within the XMPP Federation *x* group:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter one or more federated domains.

      In this example, type `of.avaya.com`.
7. Click **Commit**.

Administering DNS SRV records for local Presence Services domains

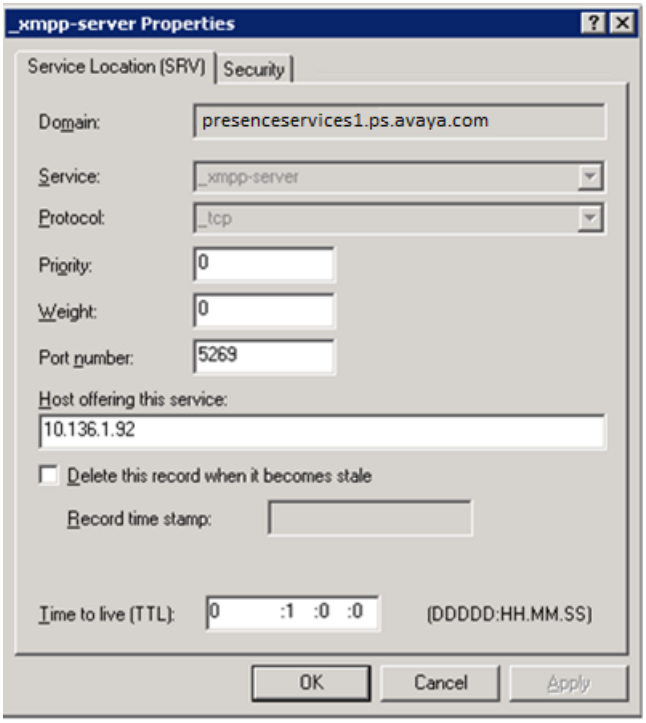
About this task

Use this procedure to administer *m* * *n* DNS SRV records to resolve xmpp-service to Engagement Development Platform Security Module IP address and S2S port for Presence Services Presence/IM domain. *m* refers to the number of servers in the Presence Services cluster. *n* refers to the number of local Presence/IM domains supported on the Presence Services cluster.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

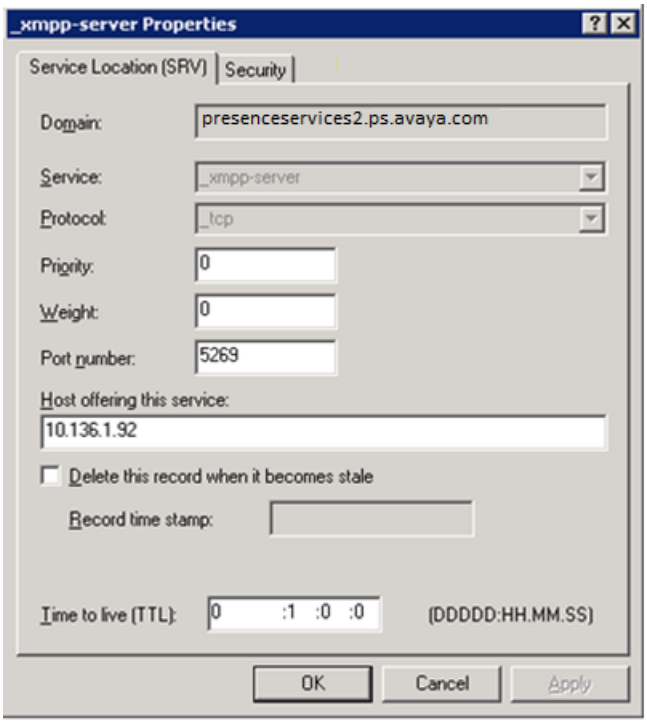
Procedure

1. On Domain Name Server used by the federated server, create an SRV record with the following values:
   - **Domain**: `presenceservices1.ps.avaya.com`
   - **Service**: `_xmpp-server`
   - **Protocol**: `_tcp`
   - **Port number**: `5269`
   - **Host offering this service**: `10.136.1.92`



2. On Domain Name Server used by the federated server, create an SRV record with the following values:
   - **Domain**: `presenceservices2.ps.avaya.com`
   - **Service**: `_xmpp-server`

- **Protocol**: `_tcp`
- **Port number**: `5269`
- **Host offering this service**: `10.136.1.92`



Administering DNS SRV records for remote domains

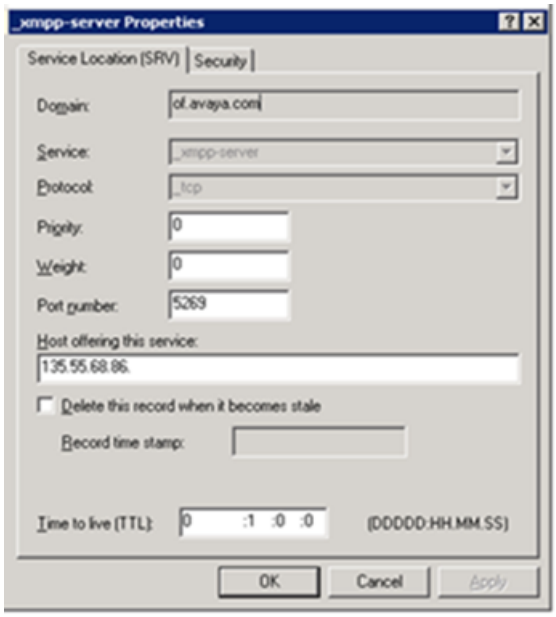
About this task

Use this procedure to administer *o* * *p* DNS SRV records to resolve xmpp-service to remote IP address and S2S port for remote Presence/IM domain. *o* refers to the number of servers in the remote deployment. *p* refers to the number of remote Presence/IM domains. This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

On Domain Name Server used by the Presence Services cluster, create an SRV record with the following values:

- **Domain**: `of.avaya.com`
- **Service**: `_xmpp-server`
- **Protocol**: `_tcp`
- **Port number**: `5269`
- **Host offering this service**: `135.55.68.86`



Verifying DNS resolution and server reachability

About this task

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. Open an SSH session to the Avaya Breeze™ Management IP address.
2. Run the `nslookup` command to verify that the xmpp-service resolves to the Openfire server IP address and S2S port for the Openfire XMPP domain.

```
                ~]$ nslookup -querytype=SRV _xmpp-server._tcp.of.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_xmpp-server._tcp.of.avaya.com  service = 0 0 5269 135.55.68.86.
```

3. Run the `ping` command to verify that the Openfire server is reachable.

```
                ~]$ ping 135.55.68.86
PING 135.55.68.86 (135.55.68.86) 56(84) bytes of data.
64 bytes from 135.55.68.86: icmp_seq=1 ttl=125 time=0.579 ms
64 bytes from 135.55.68.86: icmp_seq=2 ttl=125 time=0.961 ms
64 bytes from 135.55.68.86: icmp_seq=3 ttl=125 time=0.785 ms
64 bytes from 135.55.68.86: icmp_seq=4 ttl=125 time=0.854 ms
^C
--- 135.55.68.86 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3533ms
rtt min/avg/max/mdev = 0.579/0.794/0.961/0.143 ms
```

4. Access a command line interface on the Openfire server:
   - If Openfire has been installed on a Linux/Unix server, open an SSH session to the Openfire server IP address.
   - If Openfire has been installed on a Windows server, login to the server, and open a command line interface.
5. Run the `nslookup` command to verify that the xmpp-service resolves to the Engagement Development Platform Security Module IP address and S2S port for Presence Services Presence/IM domains.

```
                ~]# nslookup -querytype=SRV _xmpp-server._tcp.presenceservices1.ps.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_xmpp-server._tcp.presenceservices1.ps.avaya.com  service = 0 0 5269 10.136.1.92.

                ~]# nslookup -querytype=SRV _xmpp-server._tcp.presenceservices2.ps.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_xmpp-server._tcp.presenceservices2.ps.avaya.com  service = 0 0 5269 10.136.1.92.
```

6. Run the `ping` command to verify that the Presence Services servers are reachable.

```
                ~]# ping 10.136.1.92
PING 10.136.1.92 (10.136.1.92) 56(84) bytes of data.
64 bytes from 10.136.1.92: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 10.136.1.92: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 10.136.1.92: icmp_seq=3 ttl=64 time=0.045 ms
64 bytes from 10.136.1.92: icmp_seq=4 ttl=64 time=0.044 ms
64 bytes from 10.136.1.92: icmp_seq=5 ttl=64 time=0.042 ms
64 bytes from 10.136.1.92: icmp_seq=6 ttl=64 time=0.047 ms
^C
--- 10.136.1.92 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5309ms
rtt min/avg/max/mdev = 0.042/0.046/0.055/0.008 ms
```

Checklist for enabling certificate validation on Openfire when using TLS with CA signed

Table 14: Checklist for enabling certificate validation on Openfire when using TLS with CA signed

No.	Task	Reference	✔
1	Add Subject Alternative Name (SAN) DNS Name and Other Name (XMPP Address) to WebSphere Identify Certificate.	Add Subject Alternative Name DNS name and Other Name (XMPP Address) to WebSphere Identify Certificate on page 167	
2	Enable Certificate Verification on the Openfire server.	Administering Enable Certificate Verification on Openfire on page 115	

Checklist for configuring XMPP federation in a Geographic Redundant deployment

If federation with an external XMPP server is desired in a Geographic Redundant deployment, XMPP federation must be configured on both Presence Services clusters. The external server may reside inside any of the two data centers, or may be external to both of them. In these deployments, the Avaya Breeze™ servers of both the data centers send messages to the external server. However, for a given domain, the external server sends messages to only a single node of one of the data centers.

In the following checklist:

- DC-1 refers to data center 1.
- DC-2 refers to data center 2.
- *m* refers to the number of servers in the each Presence Services clusters.
- *n* refers to the number of local Presence/IM domains supported on the Presence Services clusters.
- *o* refers to the number of external servers in the remote deployment.
- *p* refers to the number of remote Presence/IM domains.

No.	Task	Reference	✔
1	Administer XMPP federation on DC-1.	Checklist for configuring XMPP federation on page 111	
2	Administer XMPP federation on DC-2.	Checklist for configuring XMPP federation on page 111	
3	Administer DNS on external XMPP server.	Administration of DNS on external XMPP server for a Geographic Redundant deployment on page 123	

Table continues…

No.	Task	Reference	✔
4	Administer additional *m*n* DNS SRV records on the primary DNS server of external XMPP server to resolve _xmpp-server to Avaya Breeze™ Security Module IP address and S2S Port for local Presence/IM domain.	Administration of DNS on external XMPP server for a Geographic Redundant deployment on page 123	
5	If a secondary DNS server is configured for external XMPP server, then administer additional *m*n* DNS SRV records on the secondary DNS server to resolve _xmpp-server to Avaya Breeze™ Security Module IP address and S2S Port for local Presence/IM domain.	Administration of DNS on external XMPP server for a Geographic Redundant deployment on page 123	

Administration of DNS on external XMPP server for a Geographic Redundant deployment

The procedure to configure primary and secondary DNS server may vary depending on the host operating system of the external XMPP server.

If the external XMPP server resides in one of the data centers:

- The XMPP server must be configured with two DNS servers.

  The DNS local to the data center should be configured as primary DNS and the DNS of the other data center should be configured as secondary or alternate DNS sever.

If the external XMPP server is deployed outside both data centers, then select one of the following as applicable to the network deployment:

- The XMPP server must be configured with a DNS external to both data centers.
- The XMPP server must be configured with DNS from one of the data center as primary and the DNS from other data center as secondary.

Administration of DNS SRV records for local Presence Services domains in Geographic Redundant deployment

In a Geographic Redundant deployment the external server must be able to discover Presence Services in both data centers. During normal operations, for a given domain, the external server talks to a single node of one of the data centers (typically local data center). However, in the event of data center failure, it must be able communicate with one of the nodes in the other data center. To accomplish this, it is required to administer additional m * n DNS SRV records with lower priority to resolve _xmpp-server to the Avaya Breeze™ Security Module IP address of other data center.

Please refer to Administering DNS SRV records for local Presence Services domains for general details on configuring such DNS SRV records.

Note:

The priority of SRV records must be assigned carefully. Smaller number in the priority field indicates higher priority of the record whereas bigger number in the priority field indicates lower priority of the record. Ensure that the priorities are assigned in such a way that the SRV records with IP addresses in the local data center of the DNS server takes precedence over the remote IP addresses.

Note:

If the deployment has multiple local Presence / IM domains, then it is recommended to load balance the traffic among various Avaya Breeze™ servers based on the domains.

Example

- There are two data centers (Presence Services Avaya Breeze™ clusters) in New York & Hong Kong.
- Each cluster has two Avaya Breeze™ Servers.
- Security module IP address of server in New York are `10.136.1.11` and `10.136.1.21`.
- Security module IP address of server in Hong Kong are `10.136.2.31` and `10.136.2.41`.
- Local presence domain are `presenceservices1.ps.avaya.com` and `presenceservices2.ps.avaya.com`.

Then, create four SRV records on New York DNS and another four SRV records on Hong Kong DNS, as shown in the table below.

Table 15: SRV records on New York DNS

Domain	Service	Protocol	Priority	Weight	Port	Host
presenceservices1.ps.avaya.com	_xmpp-server	_tcp	0	0	5269	10.136.1.11
presenceservices2.ps.avaya.com	_xmpp-server	_tcp	0	0	5269	10.136.1.21
presenceservices1.ps.avaya.com	_xmpp-server	_tcp	1	0	5269	10.136.2.31
presenceservices2.ps.avaya.com	_xmpp-server	_tcp	1	0	5269	10.136.2.41

Table 16: SRV records on Hong Kong DNS

Domain	Service	Protocol	Priority	Weight	Port	Host
presenceservices1.ps.avaya.com	_xmpp-server	_tcp	0	0	5269	10.136.2.31
presenceservices2.ps.avaya.com	_xmpp-server	_tcp	0	0	5269	10.136.2.41

Table continues…

Domain	Service	Protocol	Priority	Weight	Port	Host
presenceservices1.ps.avaya.com	_xmpp-server	_tcp	1	0	5269	10.136.1.11
presenceservices2.ps.avaya.com	_xmpp-server	_tcp	1	0	5269	10.136.1.21

XMPP Federation with Cisco Jabber

Federation with Cisco Jabber

Presence Services allows multiple Avaya Aura® domains in one Presence Services cluster or single Presence Services server to be federated with one Cisco domain per Cisco Jabber server. To federate with multiple Cisco domains, multiple XMPP server to server interfaces must be deployed on Presence Services with each only serving one Cisco Jabber domain.

Presence Services and Cisco Jabber server replies on resolving DNS SRV record to get remote server address and port.

Presence Services supports:

- Both TCP and TLS for server to server connection. The default is TLS.
- Both CA-signed and self-signed certificates.

Checklist for configuring XMPP federation with Cisco Jabber

Table 17: Checklist for configuring XMPP federation with Cisco Jabber

No.	Task	Reference	✔
1	Configure DNS SRV records.	Setting up DNS on page 126	
2	Configure Presence Services to enable federation. Presence Services support dynamic configuration change except port number.	Configuring Presence Services on page 126	
3	Configure Cisco Jabber to enable federation from Cisco Jabber console. Cisco Jabber does not support dynamic change. Restart Connection Manager required.	Configuring Cisco Jabber on page 127	
4	If using TLS. import Cisco certificate to presence server and import System Manager certificate to Cisco Jabber.	Cisco Jabber certificates on page 128	

Setting up DNS

Before you begin

Use this procedure to create DNS SRV record. This procedure is common for all XMPP federations.

Procedure

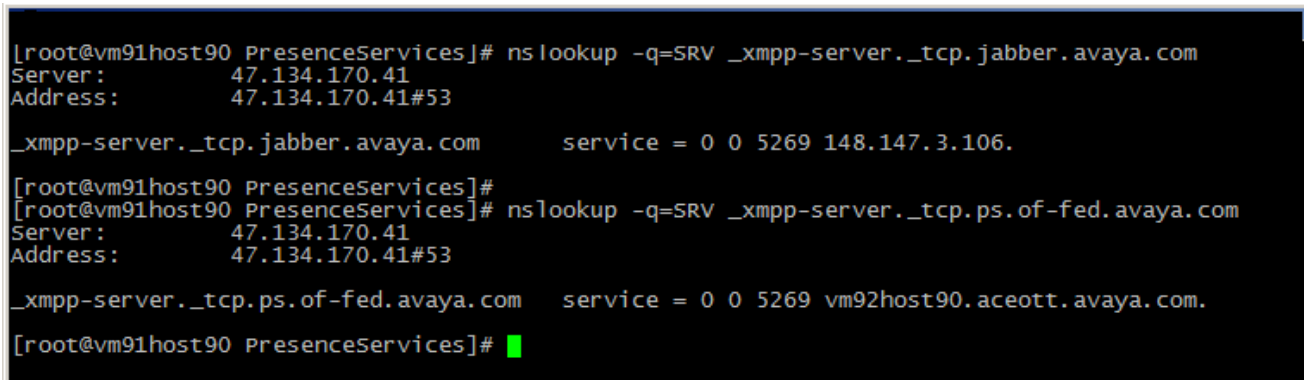
To verify SRV records run following commands.

- `nslookup -querytype=SRV _xmpp-server._tcp.<cisco jabber presence domain>`
- `nslookup -querytype=SRV _xmpp-server._tcp.<presence services domain>`

Example

- `nslookup -querytype=SRV _xmpp-server._tcp.jabber.avaya.com`
- `nslookup -querytype=SRV _xmpp-server._tcp.pres.fed.avaya.com`

If the resolved SRV record is a domain, the domain must be resolvable. For example, `vm92host90.aceott.avaya.com` must resolve to `135.20.245.92`.



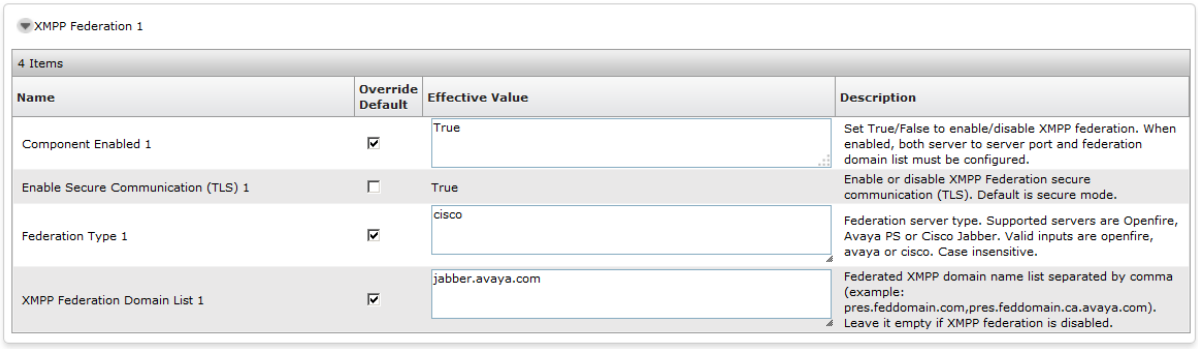
Configuring Presence Services

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™**.
2. Click **Configuration Attributes**.
3. Click the **Service Clusters** tab.
4. Select the cluster and the Presence Services service.
5. Navigate to the **XMPP Federation #** group.
6. In the **Component Enabled #** check box, enter `True`.
7. In the **Enable Secure Communication (TLS) #** check box:
   - Enter `False` for TCP.
   - Leave the default value or enter `True` for TLS.
8. In the **Federation Type #** field:
   a. Select the **Override Default** check box.

b. In the **Effective Value** field, enter `cisco`.

9. In the **XMPP Federation Domain List #** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter a list of federated domains separated by comma.

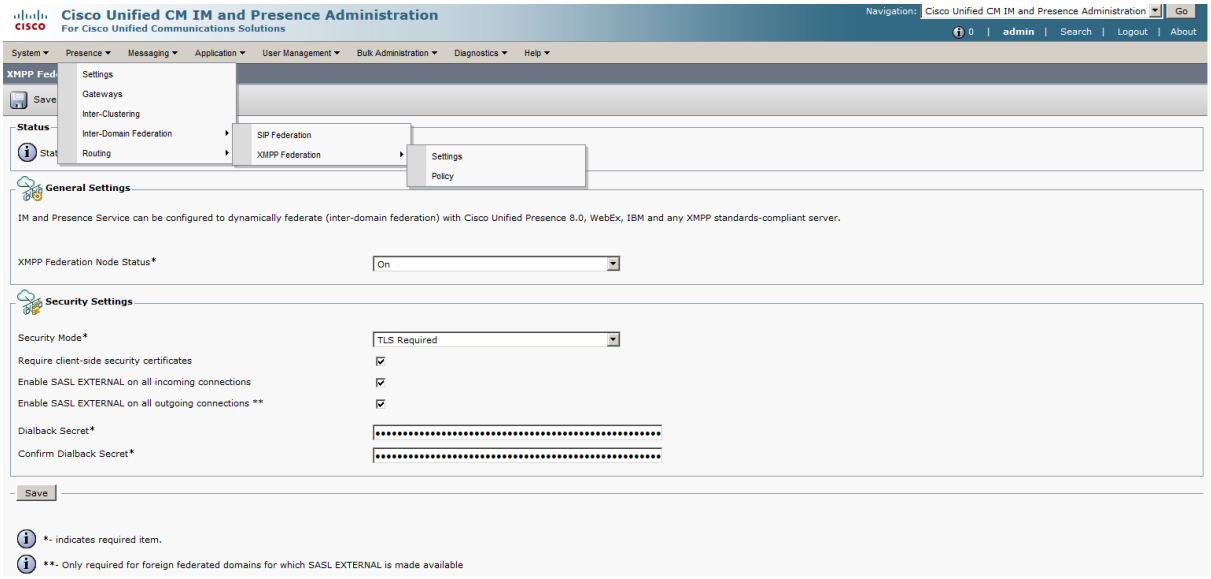


Configuring Cisco Jabber

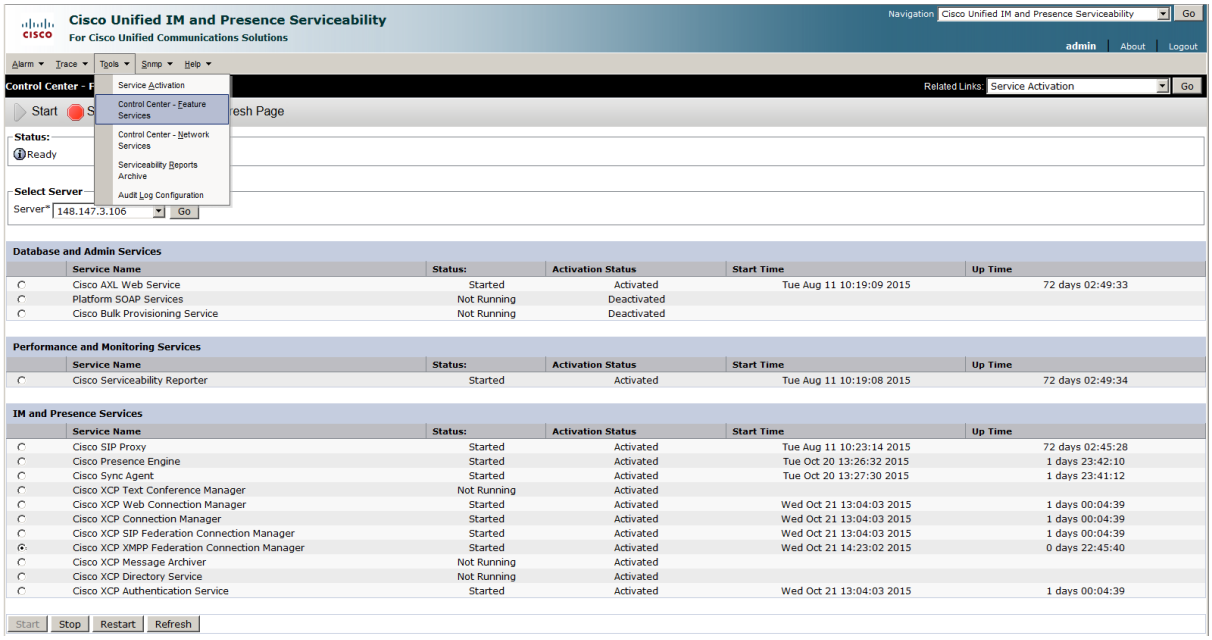
Procedure

1. Log on to Cisco Unified CM IM and Presence Administration.
2. Click **Presence** > **Inter-Domain Federation** > **XMPP Federation** > **Settings**.
3. In **General Settings** section, ensure that the **XMPP Federation Node Status** field shows **ON**.
4. In the **Security Settings** section, make the following changes depending on whether TLS or TCP is used:

Field name	TCP	TLS
Security Mode	`No TLS`	`TLS Required`
Require Client-side security certificate	`check`	`check`
Enable SASL EXTERNAL on all incoming connections	`check`	`check`
Enable SASL EXTERNAL on all outgoing connections	`check`	`check`
Dialback Secret	`secret`	`not used`
Confirm Dialback Secret	`secret`	`not used`



5. Restart Cisco XCP XMPP Federation Connection Manager for the changes to take effect.



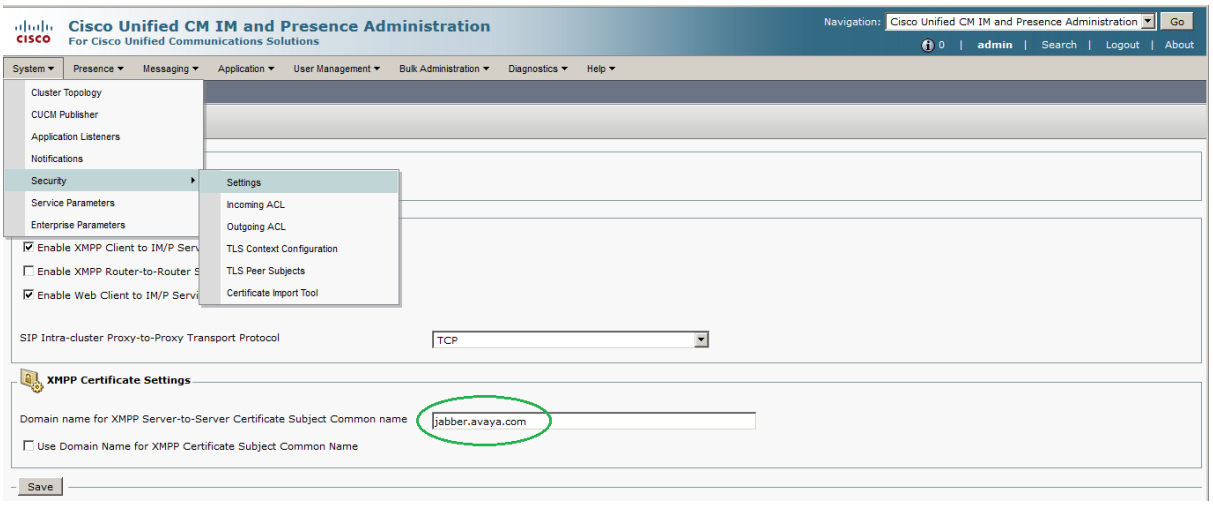
Cisco Jabber cerificates

Generating the self-signed certificate

Procedure

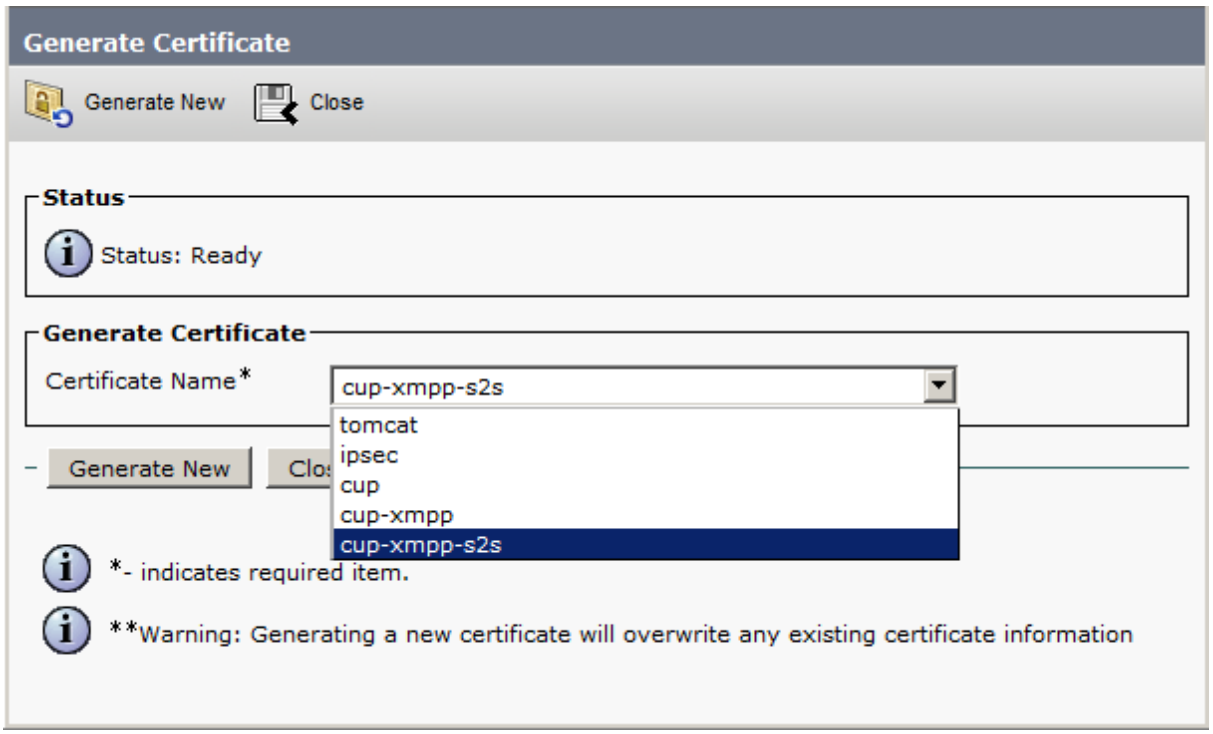
1. Log on to Cisco Unified CM IM and Presence Administration.
2. Click **System** > **Security** > **Settings**.
3. In the **XMPP Certificate Settings** section, in the **Domain name for XMPP Server-to-Server Certificate Subject Common name** name, enter presence domain for certificate.

