Avaya Aura® Presence Services Snap-in Reference

Release 7.1.2
Issue 6
June 2021

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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. 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.

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, unless otherwise stated, 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.

Contents

Chapter 1: Introduction 10
Purpose 10
Change history 10
Chapter 2: Presence Services snap-in description 12
Presence Services overview 12
Local Presence Service 13
PS connector 13
Presence Services architecture 14
New in this release 7.1.2 15
New in this release 17
Key features of Presence Services 18
Feature comparison 19
Chapter 3: Interoperability 20
Product compatibility 20
Chapter 4: Licensing 21
Licensing 21
Chapter 5: Deployment 22
Planning 22
Cluster considerations 22
Key customer configuration information 23
Presence Services single-server deployment 24
Checklist for deploying a single-server Presence Services cluster 24
Presence Services multi-server deployment 35
Checklist for deploying a multi-server Presence Services cluster 36
Presence Services geographically redundant deployment 37
Checklist for deploying a geographically redundant Presence Services clusters 38
Administering System Manager LHNR to resolve Presence Services Cluster FQDN to Avaya Breeze™ Security Module IP address of remote data centers 40
Administering Geographic Redundant Avaya Breeze™ Cluster to an existing Managed Element 41
Administering Avaya Aura user for Geographic Redundancy 42
Administration of Avaya Aura devices for Geographic Redundancy 42
Presence Services uninstallation and deletion 43
Uninstalling a snap-in service 43
Deleting a snap-in service 43
Chapter 6: Migration and upgrades 45
Upgrading from Presence Services 7.0.x to Presence Services 7.1 45
Checklist for upgrading a Geographic Redundant deployment 46
Disabling access to a data center 47

Disabling DNS ... 49
Disabling Session Manager ... 49
Disabling Avaya Breeze™ cluster running Presence Services ... 49
Enabling access to a data center ... 49
Enabling Avaya Breeze™ cluster running Presence Services ... 51
Enabling Session Manager ... 51
Enabling DNS ... 51
Considerations for upgrading Microsoft Federation deployment to Release 7.1 ... 52
Chapter 7: Administration ... 53
Access control policy ... 53
Configuring access control policy ... 54
Collectors ... 54
AES Collector ... 54
Exchange Collector ... 57
Domino Collector ... 64
Federation ... 83
Microsoft Real Time Communication (RTC) Federation ... 83
Microsoft federation with external domains ... 98
Microsoft federation with internal Avaya Aura domain and external Microsoft domain ... 138
Microsoft federation with internal and external domains using inter-PS federation ... 141
Inter-PS federation ... 146
XMPP federation ... 151
XMPP federation with NextPlane ... 168
XMPP Federation with Cisco Jabber ... 168
Zang Federation ... 183
IM Blocking in Do Not Disturb state ... 188
Configuring IM Blocking in Do Not Disturb state ... 188
Accessing the Presence Services Software Inventory web service ... 189
Instant Message Broadcast Tool ... 190
Using Instant Message Broadcast Tool ... 190
Interoperability with Avaya Multimedia Messaging ... 193
Key customer configuration information ... 195
Checklist for administering Avaya Multimedia Messaging ... 196
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 ... 197
Administering Avaya Multimedia Messaging SIP Entity ... 197
Administering home Avaya Multimedia Messaging Cluster of the user ... 198
Administering Avaya Breeze™ Cluster for Avaya Multimedia Messaging interoperability ... 198
Administering Avaya Multimedia Messaging Service Attributes ... 199
Modifying Presence Services Security Module HTTPS identity certificate ... 200
Modifying Presence Services WebSphere identity certificate ... 202
Multi-User Chat ... 204
Inter-Domain Presence and IM ... 206