4. Click **Save**.



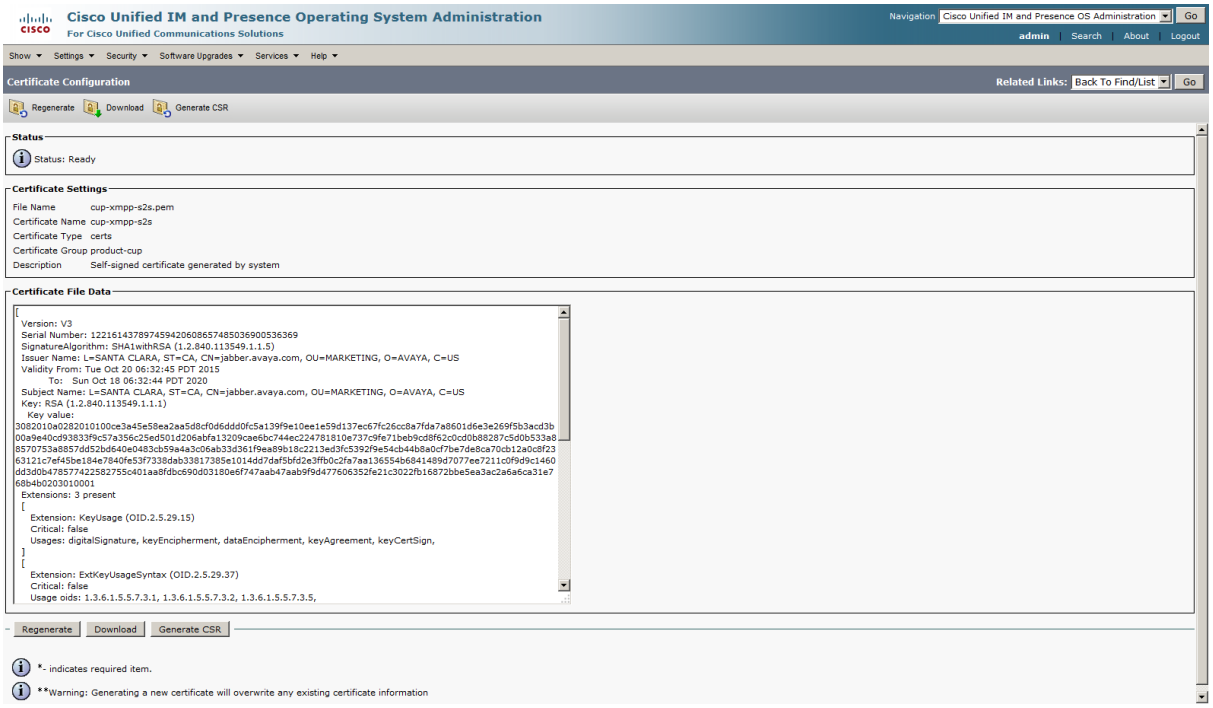
5. Click **Security** > **Certificate Management**.
6. Click **Generate New**.

   The system opens a new window.
7. In the **Certificate Name** field, select **cup-xmpp-s2s**.
8. Click **Generate New**.



The self-signed certificate is generated.

9. Find all certificates from **Certificate List**.
10. List all by using **not empty** search criteria.
11. Click **cup-xmpp-s2s.pem** to open the certificate.



12. Click **Download**.

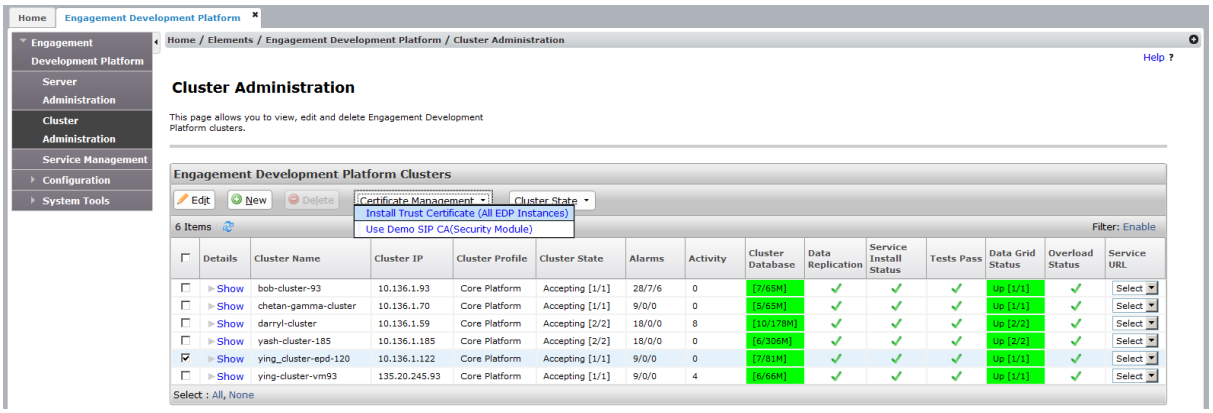
Certificate Name	Certificate Type	.PEM File	.DER File	Description
tomcat	certs	tomcat.pem	tomcat.der	Self-signed certificate generated by system
ipsec	certs	ipsec.pem	ipsec.der	Self-signed certificate generated by system
tomcat-trust	trust-certs	CISCOIM.pem	CISCOIM.der	Trusted local cluster own-certificate
ipsec-trust	trust-certs	cisco-CUCM.sv.avaya.com.pem	cisco-CUCM.sv.avaya.com.der	Trust Certificate
ipsec-trust	trust-certs	CISCOIM.pem	CISCOIM.der	CupPubIpsecCert
cup	certs	cup.pem	cup.der	Self-signed certificate generated by system
cup-xmpp	certs	cup-xmpp.pem	cup-xmpp.der	Self-signed certificate generated by system
cup-xmpp-s2s	certs	cup-xmpp-s2s.pem	cup-xmpp-s2s.der	Self-signed certificate generated by system
cup-trust	trust-certs	CISCOIM.pem	CISCOIM.der	Trusted local cluster own-certificate
cup-xmpp-trust	trust-certs	System_Manager_CA.pem	System_Manager_CA.der	avaya smgr root cert
cup-xmpp-trust	trust-certs	CISCOIM.pem	CISCOIM.der	Trusted local cluster own-certificate
cup-xmpp-trust	trust-certs	default.pem	default.der	Signed Certificate

Importing certificate into Presence Services trust store

Procedure

1. Log on the System Manager web console from where Presence Services installed.
2. Navigate to **Elements** > **Avaya Breeze™**.
3. Click **Cluster Administration**.

4. Select the cluster on which Presence Services installed.
5. Click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze instances)**.



6. Click **Browse** to select the cisco jabber certificate pem file.
7. Click **Retrieve Certificate**.
8. Click **Commit**.

   The certificate is imported.
9. Log in to the presence server, and run the following command:

   ```
   find / opt —name trust.jks -exec keytool -V —list -keystore {}\;
   ```
10. Press `Enter` when prompted for password to verify loaded certificate.

    If certificate is loaded successfully, the certificate content is displayed.

```
Alias name: 657aa3eb9dca58e1692122b0
Creation date: Oct 21, 2015
Entry type: trustedCertEntry

Owner: L=SANTA CLARA, ST=CA, CN=jabber.avaya.com, OU=MARKETING, O=AVAYA,
C=USIssuer: L=SANTA CLARA, ST=CA, CN=jabber.avaya.com, OU=MARKETING, O=AVAYA, C=US
Serial number: 5be76fe7b9eb21fb7c4bd1b8f4975031
Valid from: Tue Oct 20 09:32:45 EDT 2015 until: Sun Oct 18 09:32:44 EDT 2020
Certificate fingerprints:
                          MD5: 5C:CB:65:0C:94:8B:A5:5D:E7:10:B4:84:2D:40:19:9B
                                    SHA1: 65:7A:A3:EB:9D:CA:
58:E1:69:21:22:B0:97:38:FB:26:C9:0A:C4:B6
                        SHA256: AC:6B:B6:53:45:F6:8F:B8:1C:AD:
51:49:A9:1E:EE:D2:FA:F4:1C:1A:C6:44:EE:80:C1:BD:8D:75:4D:89:99:E8
                                    Signature algorithm name: SHA1withRSA
                                      Version: 3

Extensions:
#1: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
clientAuth
ipsecEndSystem
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
```

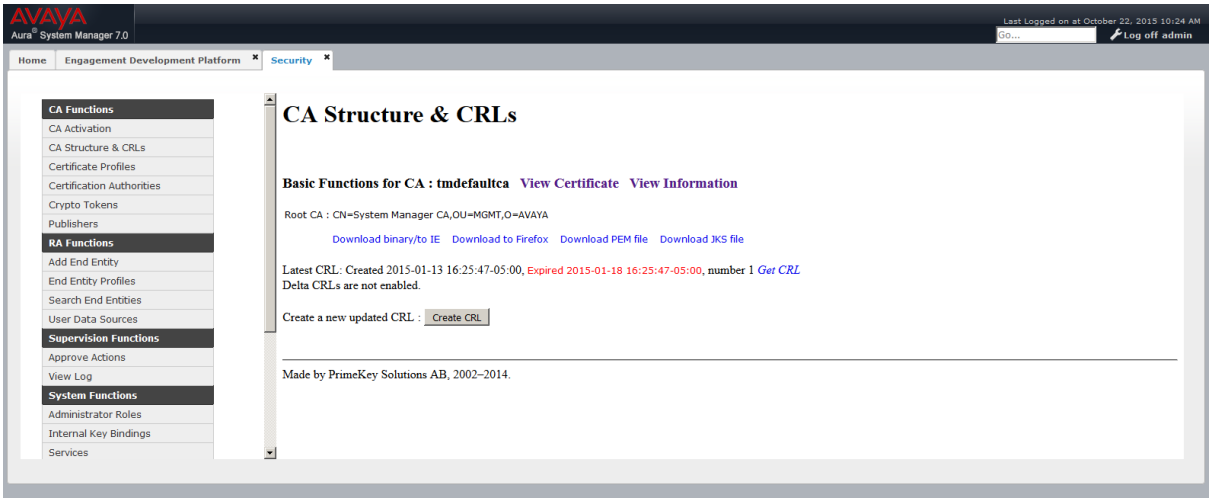
```
DigitalSignature
Key_Encipherment
Data_Encipherment
Key_Agreement
Key_CertSign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 20 A7 37 9E A8 A5 2D 69  10 6A 1A 0F C3 8B 2D 6B  .7...-i.j....-k
0010: 9C FF 7C 2E
]
]
```

11. Restart the cluster for the changes to take effect.

Importing System Manager root certificate into Cisco Jabber trust store

Procedure

1. On the System Manager web console, navigate to **Security** > **Certificate** > **Authority** > **CA Structure & CRLs**.
2. Click **Download PEM** to download the System Manager root certificate.



3. Log on to Cisco Unified CM IM and Presence Administration.
4. Click **System** > **Security** > **Certificate Management**.
5. Click **Upload Certificate/Certificate chain**.

   The system displays new window.
6. Select **cup-xmpp-trust**.
7. Click **Browse** to select the file to be loaded.
8. Click **Upload File**.

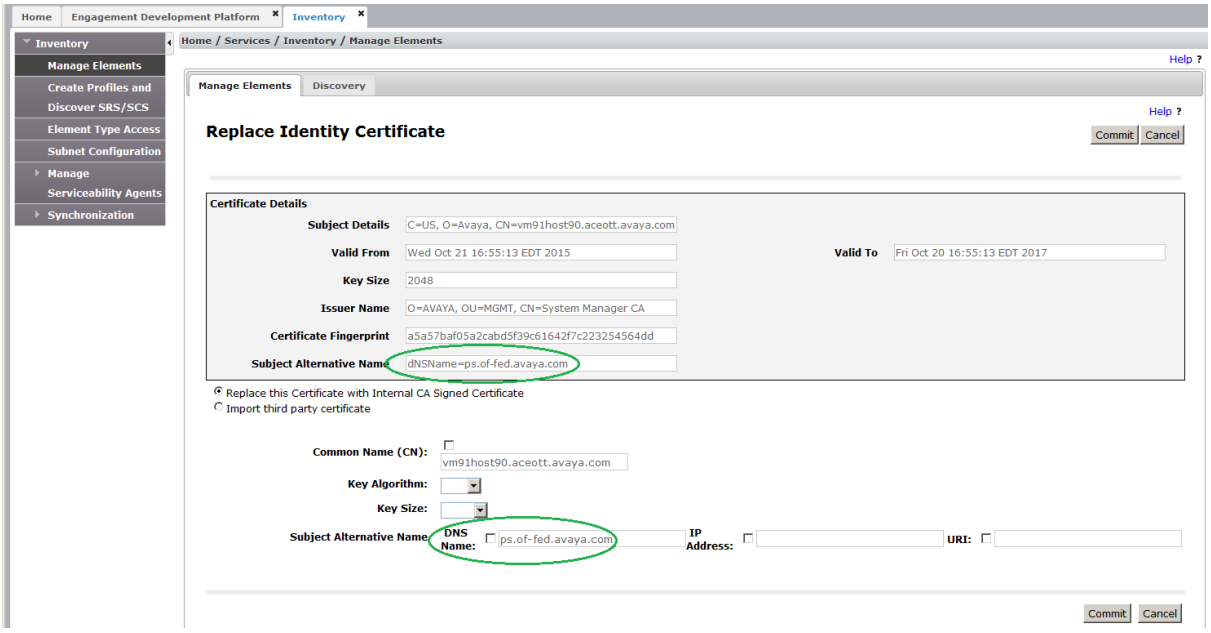
Modifying default certificate to Subject Alternative Name certificate

About this task

When Presence Services is installed, Avaya Breeze™ generates a default certificate. The owner is machine hostname. When Presence Services federates with remote XMPP server, Presence Services uses presence domain which is different from the hostname in most of the cases. To pass certificate validation on remote machine, the presence domain is added to default certificate. This setting is achieved by using Subject Alternative Name.

Procedure

1. Log on to the System Manager web console from where Presence Services is installed.
2. Click **Services** > **Inventory**.
3. Click **Manage Elements**.
4. Select the Avaya Breeze™ instance.
5. Click **More Actions** > **Configure Identity Certificate**.
6. Select **Websphere**, and click **Replace**.
7. Select the **DNS Name** check box, and enter the presence domain.



8. Click **Commit**.
9. Restart the cluster for the changes to take effect.
10. To verify that the presence domain is added, on the Presence Services server, run the following command: `find/opt—name key.jks-exec keytool —V —list —keystore {} \;|grep<presence domain>`.

```
Certificate[1]:
Owner: C=US, O=Avaya, CN=vm91host90.aceott.avaya.com
Issuer: O=AVAYA, OU=MGMT, CN=System Manager CA
```

```
Serial number: 785bae26105c2ced
Valid from: Fri Oct 23 09:21:34 EDT 2015 until: Sun Oct 22 09:21:34 EDT 2017
Certificate fingerprints:
                         MD5: 8B:AD:8C:2F:40:8A:B6:55:04:44:EE:8F:AE:91:4D:BF
                      SHA1: A8:40:84:64:5C:1C:66:7C:
5A:A7:85:40:B9:D4:E8:A2:AE:E3:96:A2
                       SHA256:12:28:A2:5E:9E:07:BB:D1:36:BF:E3:7A:E2:B1:77:3F:
2F:F1:EB:55:DF:D3:31:20:97:B3:BB:6E:4B:08:AF:58
Signature algorithm name: SHA256withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 97 57 54 F9 71 DC D1 CB  2C 3B 7B 65 9B 07 E5 9A .WT.q...,;.e....
0010: 9A AB ED 50
]
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:false
PathLen: undefined

]
#3: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
clientAuth
]


#4: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Non_repudiation
Key_Encipherment
Data_Encipherment
Key_Agreement
]

#5: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
DNSName:  ps.of-fed.avaya.com
DNSName: ps.cisco-fed.avaya.com
]

#6: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 80 9C 80 2A 04 52 46 33  46 AF 5A 65 FC 65 C4 46 ...*.RF3F.Ze.e.F
0010: 9B 38 3B 7A                                       .8;z
]
]
```

Generating the Certificate Signing Request file

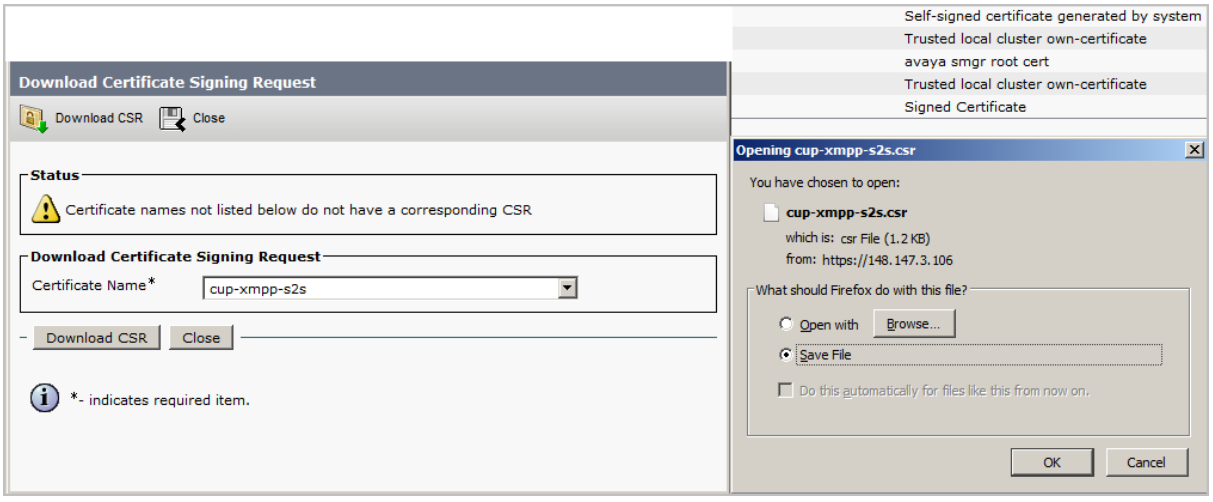
Procedure

1. Log on to Cisco Unified CM IM and Presence Administration.
2. Click **System** > **Security** > **Certificate Management**.
3. Click **Generate**.

The system displays a new window.

4. Select **cup-xmpp-s2s**.
5. Click **Generate** to generate the Certificate Signing Request (CSR) file.

6. Click **Download CSR** to save the **cup-smpp-s2s.csr** file.

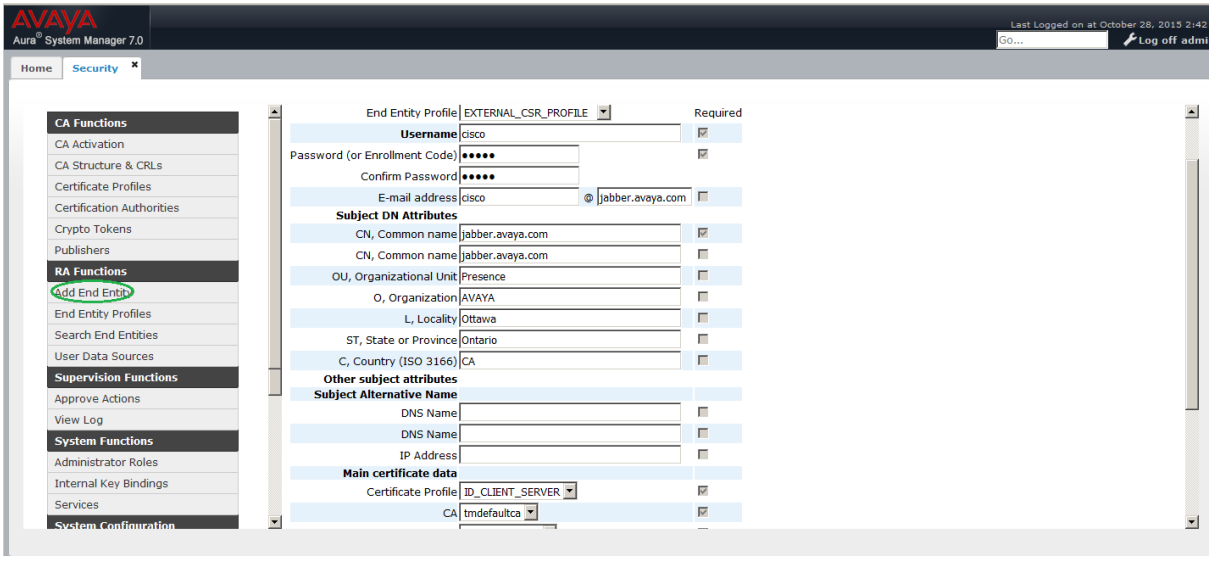


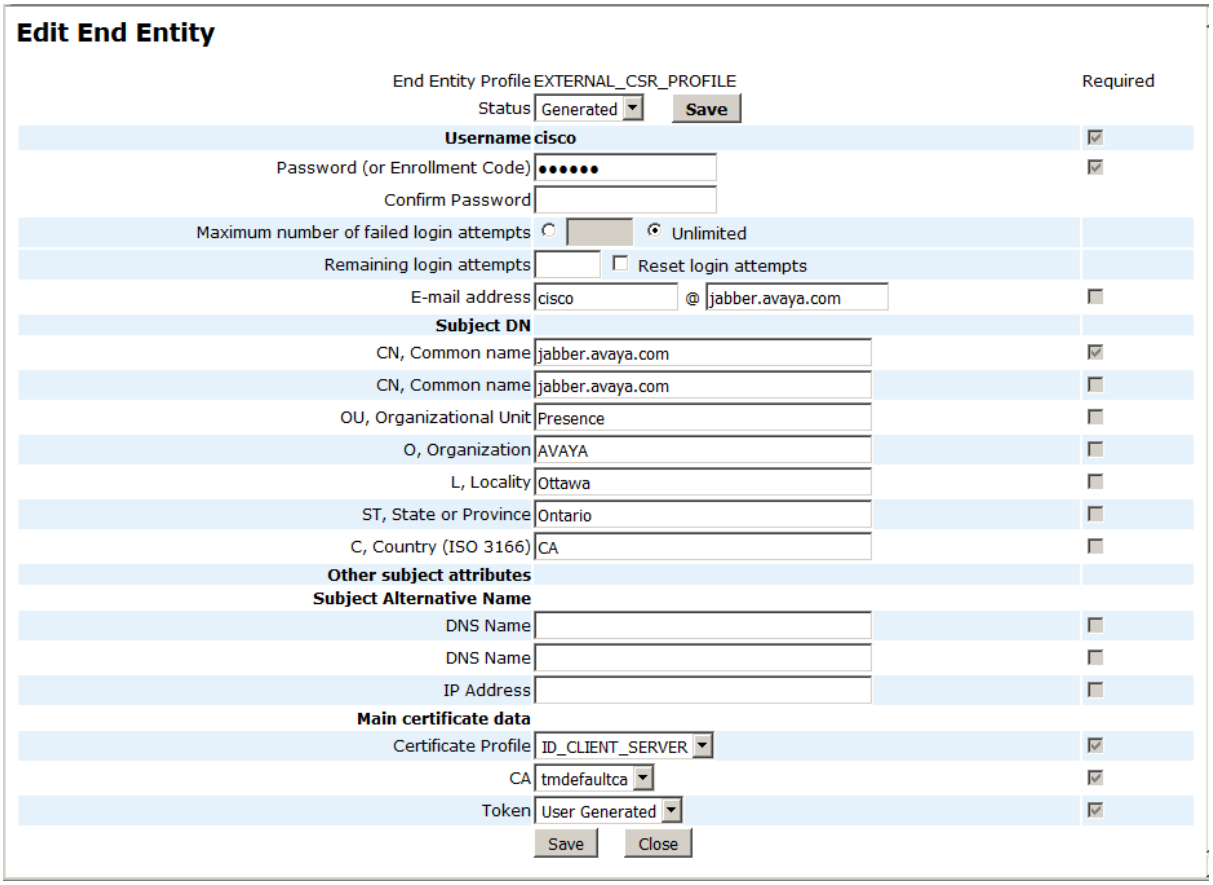
Generating profile on System Manager

Procedure

1. On the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.

2. Select **Add End Entity**, and enter the following details:
   - **End Entity Profile**: `EXTERNAL_CSR _PROFILE`
   - **Username**: `Cisco`
   - **Password/Enrollment Code**: `Cisco`
   - **Confirm Password**: `Cisco`
   - **CN, Common name**: `<cisco jabber domain>`
   - **O, Organization**: `Avaya`
   - **C, Country**: `CA`
   - **OU, Organization Unit**: `Presence`
   - **L, Locality**: `Ottawa`
   - **ST, State or Province**: `Ontario`
   - **Certificate Profile**: `ID_CLIENT_SERVER`
   - **CA**: `tmdefaultca`
   - **Token**: `User Generated`



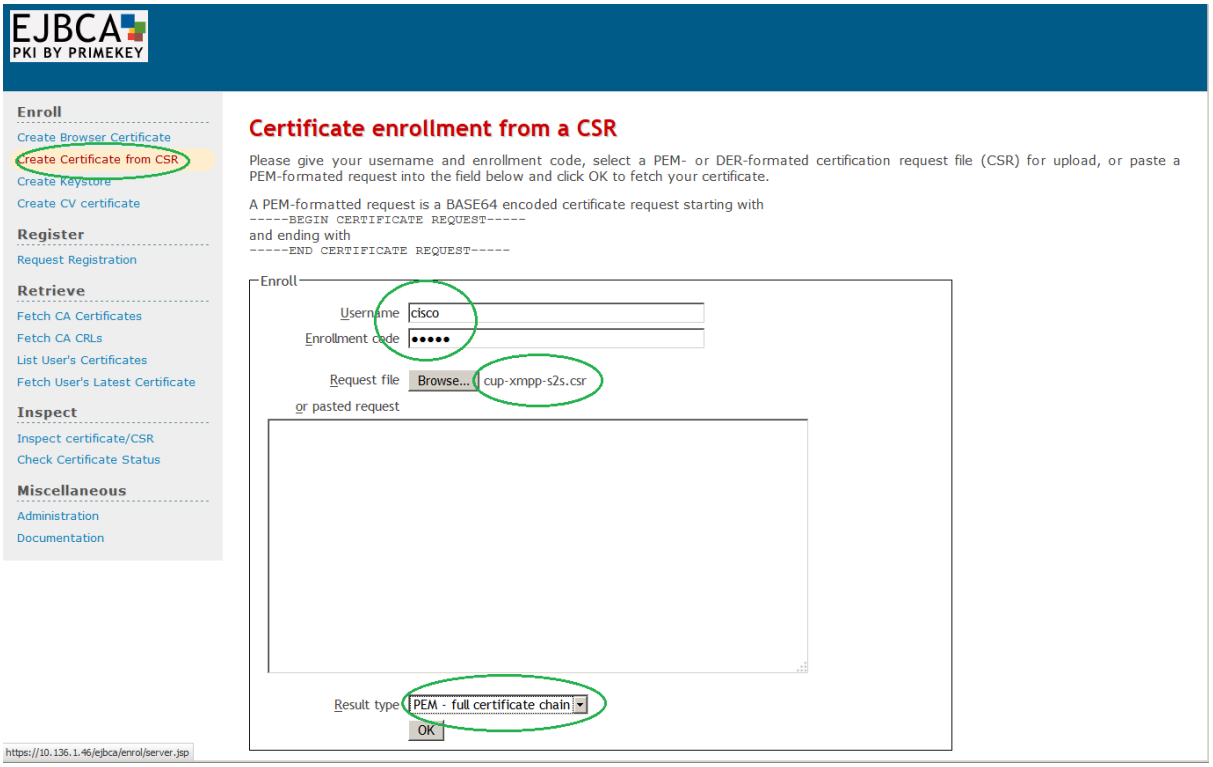


3. Click **Add**.

Signing the Cisco Jabber CSR on System Manager

Procedure

1. On the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
2. Select **Public Web**.
3. Click **Create Certificate from CSR**, and enter the following details:
   - Username: `cisco`
   - Enrollment code: `cisco`
   - Paste the signing request from Openfire.
   - In the **Result Type** field, select **PEM - full certificate chain**



4. Click **OK**.
5. Open the resulting PEM file in text editor on Windows.

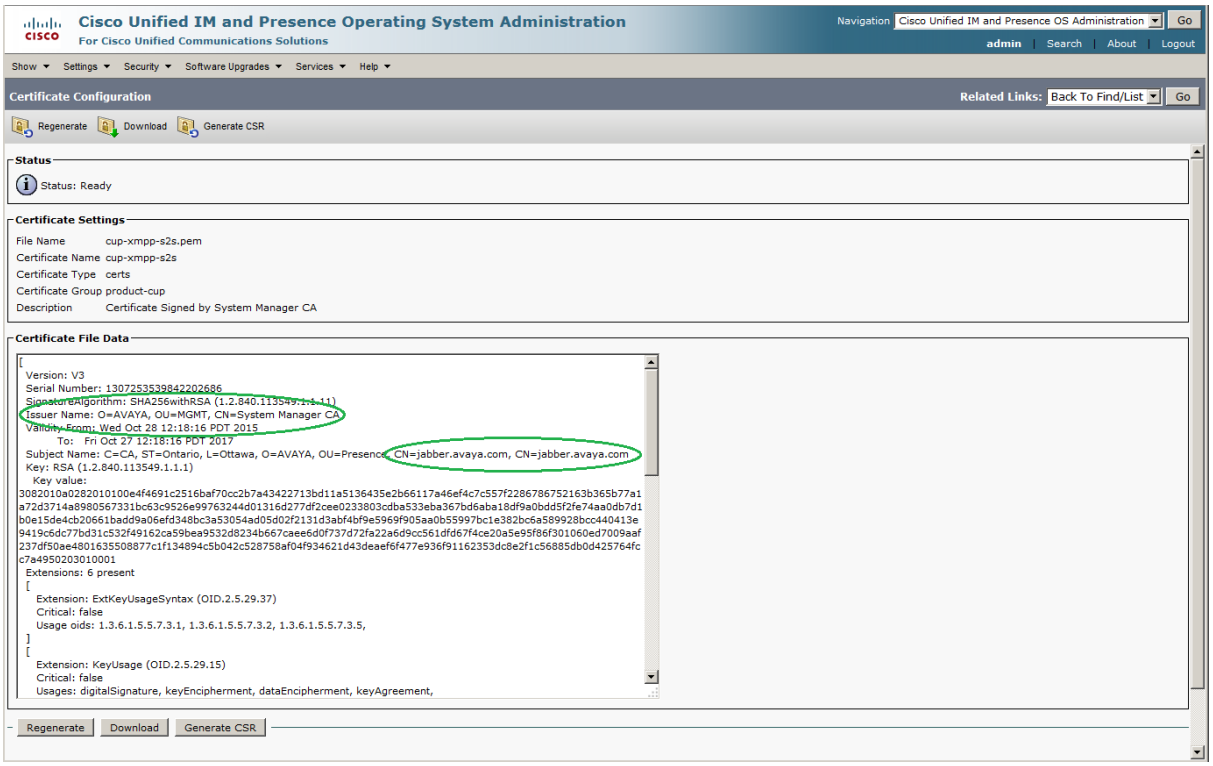
Installing System Manager signed Cisco certificate on Cisco Jabber

Procedure

1. Log on to Cisco Unified CM IM and Presence Administration.
2. Click **System** > **Security** > **Certificate Management**.
3. Click on **Upload Certificate/Certificate Chain** button.