Configuring Inter-Domain Presence and IM.......... 206
Inter-Tenant Presence and IM.......... 207
Configuring Inter-Tenant Presence and IM.......... 207
Managing users.......... 208
Soft delete vs. hard delete.......... 208
Message Archiver.......... 208
Enabling Message Archiver.......... 210
Multi-tenancy.......... 211
Offline IM Storage.......... 212
Configuring Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route.......... 212
Port management.......... 215
Changing a service port.......... 215
Roster size enforcement.......... 216
Configuring Roster Limit.......... 217
Network Management System configuration.......... 218
Configuring System Manager.......... 218
Exporting the MIB file.......... 221
Installing OpenNMS.......... 223
Starting OpenNMS.......... 225
Configuring Linux firewall.......... 226
Accessing the OpenNMS web console.......... 226
Importing MIB files into OpenNMS.......... 226
Modifying OpenNMS event definitions.......... 228
Creating OpenNMS node elements.......... 229
Testing the OpenNMS installation.......... 230
Viewing the Alarm events in OpenNMS.......... 231
Restarting Presence Services.......... 233
Chapter 8: Certificate Management.......... 235
Adding Subject Alternative Name DNS name to Security Module HTTPS Identify Certificate.......... 235
Add Subject Alternative Name DNS name and Other Name (XMPP Address) to WebSphere Identify Certificate.......... 236
Exporting Openfire Certificate (Linux).......... 236
Exporting Openfire Certificate (Windows).......... 237
Importing certificate into Cluster Truststore.......... 237
Importing System Manager root CA certificate into Openfire Truststore (Windows).......... 238
Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store.......... 239
Creating Entity Profile on System Manager.......... 239
Generating a certificate signing request on the Openfire server.......... 240
Signing the Openfire certificate signing request (CSR) on System Manager.......... 241
Installing the System Manager CA and Signed Openfire Certificate on Openfire.......... 241
Retrieving a System Manager CA signed Certificate.......... 242

Checklist for generating new identity certificate signed by System Manager.... 242
Creating a Certificate Signing Request.... 243
Creating an end entity on System Manager.... 244
Creating the Signed Identity Certificate using the CSR.... 244
OpenSSL command to view the signed certificate.... 245
Generating new identity certificate from a third-party CA.... 246
Presence components and identity certificates.... 246
Installing far-end Trust Certificates in Avaya Breeze™.... 248
Chapter 9: Service Attributes.... 249
Service Attributes.... 249
Presence Services Service Attributes.... 249
Chapter 10: User and device administration.... 261
User and device administration.... 261
Categories of Presence/IM devices.... 261
Checklist for configuring Presence/IM users.... 262
Configuring Presence/IM routing domain on System Manager.... 264
Assigning Communication Profile Password to a user on System Manager.... 265
Assigning Avaya Presence/IM communication address to user on System Manager.... 265
Assigning Presence Profile to a user on System Manager.... 266
Enabling Application Enablement Services collection for a user on System Manager.... 267
Exporting certificate chain that signs the Session Manager identity.... 268
Importing certificate chain that signs Session Manager identity into device truststore.... 269
Exporting certificate chain that signs the Presence Services identity.... 274
Importing certificate chain that signs the Presence Services identity into device truststore... 275
Checklist for administering Presence and IM on a device.... 281
Manual presence state expiration time.... 283
Chapter 11: Performance.... 285
Capacity and scalability specification.... 285
Chapter 12: Security.... 288
Port utilization.... 288
Chapter 13: Troubleshooting.... 289
Presence Services alarms.... 289
Number of contact rosters exceeds the system limit.... 295
Number of provisioned users is over the configured attribute limit.... 295
Number of configured users is over the support limit.... 296
No DNS SRV records found for any Presence domain for XMPP Federation.... 296
Signaling security health check alarms.... 296
Cluster misconfigured health check alarms.... 297
Load Balancer is not enabled on a multi-node cluster.... 297
No FQDN is configured for a Service IP IP_ADDRESS.... 297
Server does not have an associated Presence Services managed element.... 297
Managed element is not assigned to the current cluster.... 298
Network outage causes presence to stop working for some or all users.... 298

Presence and IM fails on SIP endpoints due to the PPM getHomeCapabilities fault.................. 298
Unable to get _People View.. 299
Vysper fails to start when no domains are created in System Manager.................................... 300
Changing the logging level.. 300
Repairing replication between Avaya Breeze™ and System Manager....................................... 301
Verifying that Presence Services snap-in is ready to support Presence and IM.......................... 301
Geographic Redundancy.. 303
Failure and Recovery.. 303
Chapter 14: Resources.. 304
Documentation.. 304
Finding documents on the Avaya Support website.. 304
Accessing the port matrix document.. 305
Training.. 305
Viewing Avaya Mentor videos.. 306
Support.. 306
Appendix A: CLI commands.. 307
presAlarmTest.. 307
presCleanup.. 308
presClients.. 308
presCollectMetrics.. 310
presGraphMetrics.. 312
presHealthCheck.. 313
presUnlock.. 314
presStatus.. 315
smgrPresenceUserAccessControl.. 316
Creating a user level access control.. 317
Deleting a user level access control.. 317
Viewing a user level access control.. 317

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
6	June 2021	Removed “Avaya Product requirements” section as it is same as the “Product compatibility” section.
5	January 2020	Added the following sections:. • Manual presence state expiration time • Configuring manual presence state expiration time
4	September 2019	“Accessing the port matrix document” section is added.
3	January 2018	Updated the “Key features of Presence Services” section. Updated the “Avaya Product requirements” section.