   The system displays a new window.
4. Select **cup-xmpp-s2s**.

5. Click **Upload file**.



IM Blocking in Do Not Disturb state

You can administer Presence Services to block IMs to a user who is in the Do Not Disturb (DND) state. If blocking is enabled and a user sends an IM to a user in the DND state, Presence Services:

- Persistently stores the IM.
- Sends an XMPP message to the sender indicating that the IM has been temporarily blocked.
- Delivers the IM when the recipient changes the state from DND to another state.

By default, IMs are not blocked to users in the DND state.

DND Whitelisting

If IM Blocking in DND state is enabled, then DND Whitelisting overrides this behavior. If user A in DND state initiates a chat session to user B, user B is added to user A's DND Whitelist. While user B is in user A's DND Whitelist, IMs from user B will be delivered to user A, even if user A is in DND state. When user A closes the chat session with user B, then user B is removed from user A's DND Whitelist.

Example of IM blocking enabled

- The status of user A is Available. User B sends IM1 to user A, Presence Services delivers IM1 to user A.

- User A changes the state to DND. User B sends IM2 to user A, Presence Services blocks IM2.
- User A opens chat session to user B. User B is added to user A's DND Whitelist. Presence Services delivers IM2 to user A. User A sends IM3 to user B, Presence Services delivers IM3 to user B. User B sends IM4 to user A. Presence Services delivers IM4 to user A.
- User C sends IM5 to user A, Presence Services blocks IM5 as user C is not on user A's DND Whitelist.
- User A closes chat session to user B. Presence Services removes user B from user A's DND Whitelist. User B sends IM6 to user A, Presence Services blocks IM6.
- User A changes the state to a state other than DND, Presence Services delivers IM5 and IM6 to user A.t

Configuring IM Blocking in Do Not Disturb state

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **Instant Messaging** group.
6. In the **Block IMs for users in Do-Not-Disturb (DND) state** field:
   - To disable blocking of IMs to users in Do Not Disturb state, verify that the value is `false`.
   - To enable blocking of IMs to users in Do Not Disturb state, select **Override Default**, and in the **Effective Value** field, type `true`.
7. Click **Commit**.

Accessing the Presence Services Software Inventory web service

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**
2. Click **Cluster Administration**.

   The table displays a list of Avaya Breeze™ clusters.
3. For the cluster containing Presence Services, in the **Service URL** field, select **Presence Services Admin**.

The system displays a new window.

4. Log in using System Manager administrative credentials.

   The system displays the Presence Services Status page.

5. You can perform the following:
   - Click **IM BROADCAST** to use Instant Message Broadcast Tool.
   - Click **THIRD PARTY SOFTWARE** for information about third-party software inventory.
   - Click **USERS** for information about cluster users.
6. After making the required changes, click **Log Off**.

Instant Message Broadcast Tool

Instant Message Broadcast Tool allows the system administrator to broadcast an instant message (IM) to all or a subset of logged-in users through the XMPP-capable client.

Instant Message Broadcast Tool can accessed through the Presence Services web page. For information about using Instant Message Broadcast Tool, see “Using Instant Message Broadcast Tool”.

Using Instant Message Broadcast Tool

Before you begin

Access the Presence Services Software Inventory web service. For more information, see “Accessing the Presence Services Software Inventory web service”.

Procedure

1. On the Presence Services Software Inventory web service page, log in using the System Manager administrative credentials.
2. Click **Instant Message Broadcast Tool**.

   The system displays the Instant Message Broadcast Tool page.

3. In the message box, enter the message that you want to send to the users.

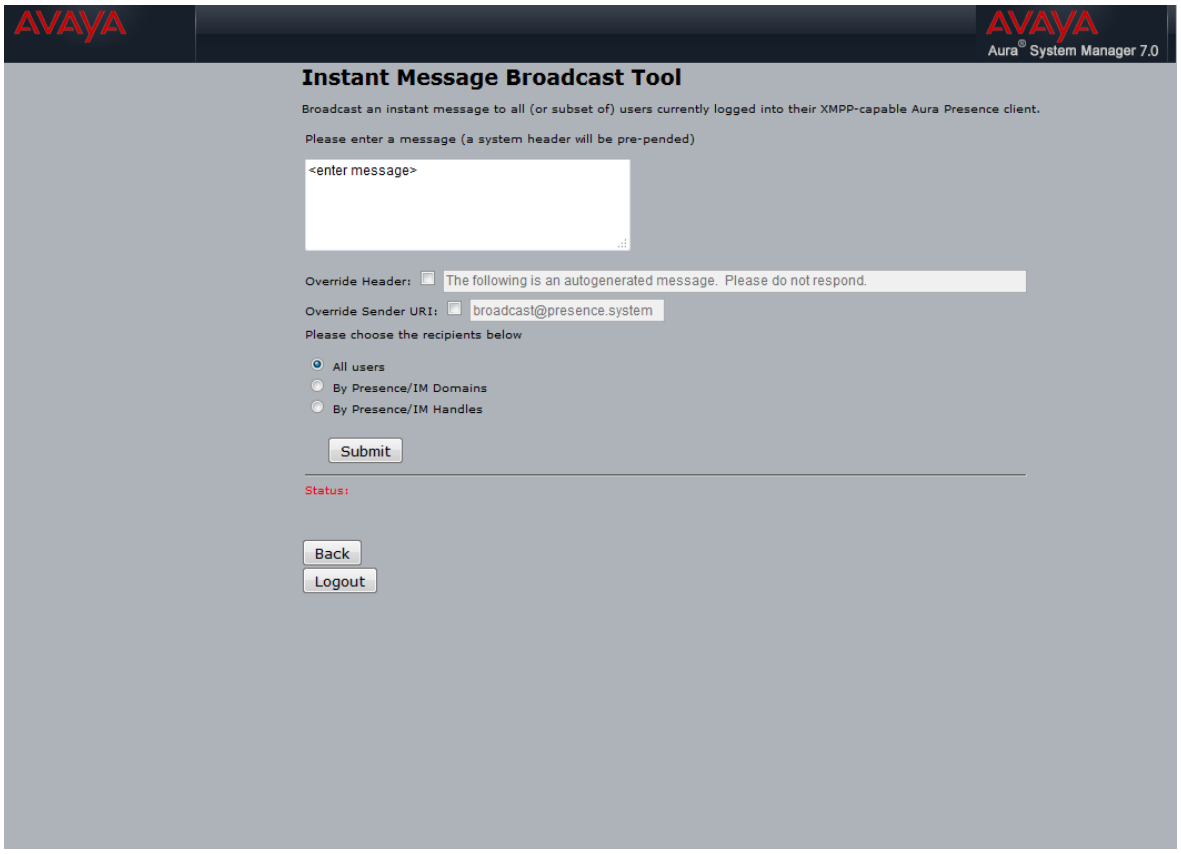
   A default header is provided which will be pre-pended to all messages.

4. To override the default header, select the **Override Header** field and enter the new header.
5. To override the Sender URI, select **override Sender URI** field.

   The sender URI is not the actual Presence/IM user but will be displayed on the chat window of the recipient.

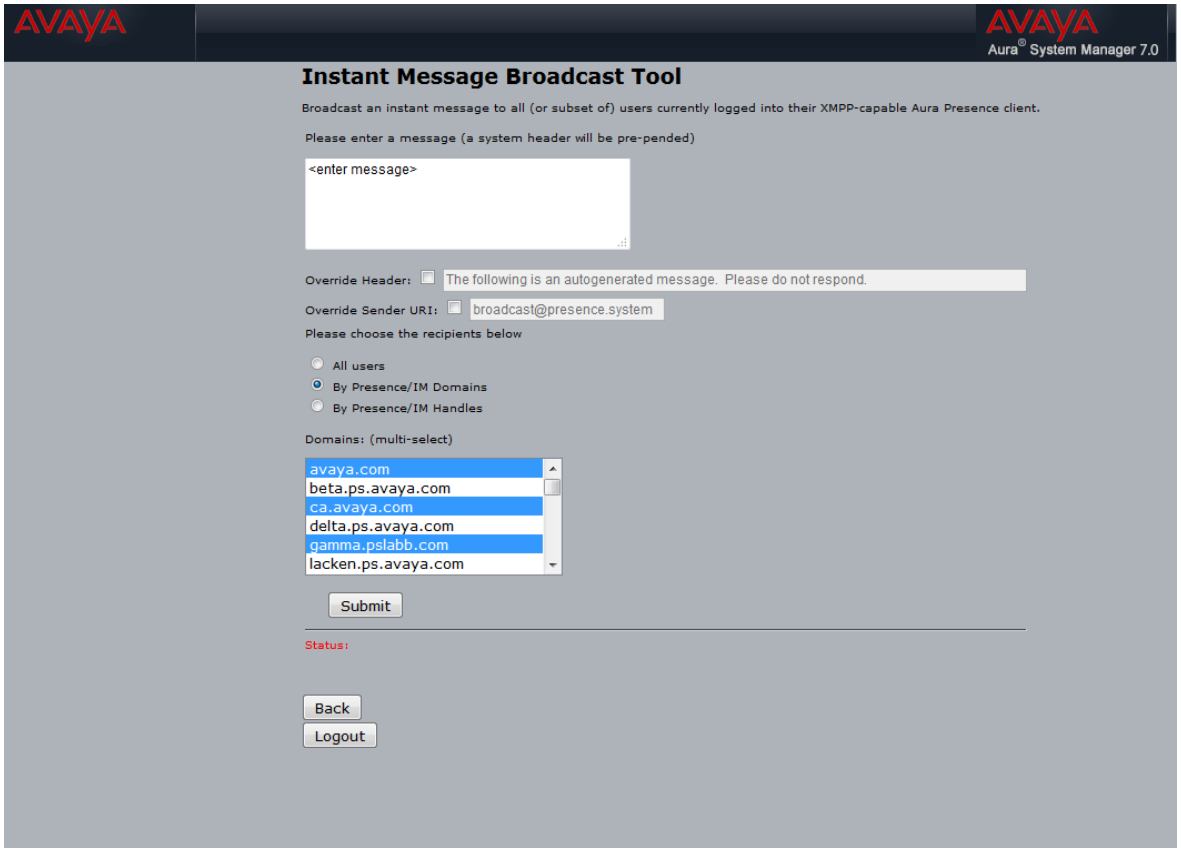
6. In the **Please choose the recipients below**, select:
   - All users: To send the message to all logged-in users.

     This is the default option.



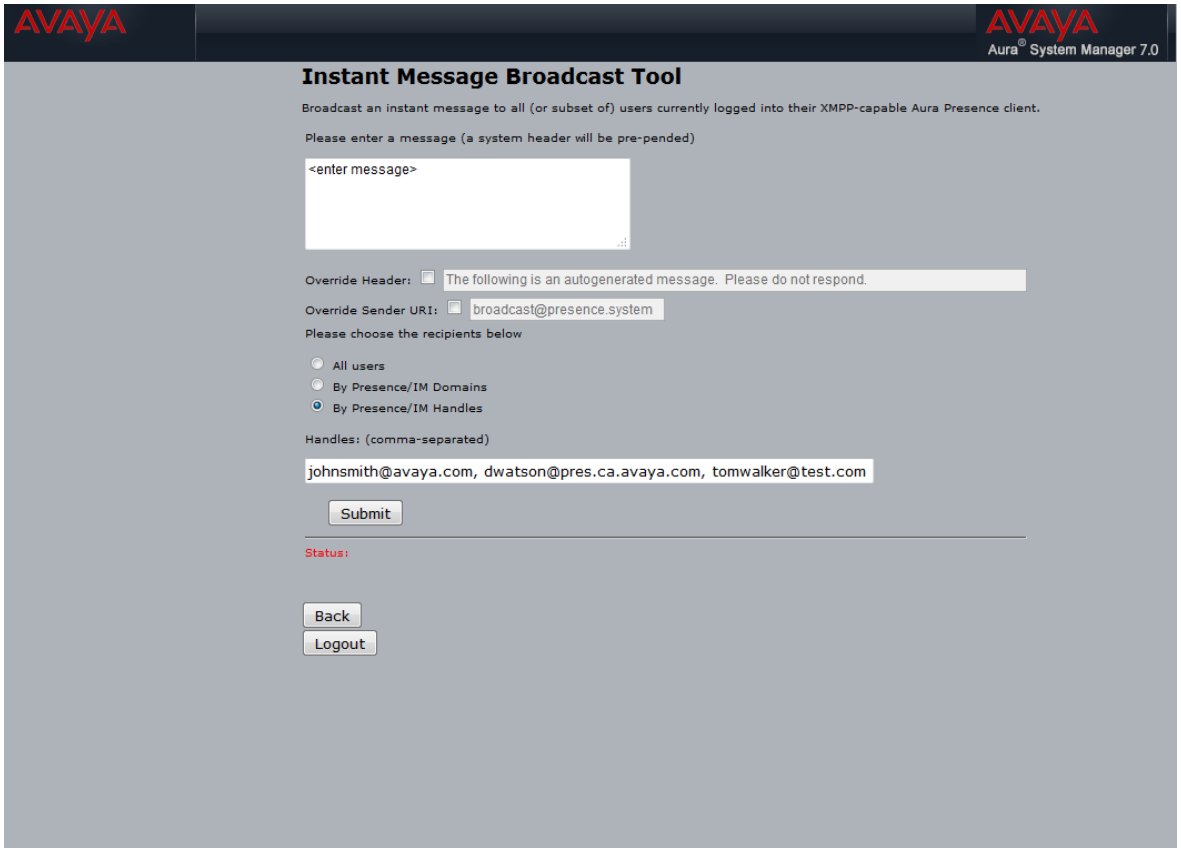
   - By Presence/IM Domains: To send the message to a set of Presence/IM domains.

     The system displays a list of domains. Select one or more applicable domains.



- By Presence/IM Handles: To send the message to a set of users using the Presence/IM handle.

  In the text-field, enter each handle separated by commas.



7. Click **Submit**.

   The system will reload the page with a successful status message.

8. To return to the Presence Services Software Inventory web service page, click **Back**.
9. To logout of the Presence Services Software Inventory web service page, click **Logout**.

Interoperability with Avaya Multimedia Messaging

Avaya Multimedia Messaging provides a rich messaging solution for Avaya Aura® users.

There are two categories of Avaya messaging devices:

- Instant Messaging: Messaging is provided by Presence Services using XMPP IM and Presence is provided by Presence Services using SIP or XMPP. Most Avaya devices fall into this category.
- Rich Messaging: Messaging is provided by Avaya Multimedia Messaging using REST and Presence is provided by Presence Services using SIP or XMPP. Some next-generation Avaya devices fall into this category.

On System Manager, users are administered in one of two modes:

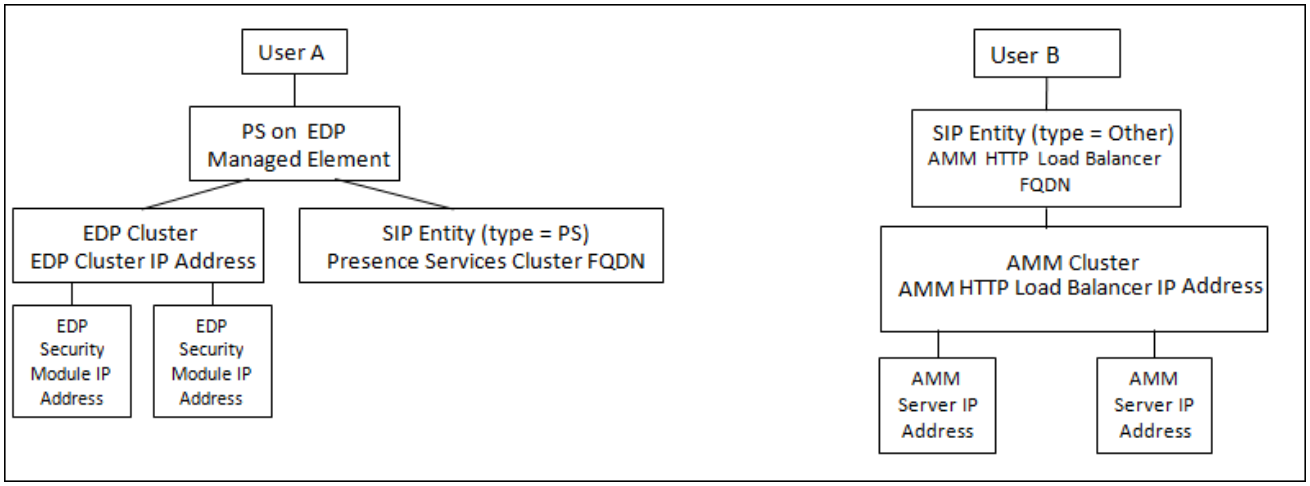
- If the user has an Instant Messaging device, then:
  - For Presence, administer the home Presence Services cluster of the user at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **System**.
  - For Messaging, administer the home Presence Services cluster of the user at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **IM Gateway SIP Entity**.
  - See “Assigning Presence Profile to a user on System Manager”.
- If the user has a Rich Messaging device, then:
  - For Presence, administer the home Presence Services cluster of the user at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **System**.
  - For Messaging, administer the home Avaya Multimedia Messaging cluster of the user at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **IM Gateway SIP Entity**. The **IM Gateway SIP Entity** field points to a SIP Entity, of type Other, that represents the Avaya Multimedia Messaging cluster.
- If the user has no Messaging device, then:
  - No Presence Profile is administered at **Users** > **User Management** > **Manage Users** > **Communication Profile**.

Messaging is supported between Avaya Instant Messaging and Avaya Rich Messaging devices. Consult Avaya Multimedia Messaging documentation for a solution description.

In the following diagram, when User A logs in to an Instant Messaging device, Messaging services are provided by a two-server Presence Services cluster, and when User B logs in to a Rich Messaging device, Messaging services are provided by a two-server Avaya Multimedia Messaging Cluster.

Presence Services connects to Avaya Multimedia Messaging using an Avaya Multimedia Messaging HTTP Load Balancer FQDN. A DNS SRV record, and DNS A record, resolve this to an Avaya Multimedia Messaging HTTP Load Balancer IP Address and port.

Avaya Multimedia Messaging connects to Presence Services using Presence Services Cluster FQDN. See “Table 1: Key customer configuration information”, Row 25. A DNS SRV record resolves this to an Avaya Breeze™ HTTP Load Balancer FQDN and port. A DNS A record resolves Avaya Breeze™ HTTP Load Balancer FQDN to an Avaya Breeze™ Cluster IP Address. See “Table 1: Key customer configuration information”, Row 22. In Presence Services Release 7.0.1, the Avaya Breeze™ Cluster IP address is required for accessing Presence Services web services, and for Presence Services deployments that interoperate with Avaya Multimedia Messaging. This IP address must be routable. When incoming messages are routed to the Avaya Breeze™ Cluster IP address, the Avaya Breeze™ HTTP Load Balancer distributes incoming messages equally across all servers in the cluster.



Key customer configuration information

Before performing the tasks in the “Checklist for administering Avaya Multimedia Messaging”, obtain the following information, and record in the **Customer value** column of the table.

Table 18: Key customer configuration information

No.	Requirement	Customer value	Reference
1	Presence Services Cluster FQDN		See “Table 1: Key customer configuration information”, row 25
2	Avaya Breeze™ HTTP Load Balancer FQDN		—
3	Avaya Breeze™ Cluster IP address		See “Table 1: Key customer configuration information”, row 22
4	Avaya Multimedia Messaging HTTP Load Balancer FQDN		—
5	Avaya Multimedia Messaging HTTP Load Balancer IP Address		—
6	Name of Avaya Multimedia Messaging SIP Entity		—
7	Full hostname of each server in Avaya Multimedia Messaging cluster		—

Checklist for administering Avaya Multimedia Messaging

In the following table:

- *x* denotes the number of Avaya Multimedia Messaging hosted users.

- *y* denotes the number of servers in the Presence Services cluster.

Table 19: Checklist for administering Avaya Multimedia Messaging

No.	Task	Reference	✔
1	Administer DNS SRV record to resolve Avaya Messaging InterOp Gateway service to Avaya Breeze™ HTTP Load Balancer FQDN and Avaya Breeze™ HTTP Port for Presence Services Cluster FQDN.	Administering DNS SRV record to resolve Avaya Messaging InterOp Gateway service to Avaya Breeze HTTP Load Balancer FQDN and Avaya Breeze HTTP Port for Presence Services Cluster FQDN on page 148	
2	Administer DNS A record to resolve Avaya Breeze™ HTTP Load Balancer FQDN to Avaya Breeze™ Cluster IP Address.	—	
3	Administer DNS SRV record to resolve Avaya Messaging InterOp Core service to Avaya Multimedia Messaging HTTP Load Balancer FQDN and Avaya Multimedia Messaging HTTP Port for Avaya Multimedia Messaging HTTP Load Balancer FQDN.	Administering DNS SRV record to resolve Avaya Messaging InterOp Core service to AMM HTTP Load Balancer FQDN and AMM HTTP Port for AMM HTTP Load Balancer FQDN on page 148	
4	Administer DNS A record to resolve Avaya Multimedia Messaging HTTP Load Balancer FQDN to Avaya Multimedia Messaging HTTP Load Balancer IP Address.	—	
5	Administer Avaya Multimedia Messaging SIP Entity.	Administering Avaya Multimedia Messaging SIP Entity on page 149	
6	Administer *x* users' home Avaya Multimedia Messaging Cluster.	Administering home Avaya Multimedia Messaging Cluster of the user on page 149	
7	Administer Avaya Breeze™ Cluster for Avaya Multimedia Messaging interoperability.	Administering Avaya Breeze Cluster for Avaya Multimedia Messaging interoperability on page 150	
8	Administer Avaya Multimedia Messaging Service Attributes.	Administering Avaya Multimedia Messaging Service Attributes on page 150	
9	Modify *y* Presence Services Security Module HTTPS identity certificates.	Modifying Presence Services Security Module HTTPS identity certificate on page 151	
10	Modify *y* Presence Services WebSphere identity certificates.	Modifying Presence Services WebSphere identity certificate on page 153	
11	Restart Presence Services.	Restarting Presence Services on page 164	

Administering DNS SRV record to resolve Avaya Messaging InterOp Gateway service to Avaya Breeze™ HTTP Load Balancer FQDN and Avaya Breeze™ HTTP Port for Presence Services Cluster FQDN

Procedure

On the DNS server used by Avaya Multimedia Messaging, create a DNS SRV record with the following values:

- **Domain**: Enter the Presence Services Cluster FQDN. See “Table 12: Key customer configuration information”, row 1.
- **Service**: Enter `_amiogw-https`.
- **Protocol**: Enter `_tcp`.
- **Priority**: Assign any value.
- **Weight**: Assign any value.
- **Port Number**: Enter `443`
- **Host offering this service**: Enter the Avaya Breeze™ HTTP Load Balancer FQDN. See “Table 12: Key customer configuration information”, row 2.

Administering DNS SRV record to resolve Avaya Messaging InterOp Core service to AMM HTTP Load Balancer FQDN and AMM HTTP Port for AMM HTTP Load Balancer FQDN

Procedure

On DNS server used by Presence Services, create a DNS SRV record with the following values:

- **Domain**: Enter the Avaya Multimedia Messaging HTTP Load Balancer FQDN. See “Table 12: Key customer configuration information”, row 4.
- **Service**: Enter `_amiocore-https`.
- **Protocol**: Enter `_tcp`.
- **Priority**: Assign any value.
- **Weight**: Assign any value.
- **Port Number**: Enter `8453`
- **Host offering this service**: Enter the Avaya Multimedia Messaging HTTP Load Balancer FQDN. See “Table 12: Key customer configuration information”, row 4.

Administering Avaya Multimedia Messaging SIP Entity

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, type the name of the Avaya Multimedia Messaging SIP Entity. See “Table 12: Key customer configuration information”, row 6.
4. In the **FQDN or IP Address** field, enter the Avaya Multimedia Messaging HTTP Load Balancer FQDN. See “Table 12: Key customer configuration information”, row 4.
5. In the **Type** field, select **Other**.

   Refer to the Avaya Multimedia Messaging documentation for other fields.
6. Click **Commit**.

Administering home Avaya Multimedia Messaging Cluster of the user

About this task

Perform this procedure for each Avaya Multimedia Messaging hosted user.

Procedure

1. On the System Manager web console, navigate to **Home** > **Users** > **User Management** > **Manage Users**.
2. Select the user, and click **Edit**.
3. Click the Communication Profile tab.
4. Select the **Communication Profile with the Default** check box.
5. In the Communication Profile tab, select the check box to the left of Presence Profile, and use the arrow to expand the profile.
6. In the **System** field, administer the home Presence Services cluster of the user as described at “Assigning Presence Profile to a user on System Manager”.
7. In the **IM Gateway SIP Entity** field, select the Avaya Multimedia Messaging SIP Entity created in “Administering Avaya Multimedia Messaging SIP Entity”.
8. Click **Commit**.

Administering Avaya Breeze™ Cluster for Avaya Multimedia Messaging interoperability

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Cluster Administration**.
3. Select the cluster, and in the **Cluster State** field, select **Deny New Service**.
4. When the system displays a warning box, select **Continue**.
5. Select the cluster, and click **Edit**.

   The system displays a Cluster Editor window.
6. Expand the Cluster Attributes section.
7. Select the checkbox to the right of the **Only allow HTTPS traffic** field.
8. Select the checkbox to the right of the Is **load balancer enabled** field.
9. Click **Commit**.
10. Select the cluster, and in the **Cluster State** field , select **Accept New Service**.
11. When the system displays a warning box, select **Continue**.

Note:

The Avaya Breeze™ HTTPS Load Balancer performs a keep-alive between all Avaya Breeze™ Management IP addresses, and Avaya Breeze™ Security Module IP addresses within the cluster. To ensure that the keep-alives are successful, provide DNS records, or `/etc/hosts` entries, so that all servers can reach all other servers within the cluster.

Administering Avaya Multimedia Messaging Service Attributes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. To enable Avaya Multimedia Messaging, navigate to the **AMM Integration Enabled** field within the Avaya Multimedia Messaging group.
   a. Select the **Override Default** check box.

b. In the **Effective Value** field, type `True`.

Avaya Multimedia Messaging is disabled by default.

6. Within the Avaya Multimedia Messaging group, the default value for the **Web service path of the Avaya Multimedia Messaging Server** field is `aem/xmpp/stanza`.

   Refer to Avaya Multimedia Messaging documentation, or do not override the default value.

7. In the **Trusted hostnames of Avaya Multimedia Messaging Server(s)** field within the Avaya Multimedia Messaging group, enter the full hostname of each server in the Avaya Multimedia Messaging Server cluster as a comma-separated list.

   See “Table 12: Key customer configuration information”, row 7.

8. Click **Commit**.

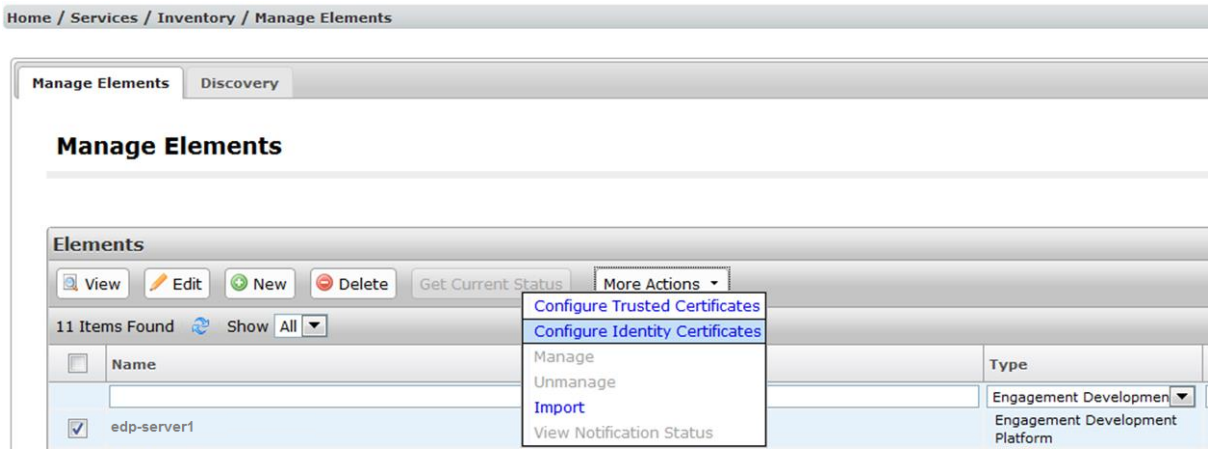
Modifying Presence Services Security Module HTTPS identity certificate

About this task

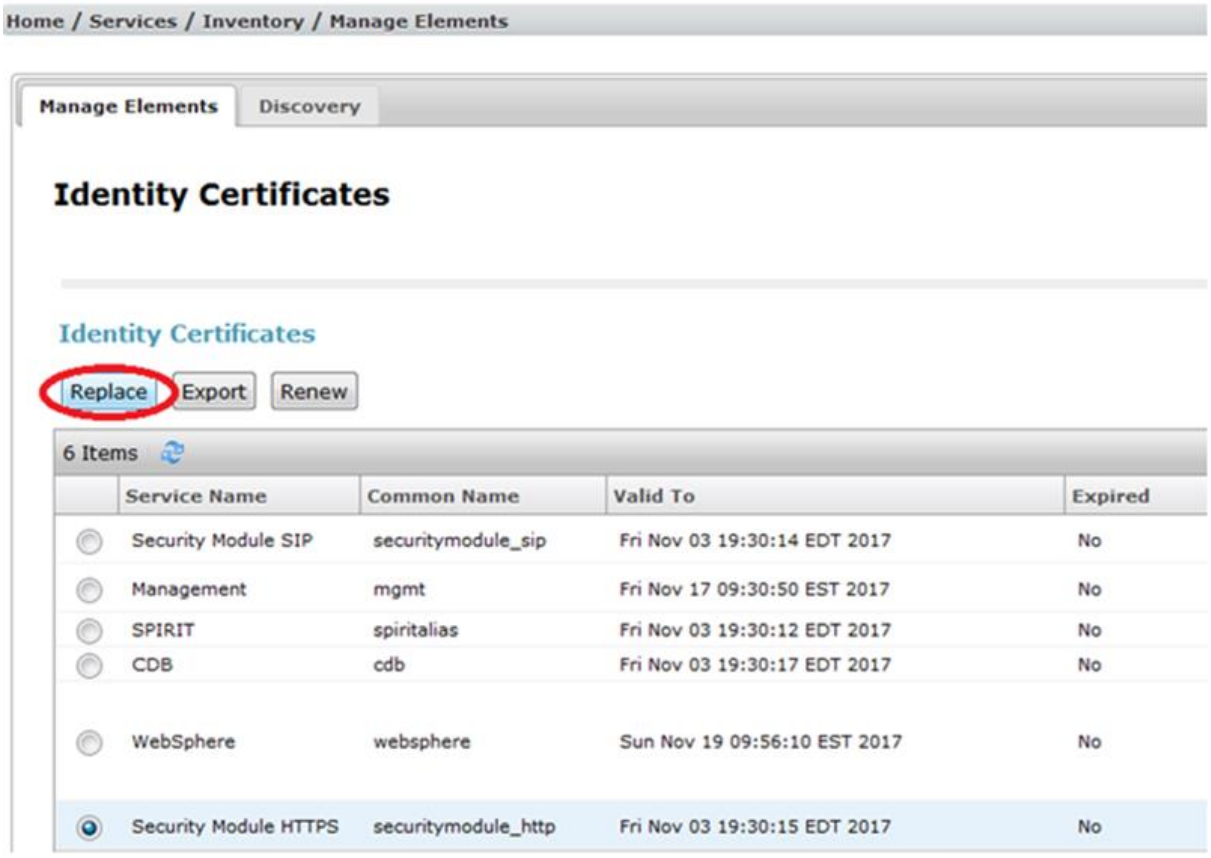
Perform the following procedure for each server in the Presence Services cluster.

Procedure

1. On the System Manager web console, navigate to **Services** > **Elements** > **Inventory** > **Manage Elements**.
2. Select the Avaya Breeze™ server.
3. From the **More Actions** menu, select **Configure Identity Certificates**.

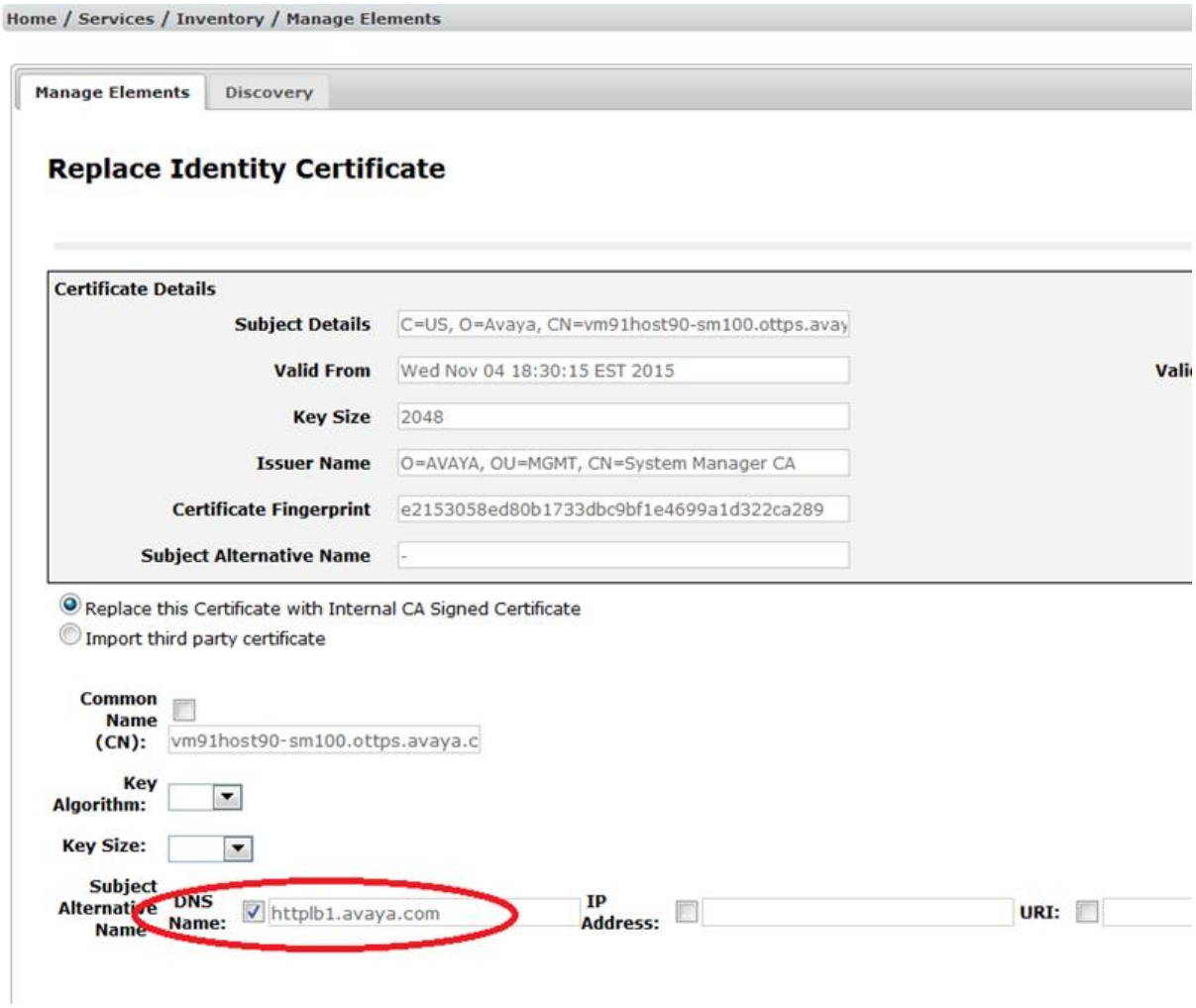


4. Select **Security Module HTTPS**, and click **Replace**.



5. Within the **Subject Alternative Name** field, select the **DNS Name** check box, and enter the Avaya Breeze™ HTTP Load Balancer FQDN.

   See “Table 12: Key customer configuration information”, row 2.



6. Click **Commit**.

Modifying Presence Services WebSphere identity certificate

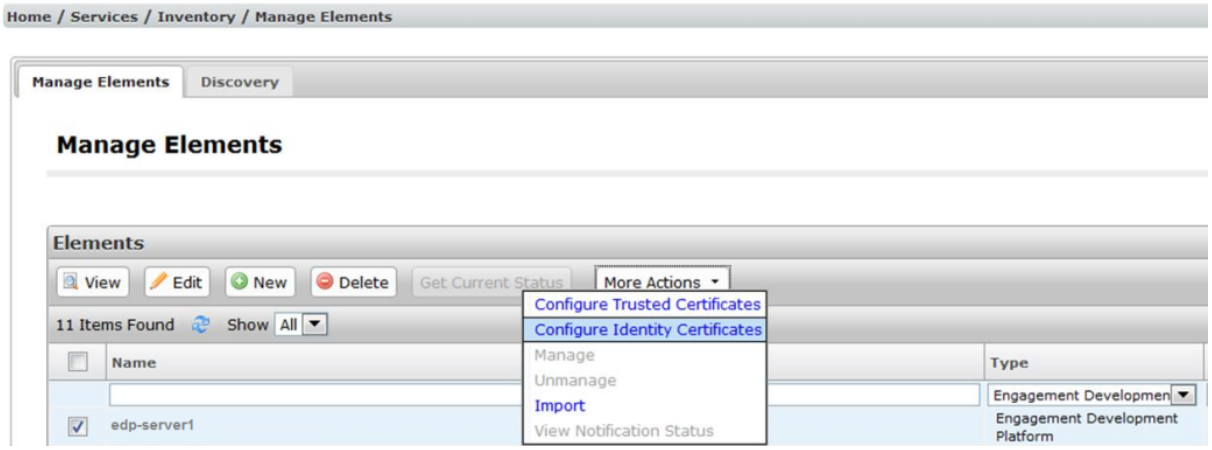
About this task

Perform the following procedure for each server in the Presence Services cluster.

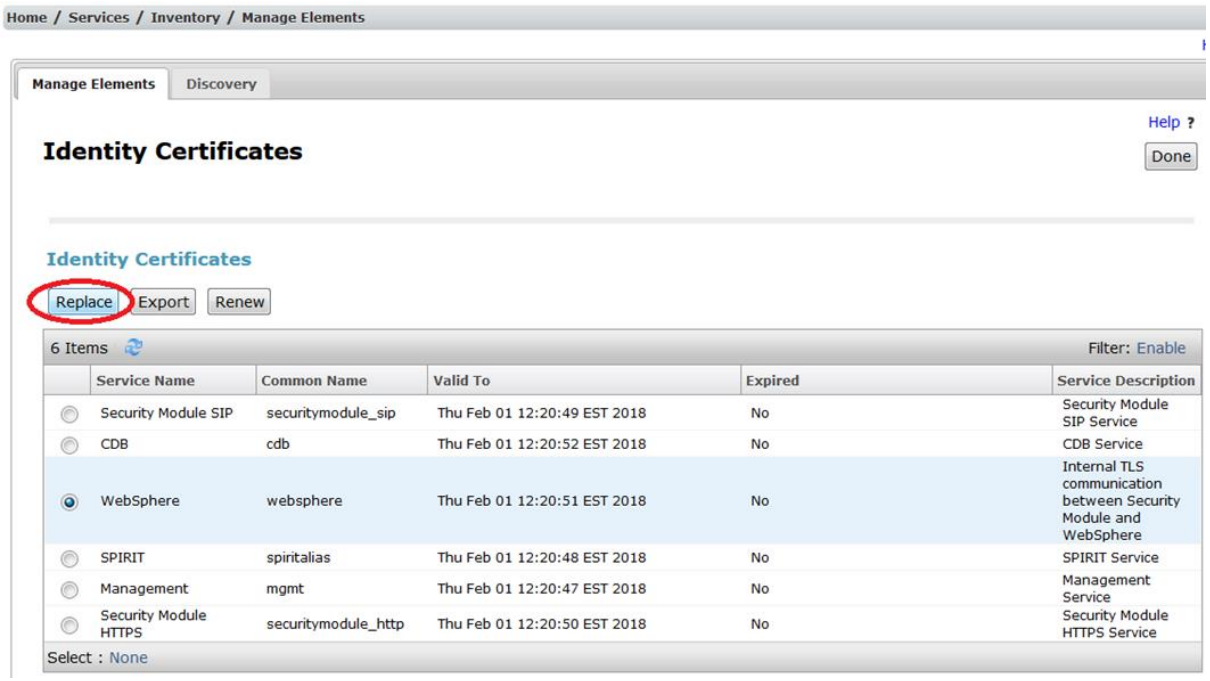
Procedure

1. On the System Manager web console, navigate to **Services** > **Elements** > **Inventory** > **Manage Elements**.
2. Select the Avaya Breeze™ server.

3. From the **More Actions** menu, select **Configure Identity Certificates**.

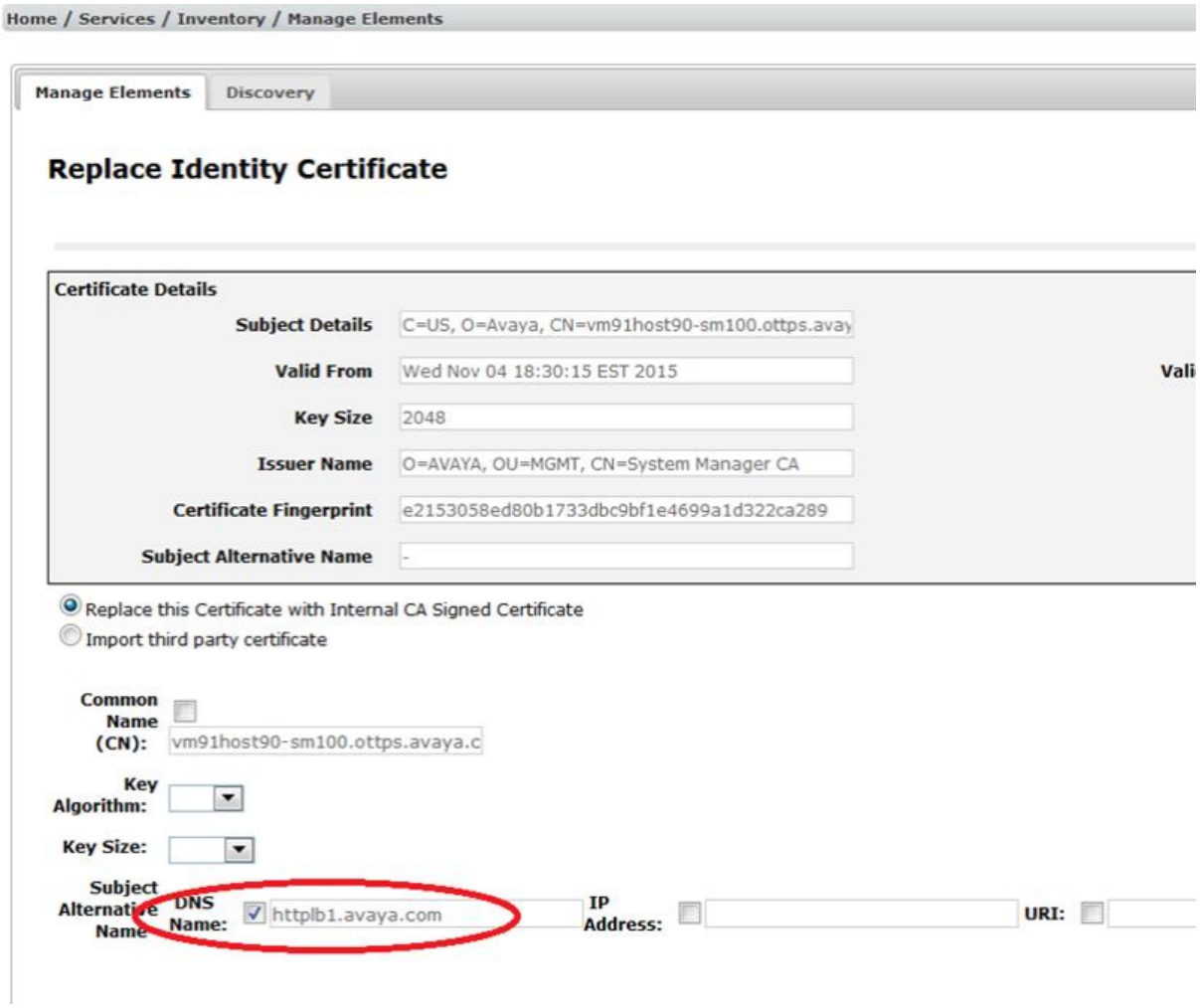


4. Select **WebSphere**, and click **Replace**.



5. In the **Subject Alternative Name** field, select the **DNS Name** check box, and enter the Avaya Breeze™ HTTP Load Balancer FQDN.

   See “Table 12: Key customer configuration information”, row 2.



6. Click **Commit**.

Inter-Domain Presence and IM

Presence Services supports multiple Presence/IM domains. For more information, see “Configuring Presence/IM routing domain on System Manager”. By default, users with Avaya Presence/IM communication addresses in different Presence/IM domains can exchange Presence and IMs. You can administer Presence Services to block presence and IM exchange between users with Avaya Presence/IM communication addresses in different Presence/IM domains.

Configuring Inter-Domain Presence and IM

About this task

This procedure only applies to Avaya Aura® users managed by the same System Manager instance.

If federation is enabled on Presence Services, Presence and IM exchange is always allowed between Avaya Aura® users and federated users even if they are in different domains.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **System** group.
6. In the **Enable Inter-Domain Presence and IM** field:
   - To enable Inter-Domain Presence and IM, verify that the value is `True`.
   - To disable Inter-Domain Presence and IM, select **Override Default**, and in the **Effective Value** field, type `False`.
7. Click Commit.

   Inter-Domain Presence and IM is enabled by default.

Managing users

Soft delete vs. hard delete

When managing users on System Manager at **Home** > **Users** > **User Management** > **Manage Users**, a delete option is provided that supports both soft and hard delete. Depending on the delete you perform, ACLs and contact lists may or may not be deleted.

Soft delete

The user is marked as deleted. The logged-in users will be logged out and watchers will not see the presence of the deleted user. If the user is restored, the contacts and ACL rules will be restored.

Hard delete

The logged-in users will be logged out and watchers will not see the presence of the deleted user. The deleted users contacts and ACL rules are removed from the system.

To re-add the user in the system, the end user must recreate the contacts and re-answer any ACL pop ups.

Message Archiver

If Message Archiver is enabled, Presence Services temporarily stores all incoming and outgoing IMs in a local database. An administrator must provide a reliable storage server to which Presence Services periodically transfers the files from the database. Archived IMs can only be accessed from the SFTP server. The administrator is responsible for providing, on the SFTP server, a secure, password-protected repository for the archived IMs.

Archived IMs are transferred to the SFTP server as a zip file which contains two files:

- A text summary file which identifies the number of entries, and timestamps for the first and last entry
- An XML file which contains the IMs

By default, Message Archiver is disabled. You can enable Message Archiver on System Manager. For more information, see “Enabling Message Archiver”.

Based on the configured upload frequency, Presence Services periodically uses SSH File Transfer Protocol (SFTP) to transfer all IMs to the remote server. If successful, Presence Services removes the IMs from the database.

The first time the file transfer is unsuccessful, Presence Services:

- Raises the major alarm: Message Archive upload failed.
- Stores the date/time of the initial failure.
- Continues to persistently store all IMs in the database.

If a subsequent attempt is successful, Presence Services clears the major alarm and removes the IMs from the database. However, if subsequent attempts are unsuccessful, as long as the upload failure threshold is not reached, the Major alarm remains raised, and Presence Services continues to persistently store all IMs in the database.

After the remote upload failures threshold is reached, Presence Services:

- Clears the major alarm.
- Raises the critical alarm: Message Archiving Disabled.
- Continues to persist the IMs that were previously stored, but does not persist more IMs. Presence Services continues to periodically attempt to transfer IMs to the remote server based on the configured upload frequency. If successful, Presence Services clears the critical alarm, removes the IMs from the database, and resumes persistently storing IMs in the local database.

For more information about major and critical alarms, see “Presence Services alarms”.

The following are some examples why file transfer may be unsuccessful:

- Invalid remote server credentials were configured.
- The remote server is out of service.
- Network connectivity issues.

Note:

If there are no archived messages when the upload timer expires, Presence Services does transfer a zip file. The text summary file indicates that the number of entries is zero, and the timestamps are blank. The XML file contains three lines of "header" information, but no messages.

Example

The upload frequency is 4 hours and the remote upload failures threshold is 5 days.

The first time the file transfer is unsuccessful, Presence Services

- Raises the major alarm: Message Archive upload failed.
- Stores the date/time of the initial failure.
- Continues to persistently store all IMs in the database.

After 4 hours, Presence Services attempts another file transfer to the remote server. If unsuccessful, Presence Services:

- Does not clear the major alarm.
- Continues to persistently store all IMs in the database.
- Continues to attempt a file transfer every 4 hours.

After 31 sequential file transfer failures, the remote upload failures threshold is reached and Presence Services:

- Clears the major alarm: Message Archive upload failed.
- Raises the critical alarm: Message Archiving Disabled.
- Continues to persist the IMs that were previously stored, but does not persist more IMs.

Presence Services continues to attempt a file transfer every 4 hours. If successful, Presence Services:

- Clears the critical alarm: Message Archiving Disabled.
- Removes the previously-stored IMs from the local database.
- Stores all incoming IMs in the local database.

Enabling Message Archiver

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. To enable Message Archiver, navigate to the **Message Archiving Enabled** field within the Instant Messaging group.
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, type `True`.

   Message Archiver is disabled by default.
6. In the **Message Archiving Remote Server Address** field within the Instant Messaging group, type the IP address or Fully Qualified Domain Name (FQDN) of the remote SFTP server.
7. In the **Message Archiving Remote User** field within the Instant Messaging group, type a login name to connect to the remote SFTP server.
8. In the **Message Archiving Remote Password** field within the Instant Messaging group, type a password to connect to the remote SFTP server.
9. In the **Message Archiving Remote Path** field within the Instant Messaging group, type the folder path on the remote SFTP server where Presence Services must transfer the IMs.

   Note:

   The path entered is relative to the home folder of the user and is not an absolute path.

   If you do not specify the path, Presence Services transfers the IMs to the home folder of the user.
10. To change the value of the **Message Archiving Remote Upload Frequency** field within the Instant Messaging group:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, type a value from 1 to 24 hours.

       This value is the frequency at which the Presence server attempts to transfer IMs to the remote SFTP server. The default value is 4 hours.
11. To change the value of the **Message Archiving Remote Upload Failures Threshold** field within the Instant Messaging group:
    a. Select the **Override Default** check box.
    b. In the **Effective Value** field, type a value from 1 to 15 days.

       This value is the number of days of consecutive remote upload failures before the system disables Message Archiver. The default value is 5 days.
12. Click **Commit**.

Multi-tenancy

System Manager supports the ability to assign a tenant ID to a user. For more information about tenant management, see *Administering Avaya Aura® System Manager for Release 7.0.1*.

On enabling Multi-tenancy, Presence Services:

- Blocks presence and IM sharing between users assigned to different tenants.
- Does not notify a user of any presence state changes if the contact is assigned to a different tenant.
- Does not deliver IMs if the sender is assigned to a different tenant than the recipient. Presence Services sends an XMPP message to the sender indicating that the IM has been blocked.

Offline IM Storage

If Offline IM Storage is enabled and a user sends an IM to an offline user, Presence Services:

- Stores the IM in a local database. These IMs survive events such as Presence Services restarts and High Availability failovers.
- Delivers the IM when the offline user logs in to an IM-capable endpoint.

In this situation, a user is considered to be offline only if the user is not logged in to an IM-capable device. If a user manually sets presence state to Offline but remains logged in to an IM-capable device, then Offline IM Storage does not occur. If a user is logged in to multiple IM-capable devices, and then logs out of one device, then Offline IM Storage does not occur. In both of these cases, Presence Services will deliver the IM to the devices of the user.

There is a limit on the number of offline IMs that Presence Services will store for a user.

When Offline IM Storage is enabled, Presence Services does not provide an indication to the sender that the IM is temporarily stored or is delivered to the user.

If Offline IM Storage is disabled and a user sends an IM to an offline user, Presence Services:

- Discards the IM.
- Sends an XMPP message to the sender indicating that service is not available.

If a user has reached the offline IM limit, and another user tries to send an IM to that offline IM user, Presence Services:

- Discards the IM.
- Sends an XMPP message to the sender indicating that service is not available.

By default, Offline IM Storage is enabled, and the Offline IM limit per user is 25. You can administer Offline IM Storage on System Manager.

Configuring Offline IM Storage

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **Instant Messaging** group.
6. In the **Offline IM Storage Enabled** field:
   - To enable Offline IM Storage, verify that the value is `true`.
   - To disable Offline IM Storage, select **Override Default**, and in the **Effective Value** field, type `false`.

   Offline IM Storage is enabled by default.
7. To change the maximum number of Offline IMs stored per user, in the **Offline IM Storage Targeted Maximum IMs per User** field:
   a. Select **Override Default**.
   b. In the **Effective Value** field, enter a new value.
8. Click **Commit**.

Port management

Service Ports are administered on System Manager. When Avaya Breeze™ is installed, Avaya Breeze™ opens platform ports, such as 5061 which is used for SIP signaling. When the Presence Services snap-in is loaded, Presence Services additionally opens ports 5222 and 5269.

- Port 5222 is used by endpoint devices such as one-X® Communicator to establish an XMPP Client to Server connection to Presence Services.
- Port 5269 is used by third-party XMPP servers such as Ignite Realtime Openfire to establish an XMPP Server to Server connection to Presence Services.

Note:

Any changes to the ports will require corresponding changes on endpoints or third-party server. Some endpoints may not support any port besides 5222. It is recommended that these default

ports, 5222 and 5269, not be changed because some endpoint devices and third-party servers are hard-coded to use these ports. If the port values are changed:

- Corresponding changes might be needed on endpoints or third-party servers.
- A Presence Services restart is required.
- For S2S, DNS SRV records need to be updated.

Changing a service port

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™**.
2. Click **Configuration** > **Service Ports**.
3. In the **Service** field, select the Presence Services snap-in.
4. In the **Cluster** field, select the Presence Services cluster.
5. In the **Selected Service Ports** table:
   - To change the XMPP Client to Server port, in the **XMPP_C2S_Port** row, select **Override Default** and enter the new port in the **Effective Port Value** field.
   - To change the XMPP Server to Server port, in the **XMPP_S2S_Port** row, select **Override Default** and enter the new port in the **Effective Port Value** field.
6. Click **Commit**.
7. Restart Presence Services.

Related links

Restarting Presence Services on page 164

Roster size enforcement

Following are the types of users:

- Aura users: Presence and IM services are provided by Presence Services.
- Federated users: Presence and IM services are provided by a third-party server, which is federated with Presence Services.

When two users user A and user B have a presence relationship, the users assume one of three roles:

- Watcher: When user A adds user B to the contact or buddy list by subscribing to presence of user B , user A is a Watcher of user B.
- Presentity: When user A adds user B to the contact or buddy list by subscribing to presence of user B, user B is a Presentity of user A.

- Two-way: When user A adds user B to the contact or buddy list by subscribing to presence of user B, and user B adds user A to the contact or buddy list by subscribing to presence of user A, user A is both a Watcher of user B and a Presentity of user B.

Roster is the list of presence relationships of a user. On Presence Services, the size of roster of a user can be administered. By default, an Aura user can have:

- A maximum of 100 presentities (contacts), that is, 100 relationships where the user role is Watcher or Two-way.
- A maximum of 100 federated watchers, that is, 100 relationships where the user role is Presentity or Two-way, and the watcher is a federated user

In the case where an Aura user has a Two-way relationship with a federated watcher, the relationship is subject to both limits. For instance, if an Aura user has a Two-way relationship with 100 federated users, then both default limits have been reached.

For an Aura H.323 watcher, once an Aura user's maximum number of presentities or contacts has been reached, when the watcher attempts to add another presentity:

- Presence Services rejects the subscription and returns an XMPP error.
- The watching user will not see presence of the presentity.
- The device of watching user may display an error to the user. For more information, consult Avaya endpoint documentation.

For an Aura SIP watcher, once an Aura user's maximum number of presentities or contacts has been reached, when the watcher attempts to add another presentity:

- Presence Services rejects the subscription and returns a SIP error.
- The watching user will not see presence of the presentity.
- The Presence Buddy flag of the contact will be set to No. On System Manager, this is available at **Users** > **User Management** > **Manage Users** > **Contacts** > **Associated Contacts**.
- The device of watching user may display an error to the user. For more information, consult Avaya endpoint documentation.

For a federated SIP or XMPP watcher, once an Aura user's maximum number of federated watchers has been reached, when another federated watcher attempts to subscribe to the Aura user's presence:

- Presence Services rejects the subscription and returns a SIP or XMPP error.
- Presence Services will not send the Aura user's presence information to the federated server.

Refer to the third-party server documentation to determine how the third-party server behaves in this scenario.

Configuring Roster Limit

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Globals or the Service Clusters tab.
4. In the **Service** field, select the Presence Services snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute.
5. Navigate to the **System** group.
6. In the **Roster Limit Maximum Number of Contacts** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter a value between 1 and 1000 that represents the maximum number of Aura and federated presentities that an Aura watcher can add to the contact list.

      The default number of users is 100.
7. In the **Roster Limit: Maximum Number of External Watchers** field:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter a value between 1 and 1000 that represents the maximum number of federated watchers that can add an Aura user to the contact list.

      The default number of users is 100.
8. Click **Commit**.

Restarting Presence Services

Procedure

1. On the System Manager dashboard, navigate to **Elements** > **Avaya Breeze™**.
2. Click **Service Management**.
3. Locate the Presence Services SVAR, and click the **PresenceService** link.

   The system displays the PresenceServices: Avaya Breeze Instance Status page.
4. In the **Service Install Status** column, verify the clusters on which the service is installed.
5. Click **Service Management**, and click the check-box on the left to select the service.
6. Click **Stop**.

   The system displays a confirmation window listing all clusters on which the service is installed.
7. Select the clusters that you want to stop, and click **Stop**.

   On the Service Management page, in the **State** column, the service state will change to **Stopping**.

8. Click the **Refresh Table** icon to refresh the screen.

   Eventually, the **State** column will display **---**, indicating that the service has stopped.

   If you click the **PresenceServices** link, the PresenceServices: Avaya Breeze Instance Status window will open showing the state as **Stopped** in the **Service Install Status** column.

9. Click **Service Management**, and click the check-box on the left to select the service.
10. Click **Start**.

    Note:

    Before starting Presence Services, ensure that **Service Install state** is **Stopped**, as described in Step 8.

    The system displays a confirmation window listing all clusters on which the service is installed.

11. Select the clusters that you want to start, and click **Start**.

    On the Service Management page, in the **State** column, the service state will change to **Starting**.

12. Click the **Refresh Table** icon to refresh the screen.

    Eventually, the **State** column will display **Installed**, indicating that the service has started.

    If you click the **PresenceServices** link, the PresenceServices: Avaya Breeze Instance Status window will open showing the state as **Installed** in the **Service Install Status** column.

    Note:

    When the Presence Services snap-in is restarted or a cluster High Availability event occurs, the system might take up to an hour for some connected endpoints to receive presence updates. The existing subscriptions need to be reestablished. For over-engineered or lightly-loaded Presence deployments, you can shorten this recovery time by shortening the SIP Subscription time.

13. To shorten the SIP Subscription time:

    a. On the System Manager web console, navigate to **Home** > **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.

    b. Click the **Service Globals** or the **Service Cluster** tab, and select the **PresenceServices** service.

    c. In the **System** group, set the **SIP Subscription Time** to the desired setting.

       For the presence deployments with more than 5000 users per server, leave the **SIP Subscription time** at the default value of 4800 seconds.

14. After 2-10 minutes, verify that Presence Services is ready to support Presence and IM.

    See “Verifying that Presence Services snap-in is ready to support Presence and IM”.

Chapter 8: Certificate Management

Adding Subject Alternative Name DNS name to Security Module HTTPS Identify Certificate

About this task

Modify the certificate used for HTTPS communication on each Avaya Breeze™ Server in the Presence Services Cluster to include an subject alternative name (SAN) of type DNS Name.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Breeze™ instance.
3. From the **More Actions** menu, select **Configure Identity Certificates**.
4. Select the Security Module HTTPS service name, and click **Replace**.
5. Select **RSA for Key Algorithm**.
6. In the **Key Size** field, enter `2048`.
7. In the **Subject Alternative Name** field, select the **DNS Name** check box.
8. Add the Presence Services Cluster FQDN to the **DNS Name** field.
9. Click **Commit**.
10. Repeat Step 2 to Step 9 for each Avaya Breeze™ in the cluster.
11. Restart Presence Services.

    For more information, see the “Restarting Presence Services” section.

Add Subject Alternative Name DNS name and Other Name (XMPP Address) to WebSphere Identify Certificate

About this task

Modify the certificate used for XMPP communication on each Avaya Breeze™ Server in the Presence Services Cluster to include a subject alternative name (SAN) of type DNS Name and Other Name.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Inventory** > **Manage Elements**.
2. Select an Avaya Breeze™ instance.
3. From the **More Actions** menu, select **Configure Identity Certificates**.
4. Select the WebSphere service name, and click **Replace**.
5. Select **RSA for Key Algorithm**.
6. In the **Key Size** field, enter `2048`.
7. In the **Subject Alternative Name** field, select the **DNS Name** check box.
8. Add the Presence Services Cluster FQDN to the **DNS Name** field.
9. For the **Subject Alternative Name** field, select the **XmppAddr** check box.
10. Add all Presence Services XMPP domains to the **XmppAddr** field in a comma-separated format.
11. Click **Commit**.
12. Repeat Step 2 to Step 11 for each Avaya Breeze™ in the cluster.
13. Restart Presence Services.

    For more information, see the “Restarting Presence Services” section.

Exporting Openfire Certificate (Linux)

About this task

Export the Openfire self-signed certificate used on the Linux based Openfire server. This procedure uses the sample values in the “Key customer configuration information” section.

Procedure

1. On Linux, open an xterm.

2. Change directories to `<Openfire install dir>/openfire/resources/security`, where <Openfire install dir> is the directory where Openfire is installed.
3. Run the following to use the keytool command to export the certificate: `keytool -export -alias <of domain>_rsa -file openfire.cer -keystore keystore`.

   The keytool command is provided in the JDK distribution of Java and sometimes with Openfire in `<Openfire install dir>/jre/bin`.
4. Save the `openfire.cer` file to be imported.

Exporting Openfire Certificate (Windows)

About this task

Export the Openfire self-signed certificate used on the Windows based Openfire server. This procedure uses the sample values in the “Key customer configuration information” section.

Procedure

1. On Windows, open a DOS prompt.
2. Change the directories to `<Openfire install dir>\openfire\resources\security`, where `<Openfire install dir>` is the directory where Openfire is installed.
3. Run the following to use the keytool command to export the certificate: `keytool -export -alias <of domain>_rsa -file openfire.cer -keystore keystore`.

   The keytool command is provided in the JDK distribution of Java and sometimes with Openfire in `<Openfire install dir>\jre\bin`.
4. If the system prompts for the password, enter the keystore password.
5. Save the `openfire.cer` file to be imported.

Importing certificate into Cluster Truststore

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the cluster.
3. From the **Cluster Management** menu, select **Install Trust Certificate (All Avaya Breeze Instances)**.
4. On the next page, select **Browse**.

5. In the **File Explorer** window, select the Certificate file in DER or PEM format.
6. Click **Retrieve Certificate**.
7. Click **Commit**.
8. Navigate to **Home** > **Elements** > **Avaya Breeze™** > **Service Management**.
9. Select the service.
10. Click **Stop**.
11. Select the cluster, and click **Stop**.
12. Refresh the page until the service is stopped.
13. Click **Start**.
14. Select the cluster and click **Start**.
15. Restart Presence Services.

    For more information, see the “Restarting Presence Services” section.

Importing System Manager root CA certificate into Openfire Truststore (Windows)

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Security** > **Certificates**.
2. Click **Authority**.
3. Click **CA Structure & CRLs**.
4. Click **Download JKS file**.
5. When prompted, enter a password to protect the JKS file.
6. Change directories to `<Openfire install dir>\openfire\resources\security`, where <Openfire install dir> is the directory where Openfire is installed.
7. To determine the alias of the System Manager root CA, run the following: `<Openfire install dir>\openfire\resources\security\keytool -list -v -keystore SystemManagerCA.cacert.jks`.

   ```
   Enter keystore password: <admin password>
   Keystore type: JKS
   Keystore provider: SUN
   Your keystore contains 1 entry
   Alias name: systemmanagerca
   ```

   The keytool command is provided in the JDK distribution of Java and sometimes with Openfire in the `<Openfire install dir>\jre\bin`.

8. Export the certificate from the System Manager keystore file using the alias determined in Step 7.

```
C:\<Openfire install dir>\openfire\resources\security> keytool -export -alias
systemmanagerca -file SystemManagerCA.cacert.der -keystore
SystemManagerCA.cacert.jks
Enter keystore password: <enter password created in Step 5>
Certificate stored in file <SystemManagerCA.cacert.der>
```

9. Import the certificate into the Openfire truststore using a descriptive alias.

   For example, `SystemManagerRootCA`.

```
<Openfire install dir>\openfire\resources\security\keytool -import -alias
SystemManagerRootCA -file SystemManagerCA.cacert.der -keystore <Openfire install
dir>\openfire\resources\security\truststore
Enter keystore password: <enter the Openfire password>  (Default is changeit)
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Importing System Manager root CA certificate into Openfire Truststore (Linux)

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Security** > **Certificates**.
2. Click **Authority**.
3. Click **CA Structure & CRLs**.
4. Click **Download JKS file**.
5. When prompted, enter a password to protect the JKS file.
6. Change directories to `<Openfire install dir>/openfire/resources/security`, where <Openfire install dir> is the directory where Openfire is installed.
7. To determine the alias of the System Manager root CA, run the following: `keytool -list -v -keystore SystemManagerCA.cacert.jks`.

```
Enter keystore password: <admin password>
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: systemmanagerca
```

   The keytool command is provided in the JDK distribution of Java and sometimes with Openfire in the `<Openfire install dir>/jre/bin`.

8. Export the certificate from the System Manager keystore file using the alias determined in Step 7.

```
keytool -export -alias systemmanagerca -file SystemManagerCA.cacert.der -keystore
SystemManagerCA.cacert.jks
```

```
Enter keystore password: <enter password created in Step 5>
Certificate stored in file <SystemManagerCA.cacert.der>
```

9. Import the certificate into the Openfire truststore using a descriptive alias.

   For example, `SystemManagerRootCA`.

```
keytool -import -alias SystemManagerRootCA -file SystemManagerCA.cacert.der -
keystore <Openfire install dir>/openfire/resources/security/truststore
Enter keystore password: <enter the Openfire password>  (Default is changeit)
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Creating Entity Profile on System Manager

About this task

Create an Entity profile on System Manager to be used to signed an external certificate signing request (CSR).

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. On System Manager, navigate to **Home** > **Services** > **Security** > **Certificates**.
2. Click **Authority**.
3. Click **Add End Entity**.
4. Add the following information:
   - End Entity Profile: `EXTERNAL_CSR_PROFILE`
   - Username
   - Password or Enrollment Code
   - Confirm Password
   - CN, Common name: *Of name*
   - O, Organization: *company name*
   - C, Country: *country code*
   - OU, Organization Unit: *group name*
   - L, Locality: *city name*
   - ST, State or Province: *city or province name*
   - Certificate Profile: `ID_CLIENT_SERVER`
   - CA: `tmdefaultca`
   - Token: *User Generated*

Use the same values used in the “Generating a Certificate Signing Request on Openfire” section.

5. Click **Add**.

Generating a certificate signing request on the Openfire server

About this task

Generate a certificate signing request (CSR) on the Openfire server.

This procedure uses the sample values in the “Table 7: Single-server Cluster Federated with Ignite Openfire example values” section.

Procedure

1. On the Openfire server, navigate to **Server** > **Server Settings** > **Server Certificates**.
2. In Signing request, click **Click here to update the issuer information**.
3. Add the following information:
   - Name: `OF domain`
   - Organizational Unit: *group name*
   - Organization: *company name*
   - City: *city name*
   - State: *state or province name*
   - Country Code: *country code*

   Use the same values used in the “Creating Entity Profile on System Manager” section.
4. Click **Update Information**.
5. Copy the CSR for the RSA algorithm in to a text editor.

Signing the Openfire certificate signing request (CSR) on System Manager

Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Security** > **Certificates** > **Authority**.
2. Select **Public Web**.

3. On the next page, click **Create Certificate from CSR**, and enter the following information:
   - Username: *username*
   - Enrollment code: *password*

   username and *password* are defined in the “Creating Entity Profile on System Manager” section.
4. Paste in the certificate signing request from Openfire previously saved in a text editor in the “Generating a Certificate Signing Request (CSR) on Openfire” section.
5. Select **PEM - full certificate chain** and click **OK**.
6. Save the resulting PEM file.

Installing the System Manager CA and Signed Openfire Certificate on Openfire

Procedure

1. On the Openfire server, navigate to **Server** > **Server Settings** > **Server Certificates**.
2. Using a text editor, open the PEM file that you created in the “Signing the Openfire CSR on System Manager” section.
3. Copy and paste the System Manager CA certificate, and click **Save**.
4. Copy and Paste the *OF domain* certificate and click **Save**.
5. Delete the DSA pending request.
6. Click **Click here to restart HTTP server**.
7. Log in to the Openfire server.
8. On the Openfire server, navigate to **Server** > **Server Settings** > **Server Certificates**.
9. Click **Click here to generate self-signed certificates** to generate a self-signed DSA certificate.

Retrieving a System Manager CA signed Certificate

Procedure

1. On System Manager, navigate to **Home** > **Services** > **Security** > **Certificates**.
2. Click **Authority**.
3. Click **Search End Entities**.

4. In the **Search end entity with username** field, enter the username of the Entity Profile used to sign the certificate.
5. Click **View_Certificates**.
6. Click **Download PEM file**.
7. Save the PEM file.

Checklist for generating new identity certificate signed by System Manager

This checklist is used to generate a Certificate Signing Request (CSR) and associated private key to obtain a signed Identity certificate from the System Manager.

No.	Task	Reference	✔
1	Create a Certificate Signing Request.	Creating a Certificate Signing Request on page 174	
2	Create an end entity.	Creating an end entity on System Manager on page 175	
3	Create the signed identity certificate using the CSR.	Creating the Signed Identity Certificate using the CSR on page 176	

Creating a Certificate Signing Request

About this task

The Certificate Signing Request (CSR) file is created separately on either a Windows or Linux system.

Procedure

To generate the CSR file, enter the following `OpenSSL` command line tool:

```
openssl req -out <csr-file.csr> -new -newkey rsa:2048 -nodes keyout <my-private-key-file.pem>
```

Example

The following is a sample session:

```
$ openssl req -out csrFile.csr -new -newkey rsa:2048 -nodes -keyout myPrivateKey.pem
Generating a 2048 bit RSA private key
....+++
.....................+++
writing new private key to 'myPrivateKey.pem'
```

```
-----
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CA
State or Province Name (full name) [Berkshire]:Ontario
Locality Name (eg, city) [Newbury]:Belleville
Organization Name (eg, company) [My Company Ltd]:Avaya
Organizational Unit Name (eg, section) []:Avaya
Common Name (eg, your name or your server's hostname) []:fqdn.ca.avaya.com
Email Address []:


Please enter the following 'extra' attributesto be sent with your certificate request
A challenge password []:
An optional company name []:Avaya
```

You should now see a CSR and private key file in your test directory:

```
$ ls -l
```

```
total 6
-rw-r--r-- 1 user group 1045 Apr 20 11:35 csrFile.csr
-rw-r--r-- 1 user group 1679 Apr 20 11:35 myPrivateKey.pem
```

Creating an end entity on System Manager

Procedure

1. Login to System Manager as administrator.
2. Navigate to **Services** > **Security** > **Certificates** > **Authority**.
3. Select **RA Functions**.
4. Add **End Entity**.
5. Select **INBOUND_OUTBOUND_TLS** in the **End Entity Profile** field.
6. Enter **User name** and **Password** .

   The user name and password must be new and will be used in the “Creating the Signed Identity Certificate using the CSR” section.
7. Complete the fields that you want in the certificate.
8. Enter the appropriate values in the **CN** and **SAN** fields.
9. In the **Certificate Profile** field, select **ID_CLIENT_SERVER**.
10. In the **CA** field, select **tmdefaultca**.
11. In the **Token** field, select **User generated**.
12. Click **Add**

13. Scroll down to the bottom of the page to verify that the End Entity is added successfully.

Creating the Signed Identity Certificate using the CSR

Procedure

1. On the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
2. Click **Public Web**.
3. On the public EJBCA page:
   a. Click **Create Certificate from CSR** in the **Enroll** menu.
   b. Enter the **User name** and **Password**.

      These values should be the same that you used while creating the end entity earlier.
   c. Click **Browse** to retrieve the CSR file created earlier.
   d. Set the **Result type** field to **PEM - certificate only**.
   e. Click **OK**.
   f. Save the signed identity certificate file to your local computer.

OpenSSL command to view the signed certificate

About this task

The **OpenSSL** command line tool can be used to verify or review the identity certificate contents.

Example

```
$ openssl x509 -in newIdentiyCert.pem -text -noout
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    04:80:82:da:40:b9:db:fe
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=System Manager CA, OU=MGMT, O=AVAYA
  Validity
  Not Before: Apr 20 16:24:23 2016 GMT
  Not After : Apr 20 16:24:23 2018 GMT
Subject: CN=fqdn.ca.avaya.com, OU=SDP, O=AVAYA, L=Belleville, ST=Ontario,
C=US
   Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
   RSA Public Key: (2048 bit)
       Modulus (2048 bit):
          00:ba:3c:b2:36:33:67:dc:ff:a0:6b:7a:1d:c7:77:
          <snip>
          ef:95:be:50:23:61:af:9d:e0:4f:37:58:b2:ac:a6:
          20:d1
```

```
          Exponent: 65537 (0x10001)
       X509v3 extensions:
      X509v3 Subject Key Identifier:
         8C:17:08:0F:AF:B5:FD:7E:D6:5E:02:DD:71:A2:97:E5:F2:40:B8:36
      X509v3 Basic Constraints: critical
       CA:FALSE
      X509v3 Authority Key Identifier:
         keyid:A4:C5:C0:96:86:60:21:3A:60:3A:58:56:6B:97:70:DD:C1:51:30:0B


           X509v3 Key Usage: critical
          Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key
Agreement
              X509v3 Extended Key Usage:
                  TLS Web Server Authentication, TLS Web Client Authentication
              X509v3 Subject Alternative Name:
                 DNS:san1.ca.avaya.com
   Signature Algorithm: sha256WithRSAEncryption
     2b:07:d9:aa:0d:5b:5d:aa:d9:07:cc:6b:a3:7b:7f:9b:5c:2e:
     <snip>
     5a:d4:f1:cd:ab:a0:f4:c8:86:b6:4a:c6:22:45:07:d5:86:d7:
     49:03:c6:63
```

Generating new identity certificate from a third-party CA

About this task

The certificate Signing Request (CSR) file is created separately on either a Windows or Linux system.

Procedure

1. To generate the CSR file, enter the following `OpenSSL` command line tool:

   ```
   openssl req -out <csr-file.csr> -new -newkey rsa:2048 -nodes keyout
   <my-private-key-file.pem>
   ```

   Note:

   The **openssl** command doesn't prompt for the **SAN** fields.

2. Send the CSR to the third-party CA for signing.

   Note:

   Some third-party vendors allow uploading of CSR files and will also prompt for additional **SAN** fields.

3. The third-party vendor will return the signed certificate.

Presence components and identity certificates

The following table provides which identity certificates are used by various Presence components.

Presence component	Connection type	Identity certificate	Comments
Presence Services 7.x to Presence Services 7.x Federation	server through System Manager	SecurityModuleSIP	Asset module presents the **SecurityModuleSIP** identity certificate in the server hello during TLS negotiation.
Lync2013 Federation	server through System Manager	SecurityModuleSIP	Asset module presents the **SecurityModuleSIP** identity certificate in the server hello during TLS negotiation.
Openfire Federation	server through local XMPP port	Websphere	Presence Services presents the Webshere identity certificate in the 'server hello' during TLS negotiation.
Jabber Federation	server through local XMPP port	Websphere	Presence Services presents the Webshere identity certificate in the 'server hello' during TLS negotiation.
Presence Services 6.x Federation	server trough local XMPP port	Websphere	Presence Services presents the Webshere identity certificate in the 'server hello' during TLS negotiation.
NextPlane Federation	server through local XMPP port	Websphere	Presence Services presents the Webshere identity certificate in the 'server hello'

Table continues…

Presence component	Connection type	Identity certificate	Comments
			during TLS negotiation.
AMM	server through REST through load-balancer	SecurityModuleHTTP	Internal HTTP proxy module presents the **SecurityModuleHTTP**identity certificate in the 'server hello' during TLS negotiation.
WebServices / REST	server through load-balancer	SecurityModuleHTTP	Internal HTTP proxy module presents the **SecurityModuleHTTP**identity certificate in the 'server hello' during TLS negotiation.
Client to Server XMPP	server (through local XMPP port)	Websphere	No certificate checking

Installing far-end Trust Certificates in Avaya Breeze™

About this task

Many Presence components or features require **Trust Certificates** to be installed into the trust store on the Avaya Breeze™ to allow the feature software to connect securely to other servers on the network.

For example: AES and Exchange collectors, different types of SIP federation, and different types of XMPP federation.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze** > **Cluster Administration**.
2. Select the Avaya Breeze™ cluster from the list.
3. Click **Certificate Management**, and select **Install Trust Certificate** (all Avaya Breeze™ instances).
4. On the Install Trust Certificate page.
    a. Ensure the **Select Store Type to install trusted certificate** option is set to **All**.

b. Click **Browse** and navigate to the trust certificate file.
c. Click **Retrieve Certificate** to upload the selected file to System Manager.
d. Click **Commit**.

Chapter 9: Service Attributes

Service Attributes

Presence Services functionality is administered through Service Attributes on System Manager at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**. These attributes can be defined at a system level using the Service Globals tab, and the attributes can be selectively overridden at a cluster level using the Service Clusters tab. In Presence Services 7.0, only one attribute, that is Access Control Policy, can be administered on a Service Profile basis.

Note the following for the XMPP Federation service attributes:

- There are four instances of the XMPP Federation group: XMPP Federation 1, XMPP Federation 2, XMPP Federation 3, and XMPP Federation 4.
- Different XMPP Federation group instances should be administered if Presence Services is federated with more than one XMPP server, and any of the following conditions are met:
  - An administrator wants the ability to enable or disable the federations independently. For instance, Presence Services is federated with two Ignite Realtime Openfire servers, and an administrator wants the ability to enable federation to one server while disabling federation to the other server.
  - Presence Services is federated to different kinds of XMPP servers. For instance, Presence Services is federated with an Ignite Realtime Openfire server and a pre-7.0 Presence Services server.
  - An administrator wants the ability to configure the federations independently. For instance, Presence Services is federated with two Ignite Realtime Openfire servers, one using TLS and the other using TCP.

Presence Services Service Attributes

Table 20: Presence Services Service Attributes

Group	Service Attribute	Description	Reference
Access Control	Access Control Policy	Access control policy for user (Allow, Block, Confirm)	Access control policy on page 49

Table continues…

Group	Service Attribute	Description	Reference
AES Collector	AES Collector Enabled	Set True/False to enable/disable the AES collector. When enabled, the AES Server Username and Password must be configured.	AES Collector on page 50
	AES Server Username *	Username the AES collector will use when connecting to AES servers (* requires collector restart)	
	AES Server Password *	Password the AES collector will use when connecting to AES servers (* requires collector restart)	
	Publish DND Status *	Enable AES collector to publish DND status (True/False) (* requires collector restart)	
	Away Timer (mins) *	Time after onhook to change state to away (Range 0 - 1440m) (* requires collector restart)	
	Out-Of-Office Timer (mins) *	Time after onhook to change state to Out-Of-Office (Range 0 - 10080m) (* requires collector restart)	
Avaya Multimedia Messaging	AMM Integration enabled	Set True/False to enable/disable Avaya Multimedia Messaging integration. Avaya Multimedia Messaging integration enables forking messages to and processing messages from Avaya Multimedia Messaging. The default value is false.	—

Table continues…

Group	Service Attribute	Description	Reference
	Web service path of the Avaya Multimedia Messaging Server	The web service path of the Avaya Multimedia Messaging Server. For more information, see *Deploying Avaya Multimedia Messaging*.	
	Trusted hostnames of Avaya Multimedia Messaging Server(s)	Comma-separated list of trusted hostnames of the Avaya Multimedia Messaging Server(s). For more information, see *Deploying Avaya Multimedia Messaging*.	
Domino Collector	Domino Collector Enabled	Set True/False to enable/disable the Domino calendar collector. When enabled, the Server Username, Password and Uri must be configured.	Domino Collector on page 56
	Domino Server Web Service URI *	Resource Identifier of the Domino Web Service (* requires collector restart)	
	Domino Server Username *	Username the Domino collector will use when connecting to Domino server (* requires collector restart)	
	Domino Server Password *	Password the Domino collector will use when connecting to Domino server (* requires collector restart)	
	Domino Calendar Information Polling Period *	Calendar information collection interval in minutes. (Must be greater than 0) (* requires collector restart)	
	Domino Calendar Request Rate *	Calendar request per minute rate to the calendar server. (Must be greater than 0) (*	

Table continues…

Group	Service Attribute	Description	Reference
		requires collector restart)	
	Domino Out-Of-Office Information Polling Period *	Out-Of-Office information collection interval in minutes. (Must be greater than 0) (* requires collector restart)	
	Domino Out-Of-Office Request Rate *	Out-Of-Office request per minute rate to the calendar server. (Must be greater than 0) (* requires collector restart)	
	Domino Publishing Period *	Collector publish to Presence Services core interval in minutes. (Must be greater than 0) (* requires collector restart)	
Exchange Collector	Exchange Collector Enabled	Set True/False to enable/disable the Exchange calendar collector. When enabled, the Server Username, Password and Uri must be configured.	Exchange Collector on page 53
	Exchange Server URI *	Resource Identifier of the Exchange Server (* requires collector restart)	
	Exchange Server Username *	Username the Exchange collector will use when connecting to Exchange server (* requires collector restart)	
	Exchange Server Password *	Password the Exchange collector will use when connecting to Exchange server (* requires collector restart)	

Table continues…

Group	Service Attribute	Description	Reference
	Exchange Calendar Information Polling Period *	Calendar information collection interval in minutes. (Must be greater than 0) (* requires collector restart)	
	Exchange Calendar Request Rate *	Calendar request per minute rate to the calendar server. (Must be greater than 0) (* requires collector restart)	
	Exchange Out-Of-Office Information Polling Period *	Out-Of-Office information collection interval in minutes. (Must be greater than 0) (* requires collector restart)	
	Exchange Out-Of-Office Request Rate *	Out-Of-Office request per minute rate to the calendar server. (Must be greater than 0) (* requires collector restart)	
	Exchange Publishing Period *	Collector publish to Presence Services core interval in minutes. (Must be greater than 0) (* requires collector restart)	
Instant Messaging	Message Archiving Enabled	Enable message archiving for IM's (True/ False)	Message Archiver on page 157
	Message Archiving Remote Server Address	Server address of the remote SFTP site to upload archived IM's	
	Message Archiving Remote User	Login name of the remote SFTP site to upload archived IM's	
	Message Archiving Remote Password	Password of the remote SFTP site to upload archived IM's	
	Message Archiving Remote Path	Directory path on the remote SFTP site to upload archived IM's.	

Table continues…

Group	Service Attribute	Description	Reference
		This path is relative to the home directory of the user. If blank, default will be the home directory of the user.	
	Message Archiving Remote Upload Frequency	Frequency (1-24 hours) to upload archived IM's	
	Message Archiving Remote Upload Failures Threshold	The number of days (1-15) of consecutive remote upload failures before Message Archiver is disabled	
	Offline IM Storage Enabled	Enable storing IMs sent to offline users (True/False)	Offline IM Storage on page 160
	Offline IM Storage Targeted Maximum IMs Per User	The maximum number of IMs that will be stored when a user is offline on a per user basis (min 25, max 100). This may be exceeded during heavy traffic loads	
	Block IMs for users in Do-Not-Disturb (DND) state	Enable blocking and delayed delivery of IMs to recipients in Do-Not-Disturb (DND) state (True/False)	IM Blocking in Do Not Disturb state on page 139
Inter-PS Federation	Inter-PS Federation Enabled	Set True/False to enable/disable Inter-PS federation. When enabled, the Inter-PS federation domain list must be configured.	Inter-PS federation on page 105
	Inter-PS Domain Name List	Comma separated list of federated Presence Server domains (example: alphaps.eg.com,betaps.eg.com).	
Lync Federation	Lync Federation Enabled	Set True/False to enable/disable Lync federation. When enabled, the Lync	Lync federation on page 81

Table continues…

Group	Service Attribute	Description	Reference
		federated domain list must be configured.	
	Lync Domain Name List	Comma separated list of federated Lync domains (example: lync1.eg.com,lync2.eg.com).	
System	Number of Users	Intended number of users on this cluster. Valid range: [500-250000]	Planning on page 18 Administering Presence Services System service attributes on page 30
	High Availability	Enable High Availability for Presence/IM (True/False)	
	SIP Subscription Time	SIP Subscription Time in Seconds, minimum is 600 (10 minutes) and maximum is 43200 (12 hours)	—
	Enable Inter-Domain Presence and IM	Enables Presence and IMs to be exchanged between Aura users in different, non-federated, Aura Domains. When disabled, users in different domains will be unable to exchange Presence and IMs.	—
	Roster Limit Maximum Number of Contacts	The maximum number of contacts (1-1000) a user can subscribe for presence. When the maximum is reached, this user cannot subscribe to any more users for presence.	—
	Roster Limit: Maximum Number of External Watchers	The maximum number of unique external subscribers (1-1000) that can watch a particular user's presence. When the maximum is reached, no other external users	—

Table continues…

Group	Service Attribute	Description	Reference
		can subscribe to that user's presence.	
	Enable Sip Call Processing Time Log	Enables logging of SIP call processing time, for debug use only	—
XMPP Federation 1	Component Enabled 1	Set True/False to enable/disable XMPP federation. When enabled, both server to server port and federation domain list must be configured.	XMPP federation on page 110
	Enable Secure Communication (TLS) 1	Enable or disable XMPP Federation secure communication (TLS). Default is secure mode.	
	Federation Type 1	Federation server type. Supported servers are Openfire, Presence Services or Cisco Jabber. Valid inputs are openfire, avaya or cisco. Case insensitive.	
	XMPP Federation Domain List 1	Federated XMPP domain name list separated by comma (example: pres.feddomain.com,pres.feddomain.ca.avaya.com). Leave it empty if XMPP federation is disabled.	
XMPP Federation 2	Component Enabled 2	Set True/False to enable/disable XMPP federation. When enabled, both server to server port and federation domain list must be configured.	XMPP federation on page 110
	Enable Secure Communication (TLS) 2	Enable or disable XMPP Federation secure communication (TLS). Default is secure mode.	

Table continues…

Group	Service Attribute	Description	Reference
	Federation Type 2	Federation server type. Supported servers are Openfire, Presence Services or Cisco Jabber. Valid inputs are openfire, avaya or cisco. Case insensitive.	
	XMPP Federation Domain List 2	Federated XMPP domain name list separated by comma (example: pres.feddomain.com,pres.feddomain.ca.avaya.com). Leave it empty if XMPP federation is disabled.	
XMPP Federation 3	Component Enabled 3	Set True/False to enable/disable XMPP federation. When enabled, both server to server port and federation domain list must be configured.	XMPP federation on page 110
	Enable Secure Communication (TLS) 3	Enable or disable XMPP Federation secure communication (TLS). Default is secure mode.	
	Federation Type 3	Federation server type. Supported servers are Openfire, Presence Services or Cisco Jabber. Valid inputs are openfire, avaya or cisco. Case insensitive.	
	XMPP Federation Domain List 3	Federated XMPP domain name list separated by comma (example: pres.feddomain.com,pres.feddomain.ca.avaya.com). Leave it empty if XMPP federation is disabled.	
XMPP Federation 4	Component Enabled 4	Set True/False to enable/disable XMPP	XMPP federation on page 110

Table continues…

Group	Service Attribute	Description	Reference
		federation. When enabled, both server to server port and federation domain list must be configured.	
	Enable Secure Communication (TLS) 4	Enable or disable XMPP Federation secure communication (TLS). Default is secure mode.	
	Federation Type 4	Federation server type. Supported servers are Openfire, Presence Services or Cisco Jabber. Valid inputs are openfire, avaya or cisco. Case insensitive.	
	XMPP Federation Domain List 4	Federated XMPP domain name list separated by comma (example: pres.feddomain.com,pres.feddomain.ca.avaya.com). Leave it empty if XMPP federation is disabled.	

Chapter 10: User and device administration

User and device administration

This chapter describes:

- User administration on System Manager.
- DNS administration for devices.
- Certificate management for devices.

Note:

The steps in the procedures vary depending on:

- The type of device that the user logs in to.
- The mode that the user selects when logging into the device.

Categories of Presence/IM devices

Avaya supports four categories of Presence/IM devices:

- Category 1: Next-generation SIP mode
- Category 2: SIP mode
- Category 3: H.323 mode
- Category 4: Non-Presence/IM capable

Category 1 devices:

Category 1 devices are strongly recommended because the devices:

- Are more resilient to network or server outages.
- Support Presence/IM features such as High Availability and Geo Redundancy.
- Support higher overall capacity in a multi-node Presence Services cluster deployment as the resources are used more efficiently.
- Do not need an end user to administer Presence Services information on device.
- Do not need an end user to change device settings if a user's home Presence Services cluster changes.

The Category 1 devices do not need an end user to administer a Presence Services address or an Avaya Presence/IM communication address. Instead, the device automatically gets this information

through Personal Profile Manager (PPM) web service of Session Manager. The Presence Services address is returned as a Fully Qualified Domain Name (FQDN), which the device resolves to one or more IP addresses using DNS. FQDN addressing is required for Presence Services features such as High Availability and Geo Redundancy.

Example:

- Avaya one-X® Communicator SIP 6.2.6 or later

Category 2 devices:

Category 2 devices require an end user to administer a Presence Services address, and an Avaya Presence/IM communication address. The Presence Services address is usually administered as an IP address. The end user logs in using SIP mode.

Example:

- Avaya Communicator for Windows 2
- Avaya one-X® Communicator SIP pre-6.2.6

Category 3 devices:

Category 3 devices require an end user to administer a Presence Services address, and an Avaya Presence/IM communication address. The Presence Services address is usually administered as an IP address. The end user logs in using H.323 mode.

Example:

- Avaya one-X® Communicator H.323

Category 4 devices:

Category 4 devices are typically hard desk phones that:

- Do not support the SIP or XMPP protocol for presence and IM.
- Do not have the ability to exchange messages with other devices.
- Do not have the ability to publish their own presence state information.

Example:

- Avaya 9600 series H.323 phones
- Avaya 96X1 series H.323 phones
- Avaya digital and analog deskphones

Checklist for configuring Presence/IM users

In the following table:

- **M** indicates that the task is mandatory for the device.
- **O** indicates that the task is optional for the device.
- **—** indicates that the task is not applicable for the device.

Step 2 to Step 5 can be performed together or as independent steps.

Step 11 to Step 15 can be performed together or as independent steps.

Table 21: Checklist for configuring Presence/IM users

No.	Task	Device category				Reference
		1	2	3	4	
1	Configure Presence/IM routing domain on System Manager.	M	M	M	M	Configuring Presence/IM routing domain on System Manager on page 194
2	Assign Communication Profile Password to user on System Manager.	M	M	M	M	Assigning Communication Profile Password to a user on System Manager on page 195
3	Assign Avaya Presence/IM communication address to user on System Manager.	M	M	M	M	Assigning Avaya Presence/IM communication address to user on System Manager on page 105
4	Assign Presence Profile to user on System Manager.	M	M	M	M	Assigning Presence Profile to a user on System Manager on page 196
5	Enable Application Enablement Services collection for user on System Manager.	—	—	—	M	Enabling Application Enablement Services collection for a user on System Manager on page 197
6	Administer DNS A records to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP addresses.	M	O	O	—	—
7	Export certificate chain that signs Session Manager identity.	M	M	—	—	Exporting certificate chain that signs the Session Manager identity on page 198
8	Import certificate chain that signs Session Manager identity into device truststore.	M	M	—	—	Importing certificate chain that signs Session Manager identity into device truststore on page 199
9	Export certificate chain that signs Presence Services identity.	M	M	M	—	Exporting certificate chain that signs the Presence Services identity on page 204
10	Import certificate chain that signs Presence Services identity into device truststore.	M	M	M	—	Importing certificate chain that signs the Presence Services identity into device truststore on page 205
11	Administer Presence and IM on the device.	M	M	M	—	Checklist for administering Presence and IM on a device on page 211

Configuring Presence/IM routing domain on System Manager

About this task

On System Manager, users are configured with communication addresses, which are unique identifiers within a solution. A communication address is composed of a user part (referred to as handle on System Manager) and domain part.

Within the Presence/IM solution, a user is uniquely identified by an Avaya Presence/IM communication address, which is composed of a user part, and a Presence/IM domain part. The Presence/IM domain may be the same as a user's SIP domain, or it may be different.

For example, if the same domain is used for both SIP and Presence/IM, a user may be assigned the following communication addresses:

- Avaya SIP communication address set to `user1@domainA.com`
- Avaya Presence/IM communication address set to `user1@domainA.com`

For example, if different domains are used for SIP and Presence/IM, a user may be assigned the following communication addresses:

- Avaya SIP communication address set to `user1@domainB.com`
- Avaya Presence/IM communication address set to `user1@domainC.com`

Presence/IM domains are configured on System Manager with type as SIP. Presence Services supports multiple Presence/IM domains.

For example, there could be two users with Avaya Presence/IM communication addresses in different domains on System Manager:

- User 2 with Avaya Presence/IM communication address set to `user2@domainD.com`
- User 3 with Avaya Presence/IM communication address set to `user3@domainE.com`

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing**.

   The system displays the Introduction to Network Routing Policy page.

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

   The system displays the Domain Management page.

3. Click **New**.
4. In the **Name** field, type the `Presence/IM domain name`.
5. In the **Type** field, select `sip`.
6. Click **Commit** to save the changes.

Assigning Communication Profile Password to a user on System Manager

Before you begin

The user must already exist on System Manager at **Users** > **User Management**.

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management**.

   The system displays the User Management page.
2. In the navigation pane, click **Manage Users**.
3. Select the user, and click **Edit** .

   The system displays the User Profile Edit page.
4. Click the **Communication Profile** tab.
5. Select **Communication Profile** with the **Default** check box enabled.
6. To the right of the **Communication Profile Password**, select **Edit** .
7. In the **Communication Profile Password** field, enter the user password.
8. In the **Confirm Password** field, reenter the user password.
9. Click **Commit** to save the changes.

Assigning Avaya Presence/IM communication address to user on System Manager

About this task

An Avaya Presence/IM communication address is a unique presence identifier for a user. Servers, devices, and other users use this identifier to exchange IM and presence information with the user.

Before you begin

A user must already exist on System Manager at **Users** > **User Management**.

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management**

   The system displays the User Management page.
2. In the navigation pane, click **Manage Users**.
3. Select the user, and click **Edit**.

   The system displays the User Profile Edit page.

4. Click the **Communication Profile** tab.
5. Select the **Communication Profile** with the **Default** check box enabled.
6. In the **Communication Address** section, click **New**.
7. In the **Type** field, select **Avaya Presence/IM**.
8. In the **Fully Qualified Address** section:
   - In the first field, type the user part of the Avaya Presence/IM communication address.
   - In the second field, select the **Presence/IM routing** domain that was defined in “Configuring Presence/IM routing domain on System Manager”.
9. Click **Add**.
10. Click **Commit** to save the changes.

Note:

The Avaya Presence/IM communication address must be administered on the default Communication Profile.

Assigning Presence Profile to a user on System Manager

Before you begin

The user must already exist on System Manager at **Users** > **User Management** with an assigned **Avaya Presence/IM communication address**.

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management**.

   The system displays the User Management page.
2. In the navigation pane, click **Manage Users**.
3. Select the user, and click **Edit**.

   The system displays the User Profile Edit page.
4. Click the **Communication Profile** tab.
5. Select the **communication profile** with the **Default** check box enabled.
6. Select the **Presence Profile** check-box.

   The system displays the **Presence Profile** fields.
7. In the **System** field, from the drop-down list, select home Presence Services cluster of the user.

   This drop-down list is populated based on all Presence Services Managed Elements. For more information, see “Administering Presence Services on Avaya Breeze™ Managed Element”.

The system automatically populates the **SIP Entity** field, and the **IM Gateway SIP Entity** field.

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

Note:

The Presence Profile must be administered on the default Communication Profile.

Enabling Application Enablement Services collection for a user on System Manager

Before you begin

The user must already exist on System Manager at **Users** > **User Management** with an assigned Avaya Presence Profile.

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management**.

   The system displays the User Management page.

2. In the navigation pane, click **Manage Users**.
3. Select the user, and click **Edit**.

   The system displays the User Profile Edit page.

4. Click the **Communication Profile** tab.
5. Select the **Communication Profile** with the **Default** check box enabled.
6. Select the **Presence Profile** check-box.
7. In the **Publish Presence with AES Collector** field, specify whether the user presence should be obtained using an Application Enablement Services Collector:
   - To enable Application Enablement Services Collector for the user, set the field to **On**, or set the field to **System Default** if the Application Enablement Services system policy is **On**.
   - To disable Application Enablement Services Collector for the user, set the field to **Off**, or set the field to **System Default** if the Application Enablement Services system policy is **Off**.

   The Application Enablement Services system policy is configured at **Elements** > **Presence** > **Configuration** > **Publish Presence** > **with AES Collector** > **Default**. For more information, see “AES Collector”.

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

Exporting certificate chain that signs the Session Manager identity

Before you begin

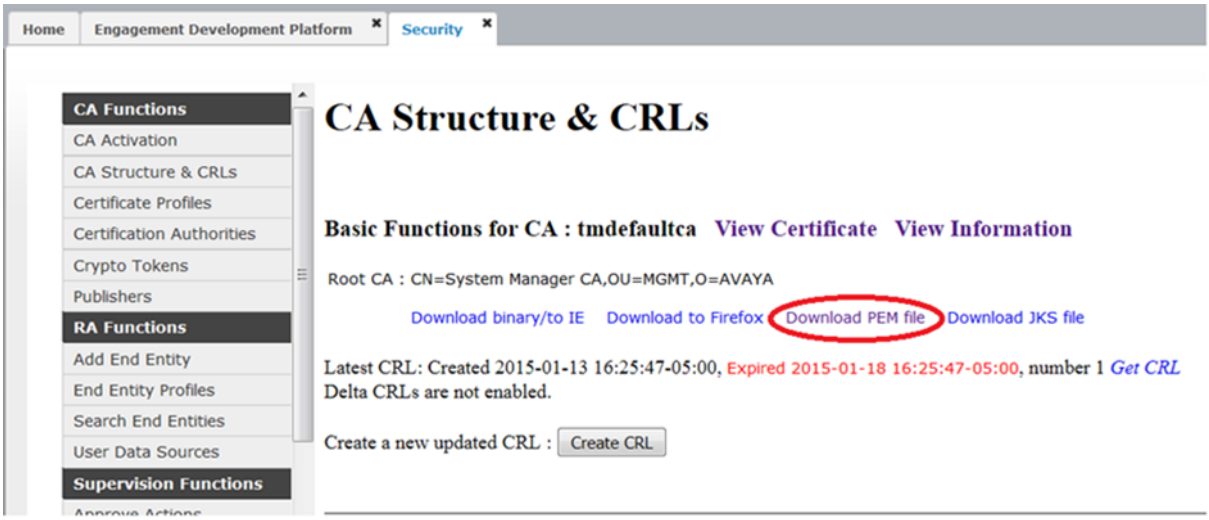
To establish a secure SIP connection to Session Manager, recent versions of SIP devices require that the certificate chain that signed the Session Manager identity be imported into truststore of the platform hosting the device.

About this task

This is the first of two steps required to establish trust between SIP devices and Session Manager. The following example procedure shows how to export the certificate chain when the Certificate Authority is System Manager.

Procedure

1. On the System Manager web console, navigate to **Services** > **Security**.
2. In the navigation pane, click **Certificates**.
3. Click **Authority**.
4. In the navigation pane, click **CA Functions** > **CA Structure & CRLs**.
5. Click **Download PEM file**.



6. In the dialog box, click **Save File** to save the certificate to the desktop.
7. At the desktop, rename `SystemManagerCA.cacert.pem` such that the file extension ends with `cer`.

   For example, `SystemManagerCA.cacert.cer`

Importing certificate chain that signs Session Manager identity into device truststore

Before you begin

To establish a secure SIP connection to Session Manager, recent versions of SIP devices require that the certificate chain that signed the Session Manager identity be imported into truststore of the platform hosting the device.

About this task

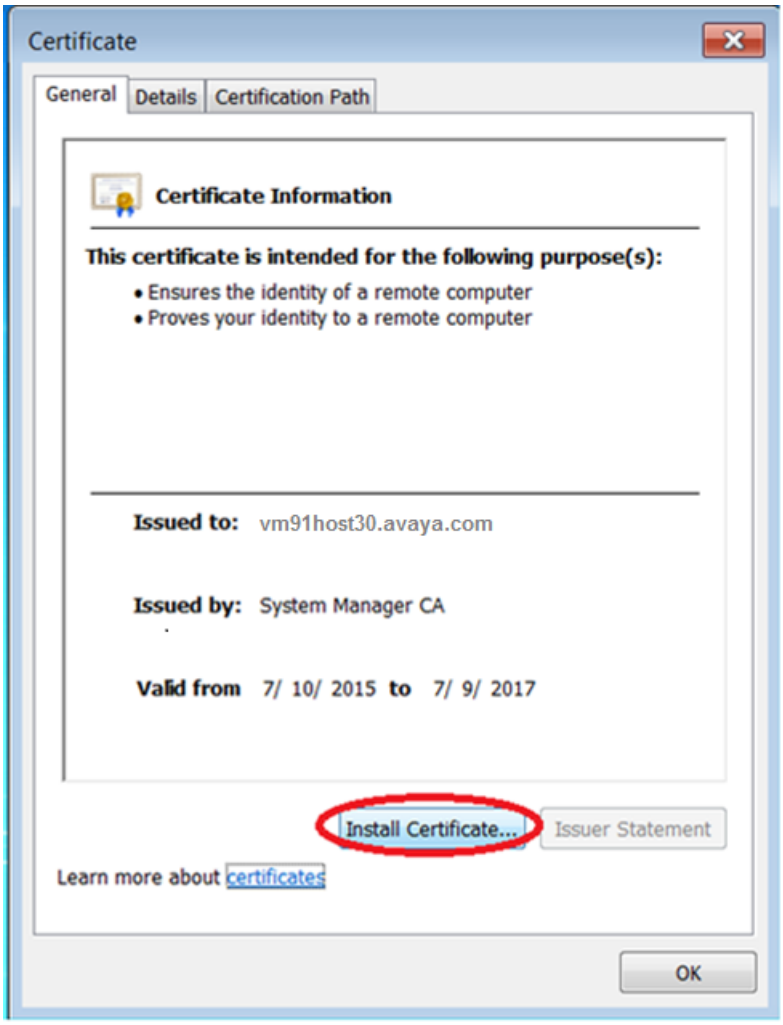
This is the second of two steps required to establish trust between SIP devices and Session Manager. The following example procedure shows how to import the certificate chain into a Windows 7 platform. For more information, consult Avaya endpoint documentation.

Procedure

1. On the desktop, locate the certificate that was exported in the “Exporting certificate chain that signs the Session Manager identity” section.
2. Either double-click on the file, or right-click and choose **Install Certificate**.
3. In the dialog box, click **Open**.

   The system displays a Certificate window.

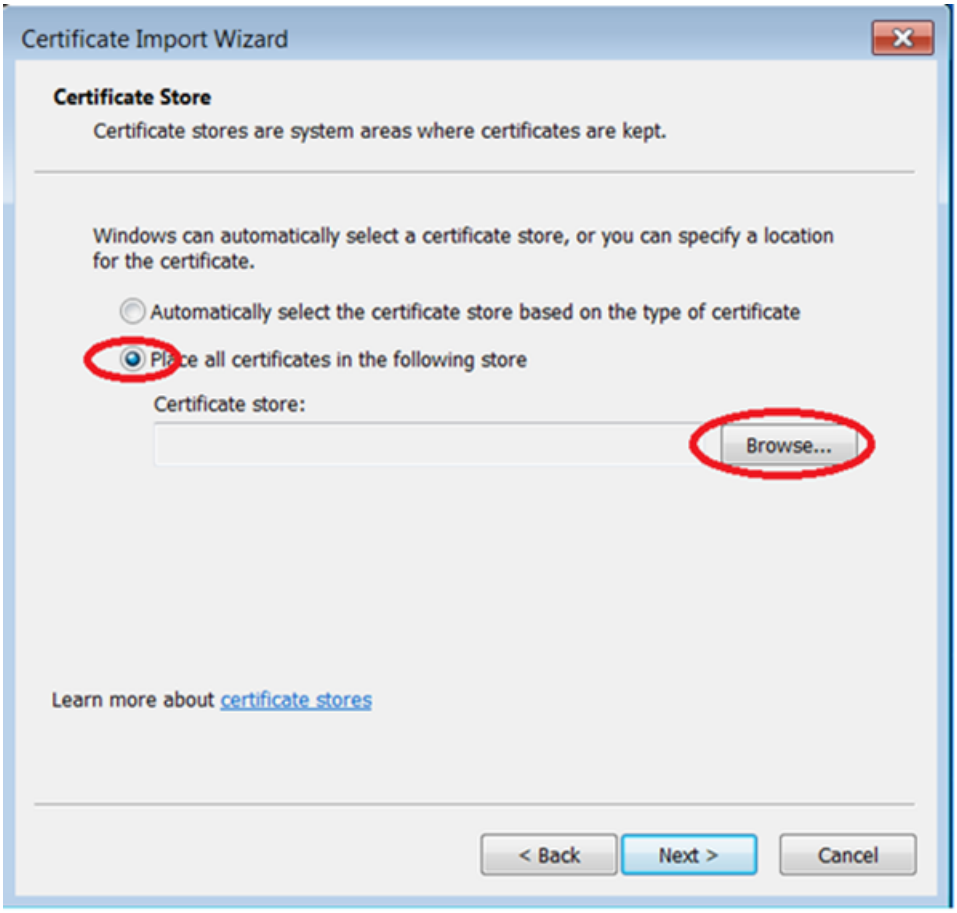
4. Click **Install Certificate**.



The system displays a Certificate Import Wizard dialog box.

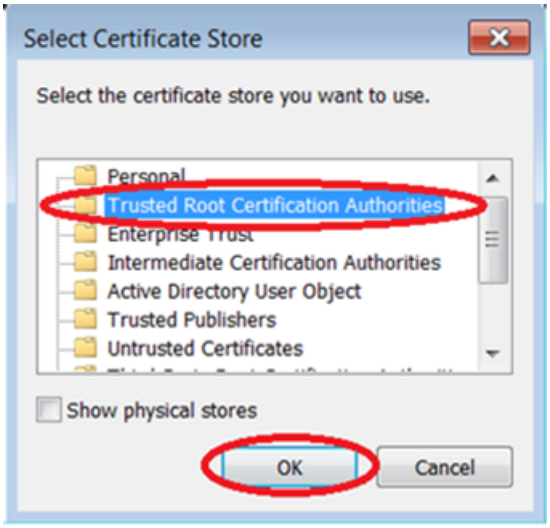
5. Click **Next**.

6. Select **Place all certificates in the following store**, and choose **Browse** to the right of the **Certificate store** field.

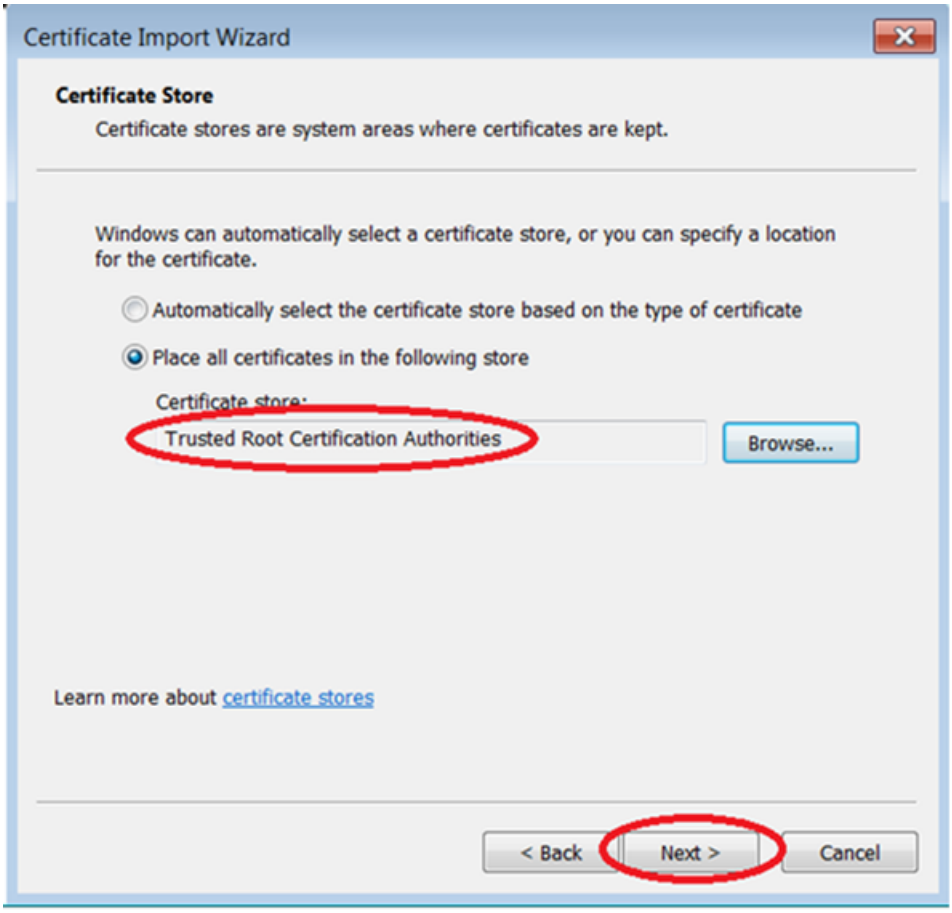


The system displays the Select Certificate Store window.

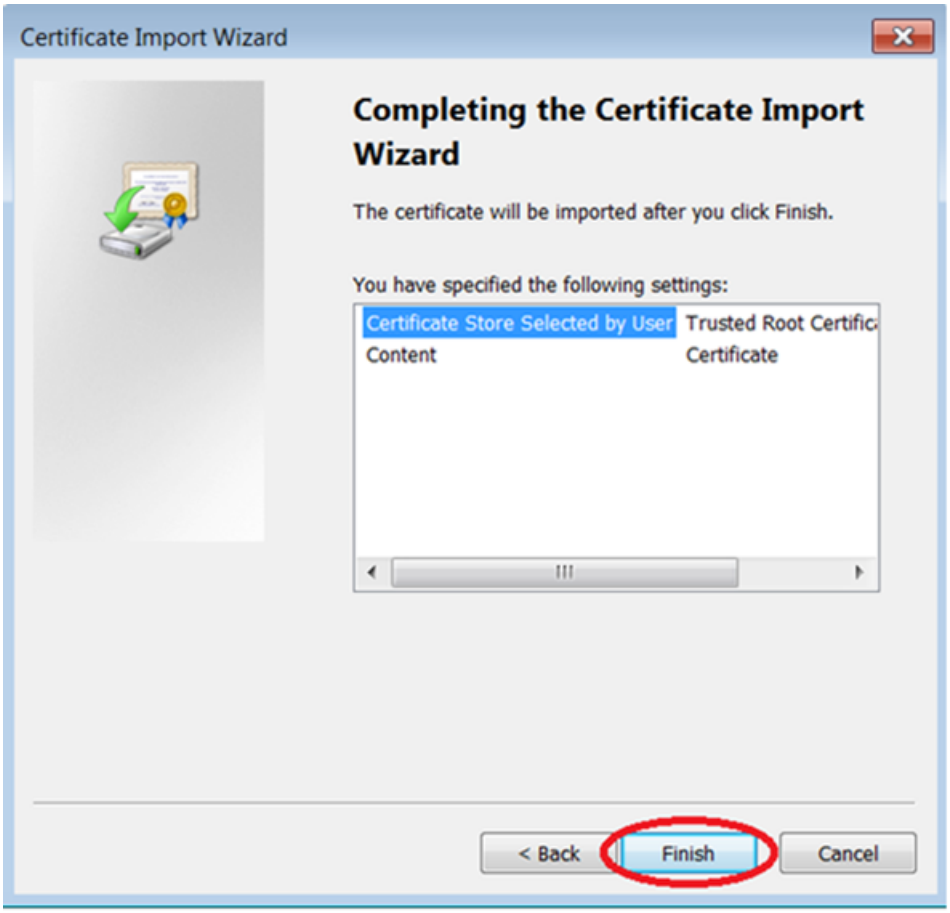
7. Select **Trusted Root Certificate Authorities**, and click **OK**.



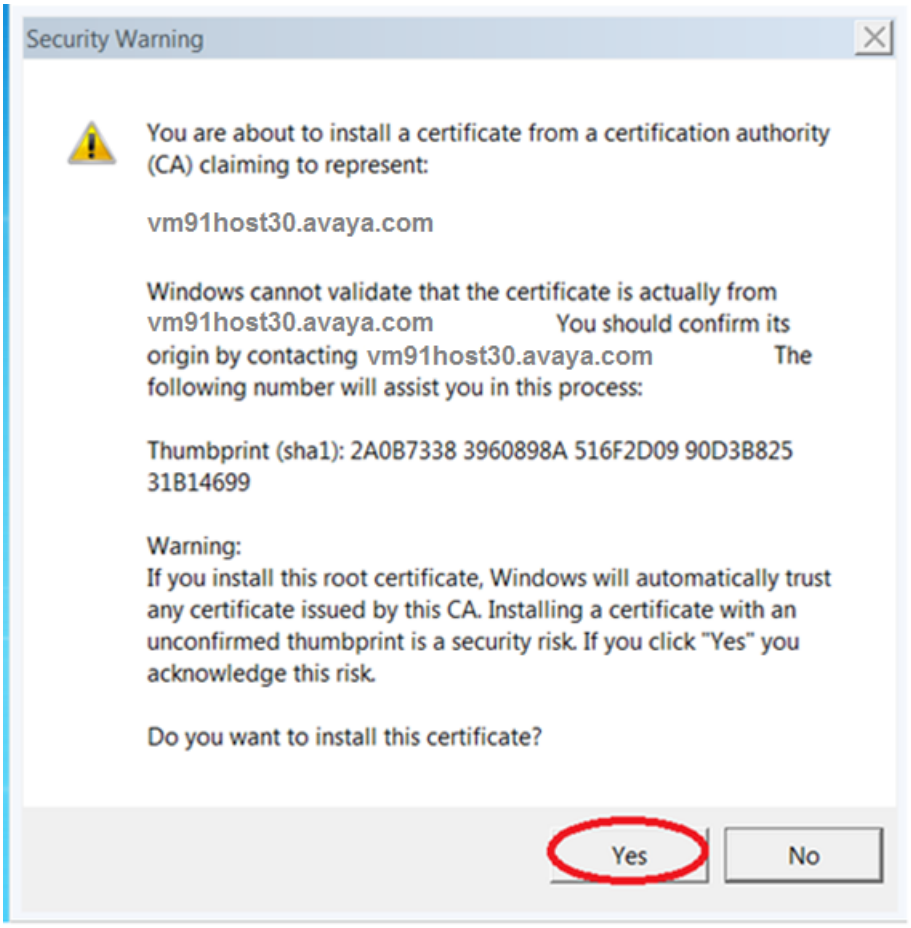
8. In the Certificate Import Wizard window, select **Next**.



9. In the Completing the Certificate Import Wizard window, click **Finish**.


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certific
Content
Certificate
< Back
Finish
Cancel

10. If the certificate had not been previously installed on this server, then the system displays a Security Warning window. Select **Yes**.



Result

The system displays a window indicating that the import was successful.

Exporting certificate chain that signs the Presence Services identity

Before you begin

To establish a secure XMPP connection to Presence Services, recent versions of SIP and H.323 devices require that the certificate chain that signed the Presence Services identity be imported into truststore of the platform hosting the device.

About this task

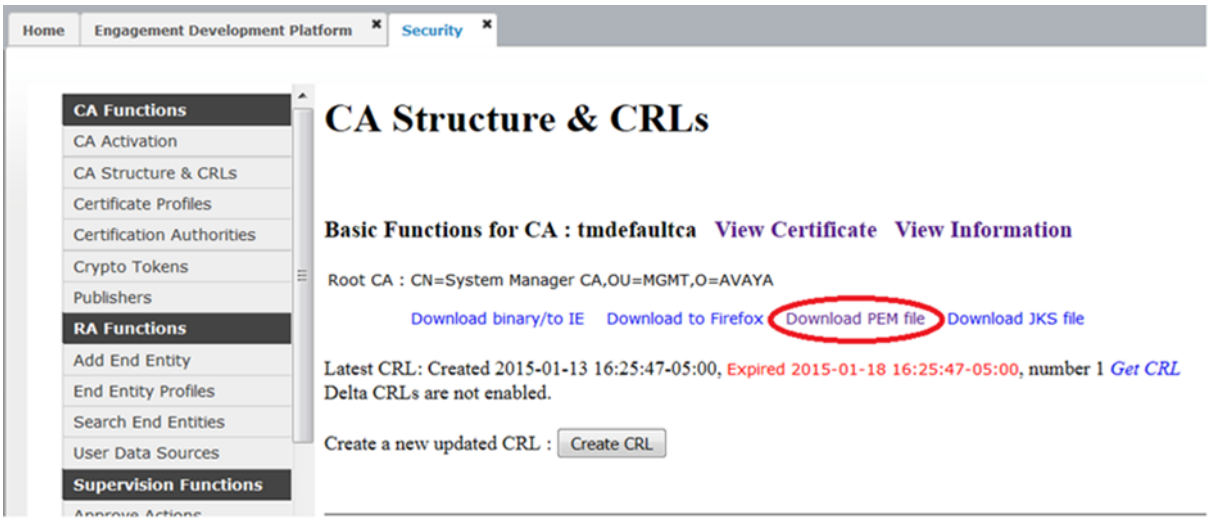
This is the first of two steps required to establish trust between devices and Presence Services for XMPP services. The following example shows how to export the certificate chain when the Certificate Authority is System Manager.

Note:

If System Manager is the Certificate Authority for both Session Manager and Presence Services , then there is no need to repeat this task if it was already performed in "Exporting certificate chain that signs the Session Manager identity"

Procedure

1. On the System Manager web console, navigate to **Services** > **Security**.
2. In the navigation pane, click **Certificates**.
3. Click **Authority**.
4. In the navigation pane, click **CA Functions** > **CA Structure & CRLs**.
5. Click **Download PEM file**.



6. In the dialog box, click **Save File** to save the certificate to the desktop.
7. At the desktop, rename `SystemManagerCA.cacert.pem` such that the file extension ends with `cer`.

   For example, `SystemManagerCA.cacert.cer`

Importing certificate chain that signs the Presence Services identity into device truststore

Before you begin

To establish a secure XMPP connection to Presence Services, recent versions of SIP and H.323 devices require that the certificate chain that signed the Presence Services identity be imported into truststore of the platform hosting the device.

About this task

This is the second of two steps required to establish trust between devices and Presence Services for XMPP services. The following example procedure shows how to import the certificate chain into a Windows 7 platform. For more information, consult Avaya endpoint documentation.

Note:

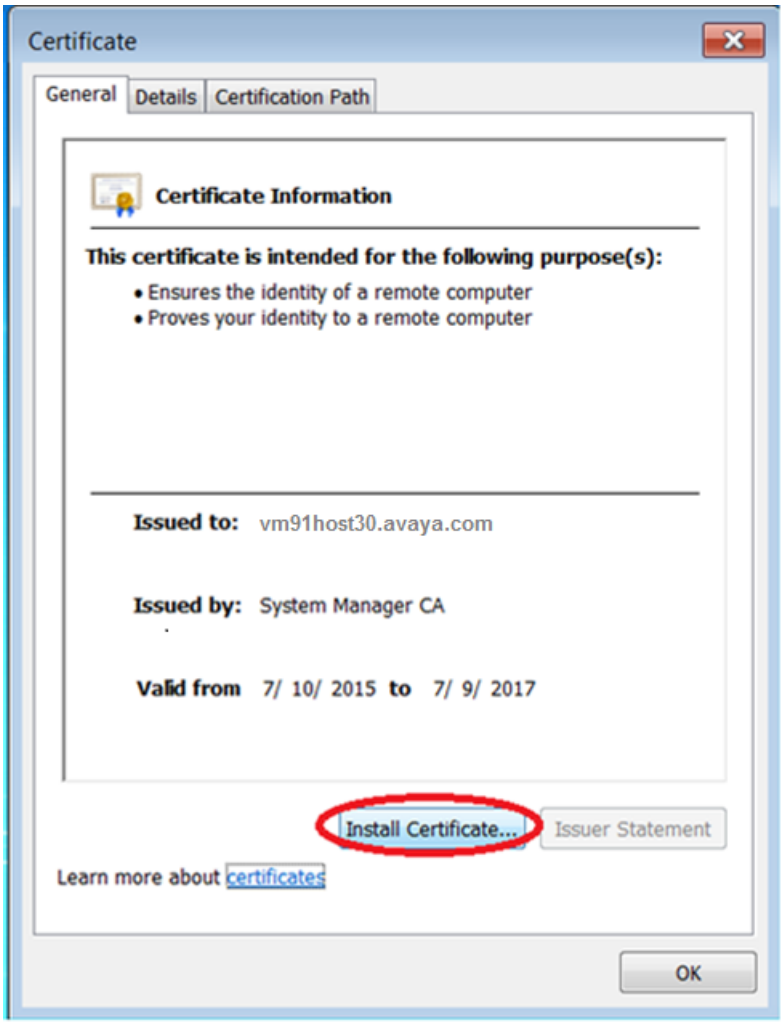
If System Manager is the Certificate Authority for both Session Manager and Presence Services , then there is no need to repeat this task if it was already performed in "Importing certificate chain that signs the Session Manager identity"

Procedure

1. On the desktop, locate the certificate that was exported in the “Exporting certificate chain that signs the Presence Services identity” section.
2. Either double-click on the file, or right-click and choose **Install Certificate**.
3. In the dialog box, click **Open**.

   The system displays a Certificate window.

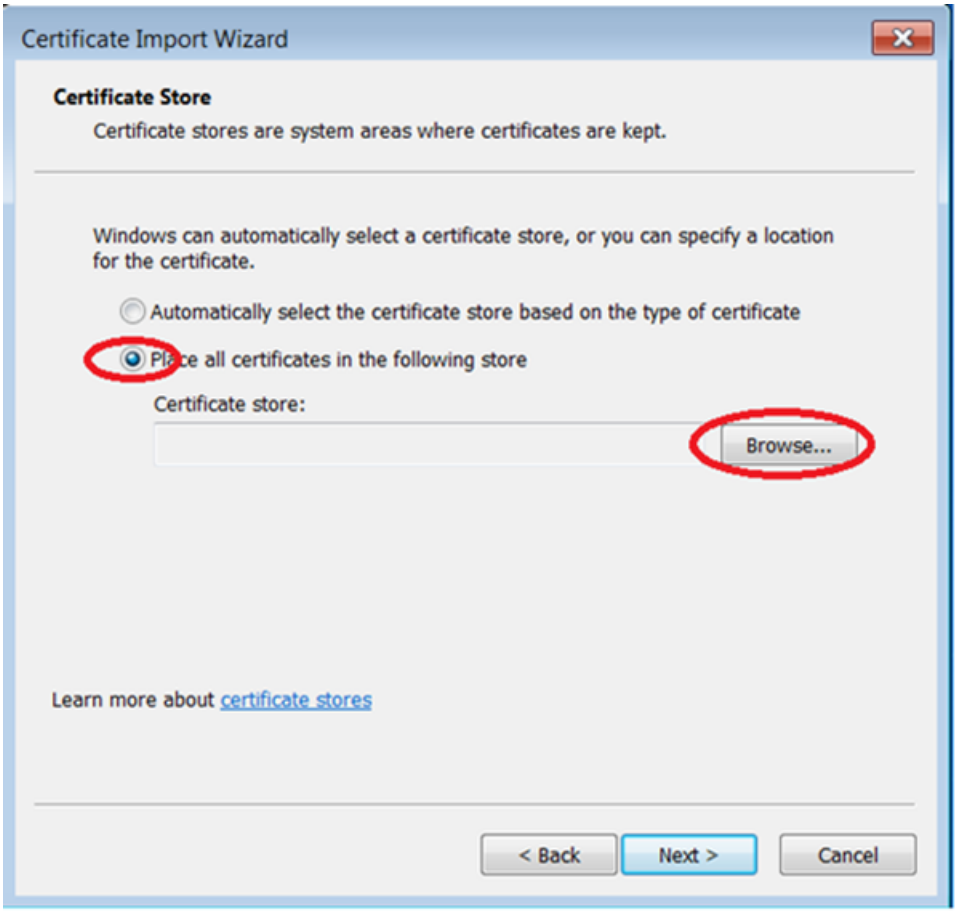
4. Click **Install Certificate**.



The system displays a Certificate Import Wizard dialog box.

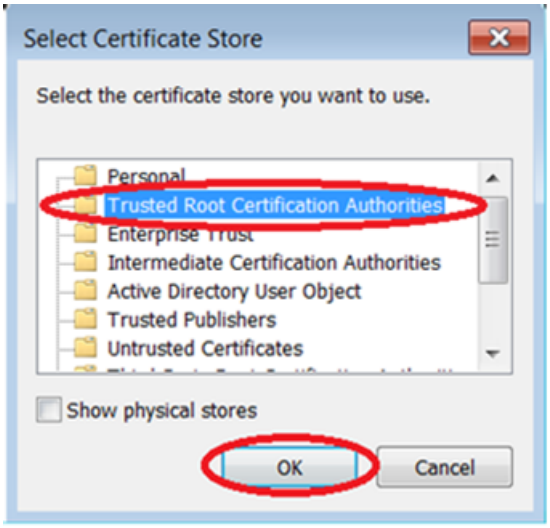
5. Click **Next**.

6. Select **Place all certificates in the following store**, and choose **Browse** to the right of the **Certificate store** field.

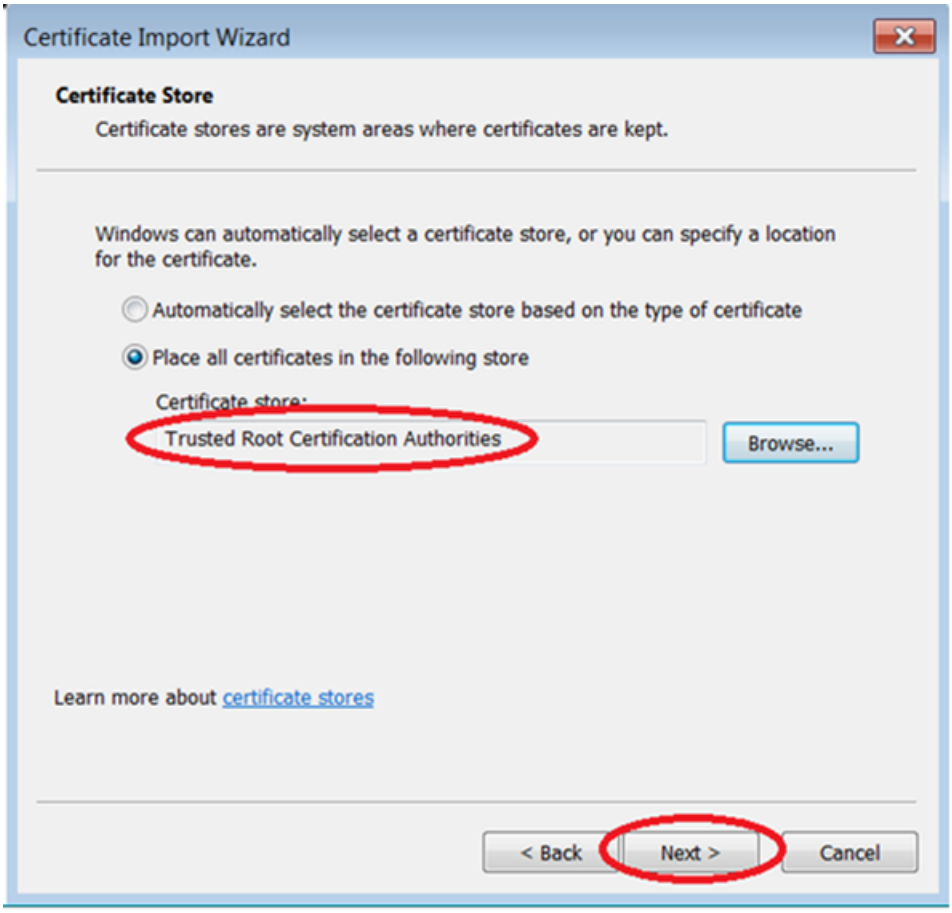


The system displays the Select Certificate Store window.

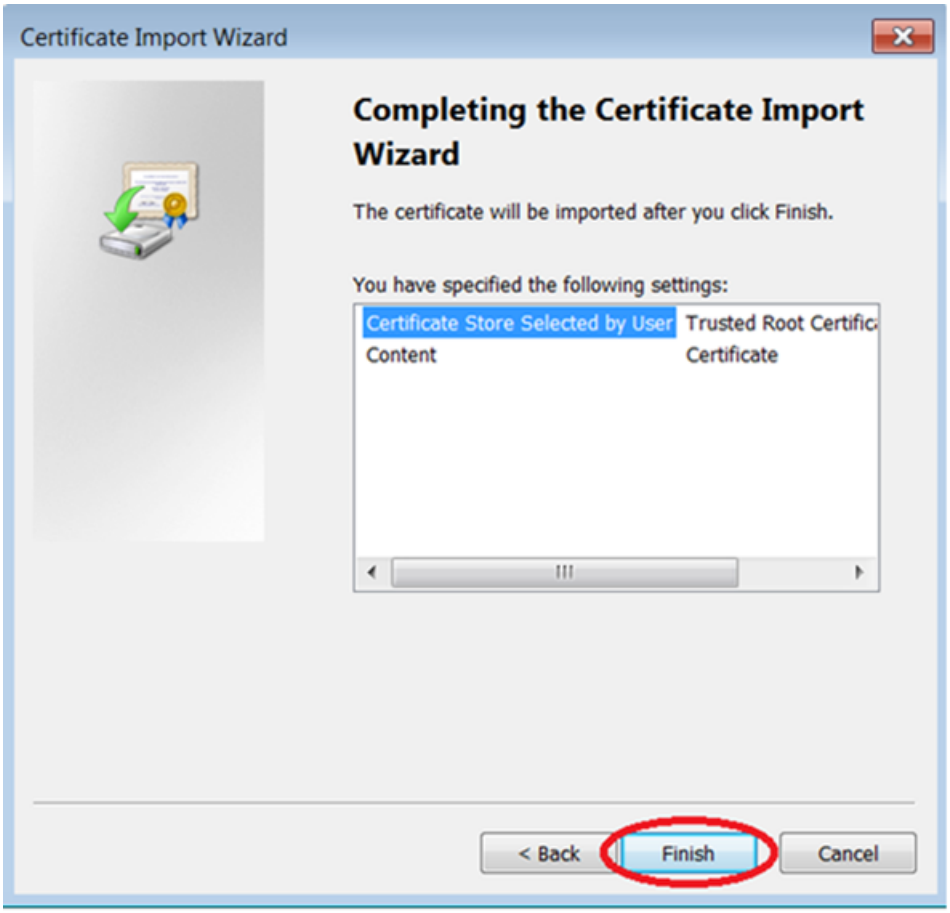
7. Select **Trusted Root Certificate Authorities**, and click **OK**.



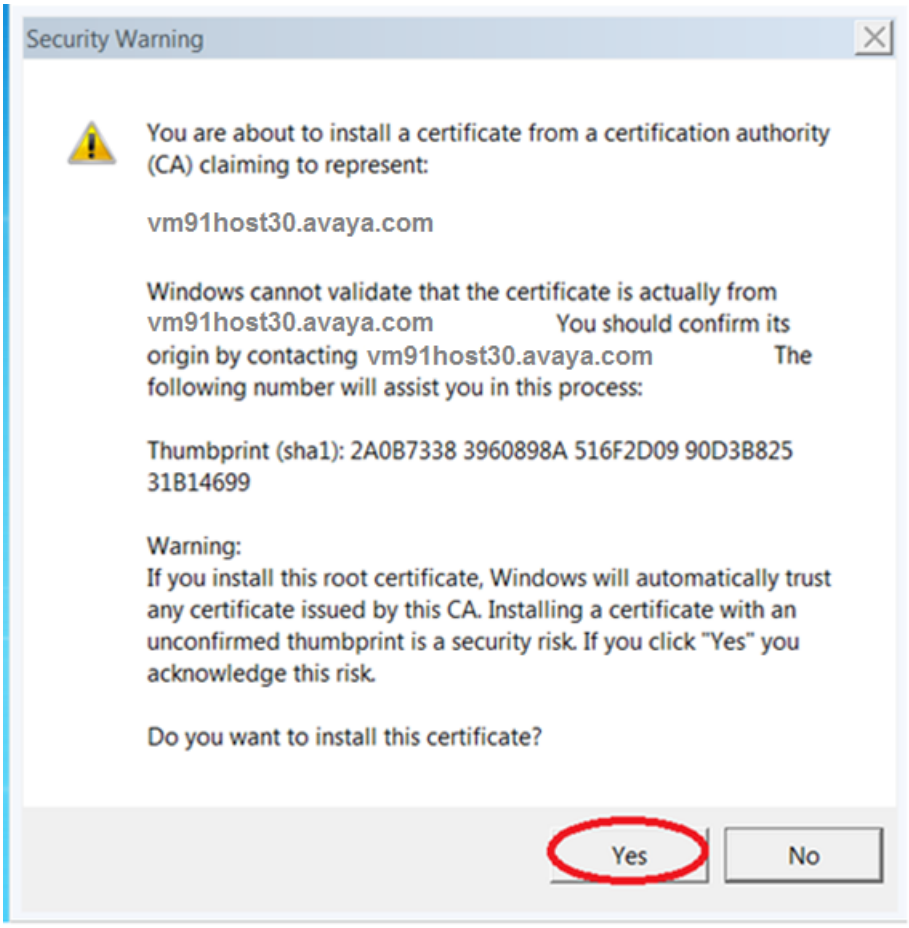
8. In the Certificate Import Wizard window, select **Next**.



9. In the Completing the Certificate Import Wizard window, click **Finish**.


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certific
Content
Certificate
< Back
Finish
Cancel

10. If the certificate had not been previously installed on this server, then the system displays a Security Warning window. Select **Yes**.



Result

The system displays a window indicating that the import was successful

Checklist for administering Presence and IM on a device

In the following table, **M** indicates that the task is mandatory for the device and **—** indicates that the task is not applicable to the device.

Table 22: Checklist for administering Presence and IM on a device

No.	Task	Device category				Notes/Reference
		1	2	3	4	
1	Administer Communication Profile	M	M	M	—	Password is required to authenticate the user for XMPP on Presence Services. See Assigning

Table continues…

No.	Task	Device category				Notes/Reference
		1	2	3	4	
	password on the device.					Communication Profile Password to a user on System Manager on page 195.
2	Administer Session Manager address on the device.	M	M	—	—	SIP Presence messages are routed to Presence Services through Session Manager. On System Manager, a user's Session Manager is administered at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Session Manager Profile**.
3	Enable Instant Messaging and Presence on the device.	M	M	M	—	On most Avaya devices, IM and Presence is disabled by default.
4	Administer Presence Services address on the device.	—	M	M	—	• For Category 1 devices, do not administer Presence Services address, as device automatically learns this using PPM. • For Category 2 and 3 devices, administer Presence Services address. If using FQDN format: - Enter Presence Services Cluster FQDN. See “Table 1: Key customer configuration information”, row 25. - Administer DNS A records to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP addresses. If using IP Address format: - For Presence Services single-server deployment, enter the Avaya Breeze™ Security Module IP address. See Administering Avaya Breeze™ SIP Entity on page 24. - For Presence Services multi-server deployment, enter one of the Avaya Breeze™ Security Module IP addresses within the cluster. See Administering Avaya Breeze™ SIP Entity on page 24. To maximize efficiency of the Presence Services cluster, a system administer must ensure that Avaya Breeze™ Security Module IP addresses are equally distributed across devices. FQDN format is strongly recommended as it is required for Presence Services features such as High Availability and Geo Redundancy.

Table continues…

No.	Task	Device category				Notes/Reference
		1	2	3	4	
5	Administer Avaya Presence/IM communication address on the device.	—	M	M	—	• For Category 1 devices, do not administer Avaya Presence/IM communication address as device automatically administers using PPM. • For Category 2 and 3 devices, administer Avaya Presence/IM communication address. See Assigning Avaya Presence/IM communication address to user on System Manager on page 105.

Chapter 11: Performance

Capacity and scalability specification

Table 23: Capacity and scalability specification

Endpoint mode	Max. no. of users	Max. no. of devices	Max. avg. no. of contacts per user	Default max. contacts per user	Max. no. of subscriptions/ minute/ server	Max. no. of presence updates per second/ server	Max. no. of XMPP IMs per second/ server
SIP	Up to 16,000 on a single server, 125,000 on an 8-server cluster[1], and 250,000 on two 8-server clusters[1]	175,000 on a single cluster and 350,000 on a dual cluster[2]	25	100[3]	300	30	44
H.323 (XMPP)	Up to 16,000 on a single server, 125,000 on an 8-server cluster[1],	125,000 on a single cluster and 350,000 on a dual cluster[2]	25	100[3]	300	30	44

Table continues…

[1] Clustered deployments of Presence Services are limited to a maximum of 8 servers in a cluster and all servers in the cluster must reside on the same subnet. A total of 250,000 users can be supported if two 8 server clusters are deployed. For cluster deployments all servers in the cluster must use the same resource profile: 12 vCPUs, 27 GB of RAM, and 28,800 Mhz of CPU reservation.

[2] When the Multi-Device Access feature is used, Presence Services can support an average of 1.4 devices per user for a maximum total of 175,000 devices per cluster or 350,000 devices per Aura system with maximum of two 8 server Presence Services clusters.

[3] By default, the maximum number of contacts permitted per user is 100. This option is configurable and the maximum can be increased but a fully-loaded Presence Services system can only support an average of 25 contacts per user.

Endpoint mode	Max. no. of users	Max. no. of devices	Max. avg. no. of contacts per user	Default max. contacts per user	Max. no. of subscriptions/ minute/ server	Max. no. of presence updates per second/ server	Max. no. of XMPP IMs per second/ server
	and 250,000 on two 8-server clusters[1]						

Table 24: Capacity and scalability specification

Feature	Restriction
AES Collector	You can configure 4000 station monitors for each collector. You can configure a maximum of 32,000 stations for each Presence Services cluster.
IBM Domino Collector	You can configure 16000 users for each collector. Each collector can only communicate with a single Domino server.
Microsoft Exchange Collector	You can configure 16000 users for each collector. Each collector can only communicate with a single Exchange cluster.
Clustering	You can configure a maximum of eight servers for each cluster with up to 10 servers when High Availability is enabled and a maximum of two clusters for each cluster System Manager.
High Availability	• Up to 16,000 Users: 1+1 (total of 2 servers in the cluster) • Up to 32,000 Users: 2+1 (total of 3 servers in the cluster) • Up to 48,000 Users: 3+1 (total of 4 servers in the cluster) • Up to 64,000 Users: 4+1 (total of 5 servers in the cluster) • Up to 80,000 Users: 5+1 (total of 6 servers in the cluster) • Up to 96,000 Users: 6+2 (total of 8 servers in the cluster) • Up to 112,500 Users: 7+2 (total of 9 servers in the cluster) • Up to 125,000 Users: 8+2 (total of 10 servers in the cluster) When High Availability is deployed, the additional servers are used for normal service as the cluster supports active-active High Availability protection and balances the load to all servers. High Availability provides fault protection for single server failures only. Cascading failures are not protected.

Chapter 12: Security

Port utilization

For the Presence Services port information, see the *Avaya Breeze™ Port Matrix* document at https://support.avaya.com/security.

Chapter 13: Troubleshooting

Presence Services alarms

The following alarms are supported on Presence Services:

- Open an SSH session to Avaya Breeze™ Management IP address, navigate to the `event.log` file located at `/var/log/Avaya/services`.
- On the System Manager web console, navigate to **Services** > **Events** > **Alarms**.
- On the System Manager web console, navigate to **Services** > **Events** > **Logs** > **Log Viewer**.

Presence Services alarms

Event ID	Alarm name	Severity	Description
`CluMon_01`	Cluster Monitor	Critical	Raised when the Presence Services node within a cluster has failed.
`PresServ_CLR_CluMon_01`	Clear Cluster Monitor	Critical	Raised when the Presence Services node is running and clears the `PresServ_CluMon_01` alarm.
`IMArc_01`	Message Archive upload failed	Major	Raised when an attempt to SFTP archived messages to a remote site has failed.
`CLR_IMArc_01`	Clear Message Archive upload failed	Major	Raised when the Presence Services node is running and clears the `IMArc_01` alarm.
`IMArc_02`	Message Archiving Disabled	Critical	Raised when Message Archiving is disabled due to too many consecutive SFTP failures.
`CLR_IMArc_02`	Clear Message Archiving disabled	Critical	Raised when the Presence Services node is running and clears the `IMArc_02` alarm.
`GR_01`	Lost Connectivity to remote Geographic Redundancy cluster	Critical	Raised when Presence Services loses connectivity to the remote Geographic Redundancy cluster.

Table continues…

Event ID	Alarm name	Severity	Description
CLR_GR_01	Clear Lost Connectivity to remote Geographic Redundancy cluster	Critical	Raised when Presence Services establishes connectivity to the remote Geographic Redundancy cluster and clears the GR_01 alarm.
GR_02	Presence Services Geographic Redundancy misconfigured	Major	Raised when Presence Services Geographic Redundancy is misconfigured.
CLR_GR_02	Clear Presence Services Geographic Redundancy misconfigured	Major	Raised when Presence Services Geographic Redundancy is configured correctly and clears the GR_02 alarm.
HLTH_01	Cluster Health Check failed	Major	Raised when a Presence Services cluster-level health check has failed.
CLR_HLTH_01	Clear Cluster Health Check failed	Major	Raised when a Presence Services cluster-level health check has passed and clears the HLTL_01 alarm.

Causes and resolutions of the alarms

Alarm name	Causes	Resolutions
Cluster Monitor	• Network outage • Hardware failure • Software failure	1. Check the CluMon_01 log to identify the failed server. 2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Server Administration**. 3. Select the failed server. 4. From the **Shutdown System** menu, select **Reboot**. 5. If this fails, open an SSH session to the Avaya Breeze™ Management IP address as root user. 6. Run the reboot command. 7. If this fails, verify the Enet connectivity to the server by pinging the server from a remote server. 8. If this fails, troubleshoot the server hardware.
Message Archive upload failed	Messaging Archiving attributes have been misconfigured.	Reconfigure the **Message Archiving** attributes on System Manager at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.

Table continues…

Alarm name	Causes	Resolutions
	For example, an invalid Remote Server Address has been entered.	
Message Archive upload failed	EXPORT_FAILED: Presence Services failed to store the archived messages in XML format.	Raise a ticket.
Message Archive upload failed	ZIP_FAILED: Presence Services failed to create a ZIP file.	Raise a ticket.
Message Archive upload failed	UPLOAD_FAILED: Remote server is reachable, but SFTP to the remote server failed for an unknown reason.	Troubleshoot the remote server to ensure that the remote server successfully accept files through SFTP.
Message Archive upload failed	EXCEPTION or UNKNOWN: Internal Presence Services failure.	Raise a ticket.
Message Archiving Disabled	Messaging Archiving is enabled and configured through the service attributes at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **Group**. This alarm is raised when the Message Archive upload failed alarm is continually raised for the duration specified in the **Message Archiving Remote Upload Failures Threshold** attribute.	Clear the condition that has caused the Message Archive upload failed alarm, that is, IMArc_01 to be raised. Once IMArc_01 is cleared, the system will clear the IMArc_02 alarm.
Lost Connectivity to remote Geographic Redundancy cluster	• Network outage • Hardware failure • Software failure	In the following example: • Clusters A and B are configured on System Manager at **Elements** > **Avaya Breeze™** > **Cluster Administration**, each with multiple Avaya Breeze™ servers assigned. • Managed Elements A and B are configured at **Services** > **Inventory** > **Managed Element** of type **Presence Services on Avaya Breeze™** with **GEO Redundant Avaya Breeze Cluster** as cluster B and A. • Geographic Redundancy works correctly, then cluster A detects loss of connectivity to cluster B. Cluster A raises a Lost Connectivity to Geographic Redundancy cluster alarm, which includes fields: • Host Name: Short host name of one server in cluster A. • Source IP Address: IP address of same server as earlier.

Table continues…

Alarm name	Causes	Resolutions
		• Description: Lost connectivity to Geographic Redundancy cluster B. To clear this alarm: 1. Restart Presence Services on cluster B. See “Restarting Presence Services”. 2. If alarm does not clear within 2-15 minutes, verify Enet connectivity between clusters by opening an SSH connection to one server in cluster A and pinging the Avaya Breeze™ Security Module IP address of a server in cluster B, and vice versa. If this fails, troubleshoot the network. 3. If no Enet connectivity issues detected, troubleshoot the hardware of servers in cluster B
Presence Services Geographic Redundancy misconfigured	• Geographic Redundancy is misconfigured • Geographic Redundancy cluster restart is pending after configuration	In this example: Clusters A and B are configured at **Elements** > **Avaya Breeze™** > **Cluster Administration**. To clear this alarm: 1. Navigate to **Services** > **Inventory** > **Managed Element** . 2. Select the Managed Element of type **Presence Services on Avaya Breeze™** with **Primary Avaya Breeze Cluster** field as cluster A, and edit the Managed Element. 3. Assign B to **GEO Redundant Avaya Breeze Cluster** field, and click **Commit**. 4. Select the Managed Element of type **Presence Services on Avaya Breeze™** with **Primary Avaya Breeze Cluster** field as cluster B, and edit the Managed Element. 5. Assign A to **GEO Redundant Avaya Breeze Cluster** field, and click **Commit**. 6. Restart Presence Services for both the clusters. See “Restarting Presence Services”.
Cluster Health Check failed	• Duplicate domains: Presence/IM domains can be configured at: - **Local Presence/IM domains** at **Elements** > **Routing** > **Domains**	• Duplicate domains: On the System Manager web console, navigate to the following pages, and reconfigure the system so that domains are not duplicated: - **Elements** > **Routing** > **Domains**

Table continues…

Alarm name	Causes	Resolutions
	- **Remote domain** at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **Inter-PS Federation** > **Inter-PS Domain Name List** - **Remote domain** at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **Lync Federation** > **Lync Domain Name List** - **Remote domain** at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **XMPP Federation *x*** > **XMPP Federation Domain Name List *x*** • Too many users have AES Collector enabled: AES Collector system policy is defined at **Elements** > **Presence** > **Configuration** > **Publish Presence with AES Collector – Default**. Users inherit the system policy, and it can be overridden via **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **Publish Presence with AES Collector**. Users are assigned to a cluster at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **System**. This alarm is raised when the number of users assigned to this cluster, with AES Collector enabled, exceeds the number supported on the cluster.	- **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **Inter-PS Federation** > **Inter-PS Domain Name List** - **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **Lync Federation** > **Lync Domain Name List** - **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes** > **XMPP Federation *x*** > **XMPP Federation Domain Name List *x*** • Too many users have AES Collector enabled: Reduce the number of users assigned to this cluster with AES Collector enabled in one of the following ways: - Modify the AES Collector system policy at **Elements** > **Presence** > **Configuration** > **Publish Presence with AES Collector – Default**. The possible values are `Off` and `On`. - Modify the individual user settings at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **Publish Presence with AES Collector**. The possible values are `On`, `Off`, `System Default`.

Changing the logging level

Procedure

1. On the System Manager web console, navigate to **Home** > **Elements** > **Engagement Development Platform**.
2. In the navigation pane, click **Configuration** > **Logging**.

   The system displays the Logging page.
3. Select the Presence Services snap-in service.
4. Select the logging level.
5. Click **Commit**.

   Note:

   The **Clear Logs** button is not supported for Presence Services.

Network outage causes presence to stop working for some or all users

Cause

High Availability initiates the backup node to take over, but the primary node is still active. Therefore, when the network recovers more than one node service the same users resulting in potential wrong presence.

Solution

1. If only one node was disconnected, that is, the cable pulled out from one server:
   a. Log in to the Avaya Breeze™ server that lost the network connectivity.
   b. Run the `stop -s dcm` command.
   c. Run the `start -s dcm` command.
   d. To check the status of DCM, run the `statapp` command.
2. If more than one node was disconnected or you are not able to determine which node was not connected:
   a. Log in to the System Manager web console.
   b. Navigate to **Elements** > **Avaya Breeze™**.
   c. Click **Service Management**.
   d. Select the cluster and click **Stop**.
   e. Select your cluster and click **Start**.

Presence and IM fails on SIP endpoints due to the PPM getHomeCapabilities fault

Cause

SIP endpoints invoke the Personal Profile Manager (PPM) web service on Session Manager to discover capabilities. PPM getHomeCapabilities is used to discover the home Presence Services cluster of an endpoint. If unsuccessful, Presence and IM are not supported on the endpoint.

Solution

1. Open an SSH session to Session Manager management IP address.
2. Start the traceSM tool.
3. When starting the capture, ensure that PPM is selected.
4. Log in to the SIP endpoint.
5. Verify that the endpoint sends PPM getHomeCapabilities to Session Manager.
6. If Session Manager returns `Fault : DataNotAvailable`:
    a. On the System Manager web console, navigate to **Elements** > **Routing** > **SIP Entities**.
    b. Edit the Session Manager SIP Entity.
    c. Add a Listen Port.
    d. In the **Listen Port** field, enter `5061`.
    e. In the **Protocol** field, enter `TLS`.
    f. In the **Default Domain** field, enter the login domain of endpoint devices.
    g. Select the **Endpoints** check box.
    h. Click **Commit**.

Repairing replication between Avaya Breeze™ and System Manager

Procedure

1. On the System Manager web console, navigate to **Services** > **Replication**.
2. In **Replica Group** column, click **CollaborationEnvironment_3.1**.
3. In **Replica Node Host Name** column, locate **Avaya Breeze™**.
4. Verify that the status of the **Synchronization Status** field is green. If not, go to Step 5.
5. If Presence Services Snap-in has been deployed, in the **Product** column, verify that both Avaya Breeze™ and Presence Services are displayed.
6. Select Avaya Breeze™, and click **Repair**.

7. After 2–15 minutes, verify that the status of the **Synchronization Status** field is green. If not, go to Step 8.
8. Verify that Enrollment Password is not expired.
    a. Navigate to **Services** > **Security**.
    b. In the navigation pane, click **Certificates** > **Enrollment Password**.
9. If the Enrollment Password is expired:
    a. Enter a password, and click **Commit**.

       It is highly recommended that the same password must be used. Otherwise, Avaya Breeze™ and Presence Services must be re-administered, because System Manager Enrollment Password was configured during deployment of Avaya Breeze™. For more information, see *Deploying Avaya Breeze™*.
    b. Open an SSH session to the Avaya Breeze™ Management Module IP address as sroot.
    c. On the command line interface, enter `initTM -f`.
    d. When prompted for the enrollment password, enter the password that you provided in Step 9a.
    e. Repeat Step 1 to Step 6.

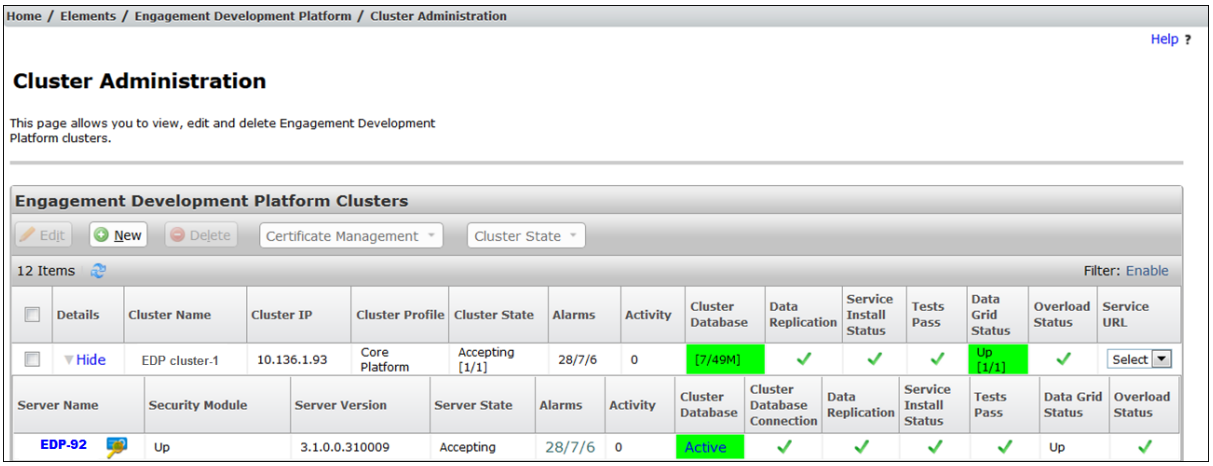
Verifying that Presence Services snap-in is ready to support Presence and IM

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Locate the row for the cluster, and verify that:
    - The **Cluster Profile** field shows `Core Platform`.
    - The **Cluster State** field shows `Accepting`.
    - The **Cluster Database** field is green, and the value of **Number of active connections for the active** is not zero.
    - The **Data Replication** field shows a green checkmark.
    - The **Service Install Status** field shows a green checkmark.
    - The **Tests Pass** field shows a green checkmark.
    - The **Data Grid Status** field shows `Up` or is green.
    - The **Overload Status** field shows a green checkmark.
3. On the row for the cluster, use the arrow in the **Details** column to display the servers assigned to this cluster.

4. For each server, verify that:
   - The **Security Module** field shows `Up`.
   - The value of the **Server Version** field is correct.
   - The **Server State** field shows `Accepting`.
   - The **Cluster Database** field is green.
   - The **Cluster Database Connection** shows a green checkmark.
   - The **Data Replication** field shows a green checkmark.
   - The **Service Install Status** field shows a green checkmark.
   - The **Tests Pass** field shows a green checkmark.
   - The **Data Grid Status** field shows `Up`.

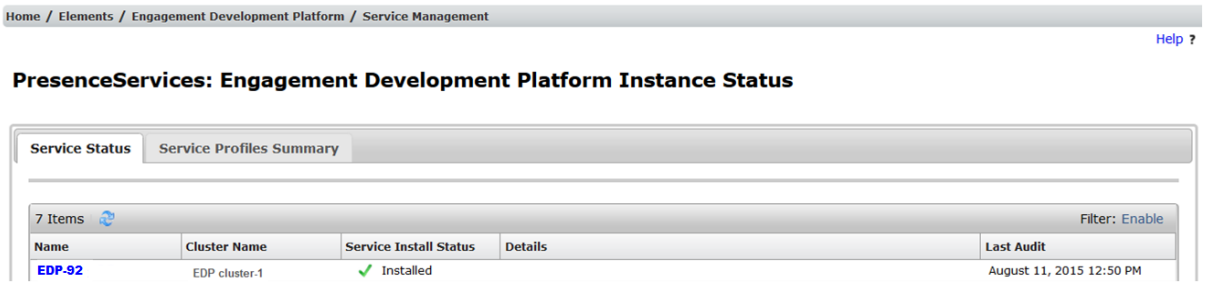
   Following is an example of a single-server Presence Services cluster that is ready to support Presence and IM:



5. Navigate to **Elements** > **Avaya Breeze™** > **Service Management**.
6. Locate the row for the Presence Services snap-in, and click on the Presence Services link within the **Name** column.

   The system displays a PresenceServices: Avaya Breeze Instance Status window.
7. Verify that the **Service Install Status** column shows `Installed` and a green checkmark in one or more rows.
8. Verify that the **Cluster Name** column identifies the expected cluster.

   Following is an example of a Presence Services snap-in that is installed on a single-server cluster:



Geographic Redundancy

Failure and Recovery

There are multiple scenarios where it is desired that a data center is made non-operational, and the users are migrated over to the other data center. Scenarios include occurrence of some disastrous event which leaves a data center completely or partially non-functional, in-service upgrades or even a routine maintenance procedure. In any of these scenarios, administrators must ensure that the access to the data center undergoing maintenance is completely disabled. For more information, see *Disabling access to a data center*.

Conversely, while recovering a failed data center or making a data center functional after maintenance, administrators must ensure that all the components are recovered and ready to provide service before the users are allowed access to the data center. For more information, see *Enabling access to a data center*.

Chapter 14: Resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Breeze™ Overview and Specification	Find information about the product characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Avaya professional services, implementation engineers, support personnel, and system administrators
Administering		
Administering Avaya Breeze™	Find the procedures to administer and configure Avaya Breeze™.	System administrators and support personnel
Administering Avaya Aura® System Manager for Release 7.0.1	Find the procedures to administer and configure System Manager.	System administrators and support personnel
Implementing		
Deploying Avaya Breeze™	Find the procedures to install Avaya Breeze™.	Avaya professional services, implementation engineers, support personnel, and system administrators

Finding documents on the Avaya Support website

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.

3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

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
2010W	What is New in Avaya Aura® Presence Services 7.0
2010T	What is New in Avaya Aura® Presence Services 7.0 Online Test

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 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 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.

Appendix A: CLI commands

presClients

This command is used to:

- List all users or devices logged in to the Presence Services instance.
- Display current presence document (PIDF) for online and offline users.
- Take actions on the subscriptions for logged-in users.

Syntax

`presClients [-h] [-u <login_name>] [-m {SIP|XMPP}] [-i <client_ip> ] [-n <ps_node>] [-t|-r|--resend-list[<list_name>]] [-p]`

Options:

- `-u <login_name>`: Avaya user login name.
- `-m {SIP|XMPP}`: Device communication protocol.
- `-i <client_ip>`: Device IP address.
- `-n <ps_node>`: Presence Services address (IP or FQDN).

Actions (must specify a filter):

- `-r`: Resend Notify(s) or stanza(s) with full PIDF to watcher for all active or non-list presence event subscriptions.
- `--resend-list [list_name]`: Resend Notify(s) with full PIDF to watcher for each presentity in the active list subscription (SIP devices only).
- `-t [restart | disable]`: Terminate active subscriptions or connections to the device. SIP devices receive a termination Notify to all active subscriptions.
  - `restart`: Client may resubscribe immediately
  - `disable`: Client must not resubscribe until logging out and logging in.

  XMPP endpoints receive a XMPP Stream closure stanza.
- `-p [tuples]`: Display current presence document (PIDF) of the user. This action can be used only with the `-u` filter.

Sample output 1

`#/opt/Avaya/snap_in/ps/bin/presClients`

```
Active Presence Server Client Connections
Cluster :  cluster-185
```

```
Nodes : 32646=135.20.245.44,32648=10.136.1.183
Active Publish & Subscriptions(node/expires remaining)
         User              IP Address        Mode          User-Agent/Resource
Last Publish Time      Publish     Self         Winfo        Acl          list(s)
-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------
  2600002@avaya.com | 135.55.68.85:60269 |   SIP |            Avaya one-X Communicator |
2015-09-30 17:49:17 |  32648/369 |  32648/1568 |  32648/1568 |  32648/1568 |
default( 32648/1568)
  2600003@avaya.com | 135.55.68.85:60834 |   SIP |                  Avaya Flare Engine |
2015-09-30 18:42:58 |  32646/3589 |  32646/4788 |  32646/4788 |     -/-  |      -/-
```

Sample output 2

#/opt/Avaya/snap_in/ps/bin/presClients -u 2600002@avaya.com -p

```
Active Presence Server Client Connections
      userid       |      ipaddress      |   lastpublishtime
-------------------+---------------------+---------------------
2600002@avaya.com | 135.55.68.145:52308 | 2016-02-26 15:45:11
PIDF:
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<presence entity="pres:2600002@yash.ps.avaya.com" xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:avav="urn:avaya:com:presence:rpid:availability"
xmlns:avcl="urn:avaya:com:PS:rpid:vclass" xmlns:pscaps="urn:com:avaya:pidf:servcaps:ps"
xmlns:d="urn:ietf:params:xml:ns:pidf:data-model"
xmlns:caps="urn:ietf:params:xml:ns:pidf:caps" xmlns:r="urn:ietf:params:xml:ns:pidf:rpid"
xmlns:apas="urn:com:avaya:pidf:rpid:extended" xmlns:cc="urn:com:avaya:presence:cc">
<tuple id="enterprise-im_b137287c-bdc2-5c3a-92a1-06d7628eea5d">
<status>
<basic>open</basic>
</status>
<r:class>Enterprise IM</r:class>
<avcl:vClass>Avaya.1XC</avcl:vClass>
<r:activities>
<avav:available/>
</r:activities>
<contact>2600002@yash.ps.avaya.com</contact>
<timestamp>2016-02-26T10:45:11.112-05:00</timestamp>
</tuple>
<tuple id="video_b137287c-bdc2-5c3a-92a1-06d7628eea5d">
<status>
<basic>closed</basic>
</status>
<r:class>Video</r:class>
<avcl:vClass>Avaya.1XC</avcl:vClass>
<r:activities>
<avav:offline/>
</r:activities>
<contact>sips:2600002@avaya.com</contact>
<timestamp>2016-02-26T10:45:11.111-05:00</timestamp>
</tuple>
<tuple id="phone_b137287c-bdc2-5c3a-92a1-06d7628eea5d">
<status>
<basic>open</basic>
</status>
<r:class>Phone</r:class>
<apas:extended-state>
<apas:phonestate>
<apas:onhook/>
</apas:phonestate>
</apas:extended-state>
<avcl:vClass>Avaya.1XC</avcl:vClass>
<r:activities>
<avav:available/>
```

```
</r:activities>
<contact>sips:2600002@avaya.com</contact>
<timestamp>2016-02-26T10:45:11.111-05:00</timestamp>
</tuple>
<d:person id="ps_generated">
<r:activities>
<avav:available/>
</r:activities>
<avav:availabilityDescription>
<avav:component type="overall-presence-state"/>
</avav:availabilityDescription>
</d:person>
</presence>
```

presHealthCheck

This CLI command is used to manually check the health of the Presence Services Snap-in on Avaya Breeze™. The health checks are the same ones normally executed by the Health Monitor. Running the **presHealthCheck** command does not result in any logs or alarms regardless of the results of the check.

Sample output 1

```
# /opt/Avaya/snap_in/ps/bin/presHealthCheck -h
```

```
Presence Services Health Check Tool
Runs all health checks that are normally executed by the Health Monitor.
Running health checks from this tool does not result in any logs or alarms regardless of
the results of the checks.
Usage: presHealthCheck
       -h Prints this help
```

Sample output 2

```
# /opt/Avaya/snap_in/ps/bin/presHealthCheck
```

```
Results are:
FederationDomainsHealthChecks:overlappingDomainsAcrossFederationConfigurations FAILED
FederationDomainsHealthChecks:overlappingDomainsAcrossSmgrConfiguredDomains PASSED
AesCollectionHealthChecks:checkForWatchingTooManyUsers PASSED
AesCollectionHealthChecks:checkForAbandonedUsers PASSED
```

presStatus

This script enables the user to view the status of components. The script provides an option to view all components or to view a specific component.

Sample output 1

```
# /opt/Avaya/snap_in/ps/bin/presStatus -h
```

```
Component not specified
Presence Services Status Script
Usage: presStatus [-u JMX_user] [-p JMX_port] [-pass JMX_password] [-i Node_IP] [-r | -h]
ComponentName
```

```
Valid components are: ps, aes, exchange, domino or all
Options: -r real-time status update (default option)
-h historical status records
--help
```

Sample output 2

```
# ./presStatus
```

```
com.avaya.presence.om:type=PsMetrics,10.138.255.255
PS Startup=Mon Dec 07 17:18:22 EST 2015
PS Version=7.0.1.0.18000
EDP Base Version=3.1.1.0.50009
Provisioned Users=6
Maximum Supported Users=1000
Geographic Redundancy Enabled=false
Cluster Name=jvh-core-platform
HA Enabled=FALSE
Number of Local Partitions=2
Total number of Active Partitions=2
Total number of Backup Partitions=0
com.avaya.presence.om:type=AesMetrics,10.138.255.255
Configured State=Enabled
Total Users=3
Watched Users=3
Abandoned Users=0
TLink=AVAYA#CMLAB1#CSTA-S#AESLAB1, Connected=TRUE, Cm=47.11.253.253, Aes=10.138.254.254,
Reason=Connected
com.avaya.presence.om:type=ExchangeMetrics,10.138.255.255
Configured State=Disabled
Number of Users=0
Calendar Next Poll=n/a
Out-Of-Office Next Poll=n/a
Publish Next Poll=n/a
Server Uri=https://pslabexchange.ca.yourdomain.com/ews/exchange.asmx
Connected=False
Reason=Idle/Not configured
com.avaya.presence.om:type=DominoMetrics,10.138.255.255
Configured State=Disabled
Number of Users=0
Calendar Next Poll=n/a
Out-Of-Office Next Poll=n/a
Publish Next Poll=n/a
Server Uri=http://10.138.252.252
Connected=False
Reason=Idle/Not configured
```

smgrPresenceUserAccessControl

This script is a user level access control script that enables user-level configuration of access control. This script is packaged with the Presence Services tools on Avaya Breeze™. This script will not run on Avaya Breeze™ and therefore must be transferred to a directory on System Manager.

This script replaces the presuseracls tool used in Presence Services Release 6.2.4. However, the presuseracls tool is still used in Presence Services Release 6.2.4.

To run the script, type sh smgrPresenceUserAccessControl on the System Manager command line. This will display online help. Refer to the online help of the script for full detailed usage information.

Sample output

```
root >sh smgrPresenceUserAccessControl -h
```

```
Description: This script can be used to view, create, modify or delete Presence Services
user level access control.
Partial input can be used to view a list of matching presentities/watchers.
This script must be run on the SMGR server with user root.
All presentity/watcher inputs are based on the SMGR full login name - not the SIP or
Presence/IM Communication Addresses.
Usage: sh smgrPresenceUserAccessControl -create) allow|block presentity watcher - create
access control
Usage: sh smgrPresenceUserAccessControl -create) allow|block presentity -ext watcher -
create access control for an external watcher
Usage: sh smgrPresenceUserAccessControl -modify) allow|block presentity watcher - modify
access control
Usage: sh smgrPresenceUserAccessControl -delete) presentity - delete all access control
for a presentity
Usage: sh smgrPresenceUserAccessControl -delete) presentity watcher - delete access
control for a presentity watcher pair
Usage: sh smgrPresenceUserAccessControl --delete-allow - delete all allow access control
for every user
Usage: sh smgrPresenceUserAccessControl --delete-block - delete all block access control
for every user
Usage: sh smgrPresenceUserAccessControl --delete-all - delete all access control for
every user
Usage: sh smgrPresenceUserAccessControl -p [presentity] - show presentity access control,
shows all if presentity is not specifiedt
Usage: sh smgrPresenceUserAccessControl -w [watcher] - show watcher referenced access
control, shows all if presentity is not specified
Usage: sh smgrPresenceUserAccessControl -h - show this help
Usage: sh smgrPresenceUserAccessControl presentity - show presentity access control
```

Creating a user level access control

Before you begin

- Transfer the `smgrPresenceUserAccessControl` file from the Presence Services CLI tools directory of Avaya Breeze™ to the System Manager folder.
- Start an SSH session using PuTTY and connect to the System Manager server using the IP addresses.

Procedure

1. Log in to the System Manager CLI as a root user.
2. Run `sh smgrPresenceUserAccessControl -c [allow | block] presentityloginname watcherloginname` to create a user level Access Control for a particular presentity watcher login name.

Deleting a user level access control

Before you begin

- Transfer the `smgrPresenceUserAccessControl` file from the Presence Services CLI tools directory of Avaya Breeze™ to the System Manager folder.

- Start an SSH session using PuTTY and connect to the System Manager server using the IP addresses.

Procedure

1. Log in to the System Manager CLI as a root user.
2. Get the presentityloginname information from the System Manager for the Access Control that needs to be deleted.
3. Type `sh smgrPresenceUserAccessControl –d presentityloginname` and press `Enter` to delete user level Access Control for a particular presentity login name.

Viewing a user level access control

Before you begin

- Transfer the `smgrPresenceUserAccessControl` file from the Presence Services CLI tools directory of Avaya Breeze™ to the System Manager folder.
- Start an SSH session using PuTTY and connect to the System Manager server using the IP addresses.

Procedure

1. Log in to the System Manager CLI as a root user.
2. Type one of the following:
   - `sh smgrPresenceUserAccessControl presentityloginname`, and press `Enter` to display all the user level ACLs for a particular presentity login name.
   - `sh smgrPresenceUserAccessControl`, and press `Enter` to display all the user level ACLs.

presCollectMetrics

The **`presCollectMetrics`** command-line tool can be used to discover real-time and historical data about the Presence Services system.

Syntax

`presCollectMetrics [-u JMX user] [-p JMX port] [-P JMX password] [-i node IP] [-r | -h] <Metrics>`

Options:

- `–u JMX user`
- `–p JMX port`
- `–P JMX password`
- `–I node IP`

- `–r`: Real-time metrics.

  By default, the real-time metrics is displayed for all components when no parameters are specified.
- `–h`: Historical metrics.
- *`Metrics`*: The valid metrics are `sip`, `gigaspaces`, and `xmpp`.

Sample output 1

```
# presCollectMetrics Gigaspaces
```

```
com.avaya.presence.om:type=GigaspacesMetrics,10.136.1.94
        CPU Percentage=0.33%
        Heap Usage (MB)=104.83
        Object Count=1803
        Thread Count=211
```

Sample output 2

```
# presCollectMetrics sip
```

```
com.avaya.presence.om:type=SipMetrics,10.136.1.94
        Active Subscriptions (Incoming)          = 4
               Directed                          = 1
               RLMI                              = 1
               Dynamic List                      = 0
               ACL                               = 1
               Winfo                             = 1
        Active Subscriptions (Outgoing)          = 60

        Active IM Sessions
               Incoming                          = 0
               Outgoing                          = 0

        Counters
        --------
        Publishes                                = 0
        Notifications                            = 0
        Instant Messaging
               In-Dialog Messages                = 0
               Out-of-Dialog Messages (Incoming) = 0
               Out-of-Dialog Messages (Outgoing) = 0
```

In a multi-node Presence Services cluster, it is possible to collect metrics for a particular node, by specifying the management IP address of that node.

Sample output 3

```
# presCollectMetrics -i 10.136.1.94
```

```
com.avaya.presence.om:type=SipMetrics,10.136.1.94
        Active Subscriptions (Incoming)          = 4
               Directed                          = 1
               RLMI                              = 1
               Dynamic List                      = 0
               ACL                               = 1
               Winfo                             = 1
        Active Subscriptions (Outgoing)          = 60

        Active IM Sessions
               Incoming                          = 0
               Outgoing                          = 0

        Counters
        --------
```

```
        Publishes                                = 0
        Notifications                            = 0
        Instant Messaging
               In-Dialog Messages                = 0
               Out-of-Dialog Messages (Incoming) = 0
               Out-of-Dialog Messages (Outgoing) = 0


Failed to connect to PS (failed to lookup mbean for: Xmpp)
com.avaya.presence.om:type=GigaspacesMetrics,10.136.1.94
        CPU Percentage=0.32%
        Heap Usage (MB)=149.23
        Object Count=1805
        Thread Count=211
```

It is possible to retrieve data about a metric type from the past 24 hours by using the -h parameter. The data is collected by the system every five minutes for up to 24 hours. When using the -h parameter, a comma-separated value (CSV) file is written to the disk. This CSV file can be loaded into a program such as, Microsoft Excel or can be used to generate a graph using the **presGraphMetrics** command-line tool.

Sample output 4

```
# presCollectMetrics -h sip
Wrote : psng-gigaspaces-20160314102531.csv
```

presGraphMetrics

This command is used to get graph historical metric data generated by the **presCollectMetrics** command-line tool. The --help parameter displays how it is used.

Syntax

`presGraphMetrics -f` *`CSV Filename`* `-T1|24 -t`

Options:

- `–f`: File name.
- `–T1|T24`: T1 will display the metrics from the last hour. T24 will display the metrics from the last 24 hours.
- `–t`: Total count

Sample output 1

```
# presGraphMetrics --help
```

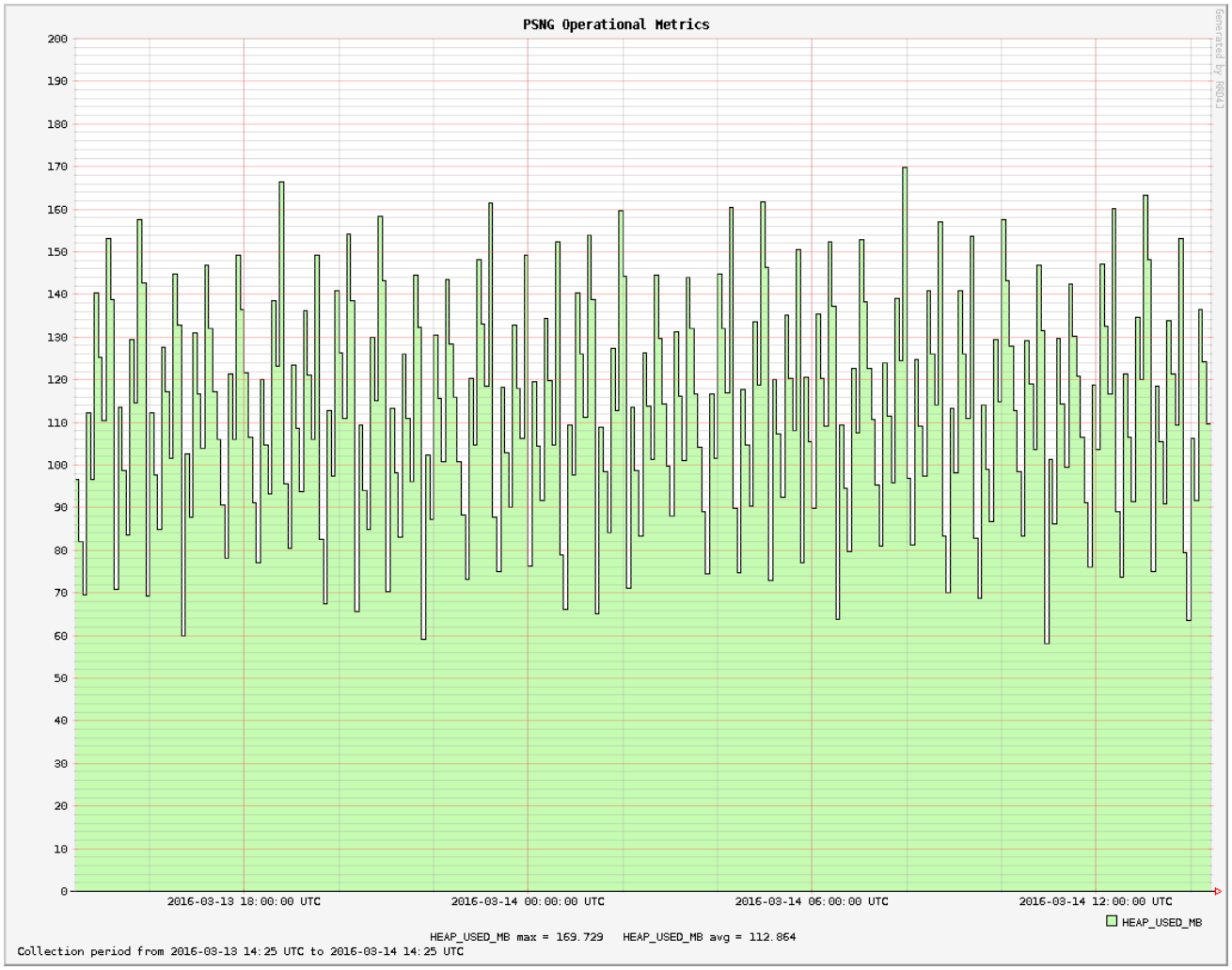
```
Invalid option: --
Presence Services Graph Metrics Tool
 Usage: presGraphMetrics -f <CSV Filename> -T<1|24> <Column Names To Graph ...>
 e.g. presGraphMetrics -f psng-gigaspaces.csv -T24 THREAD_COUNT WRITE READ
 -t show Total Count
 where T 1 = Last hour or 24 = Last 24 hours
```

Sample output 2

```
# presGraphMetrics -f ./psng-gigaspaces-0160314102531.csv -T24
HEAP_USED_MB
```

```
== Graph completed in 1.056 sec
filename = "psng-20160314103301.png"
width = 1104, height = 867
byteCount = 32778
imginfo = "<img src='psng-20160314103301.png' width='1104' height = '867'>"
No print lines found

Wrote : psng-20160314103301.png
```

The resulting PNG graphics file can be loaded by an image viewing program.



Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X