Table continues…

Issue	Date	Summary of changes
2	December 2017	• Added the “Subscribe for status with Microsoft RTC and Publish status to Microsoft RTC” section. • Added the “Microsoft federation with internal Avaya Aura domain and external Microsoft domain” section. • Added the “Checklist for configuring Microsoft federation with internal Avaya Aura domain and external Microsoft domain” section. • Added the “Configuring Presence Services attributes to enable tandem domain support” section. • Updated the “Administering DNS SRV records to resolve Avaya Multimedia Messaging conference services” section. • Updated the “Administering DNS SRV records to resolve external XMPP federation system conference services” section. • Updated the “Checklist for administering Avaya Multimedia Messaging” section. • Updated the “Multi-User chat” section. • Deleted the “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” section.
1	May 2017	Initial release

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

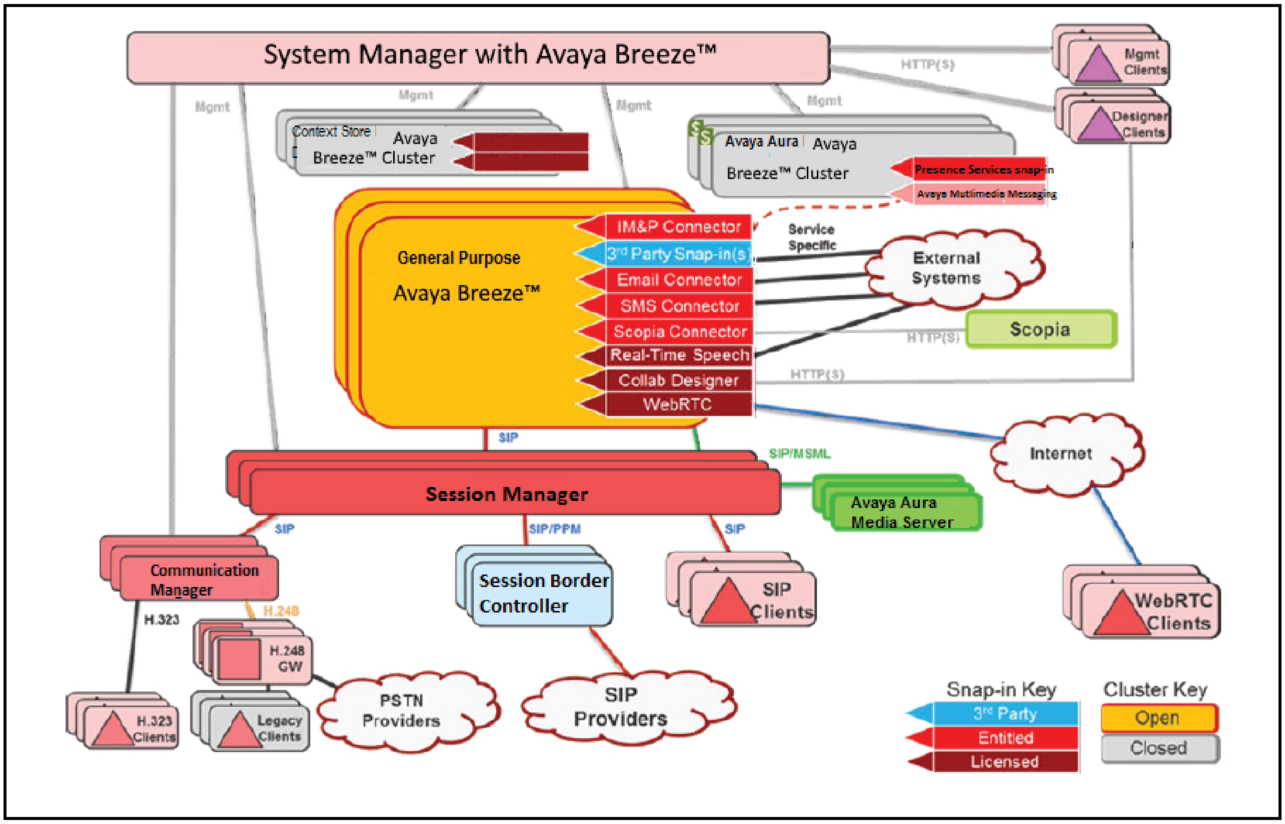


Figure 1: Avaya Breeze™ architecture

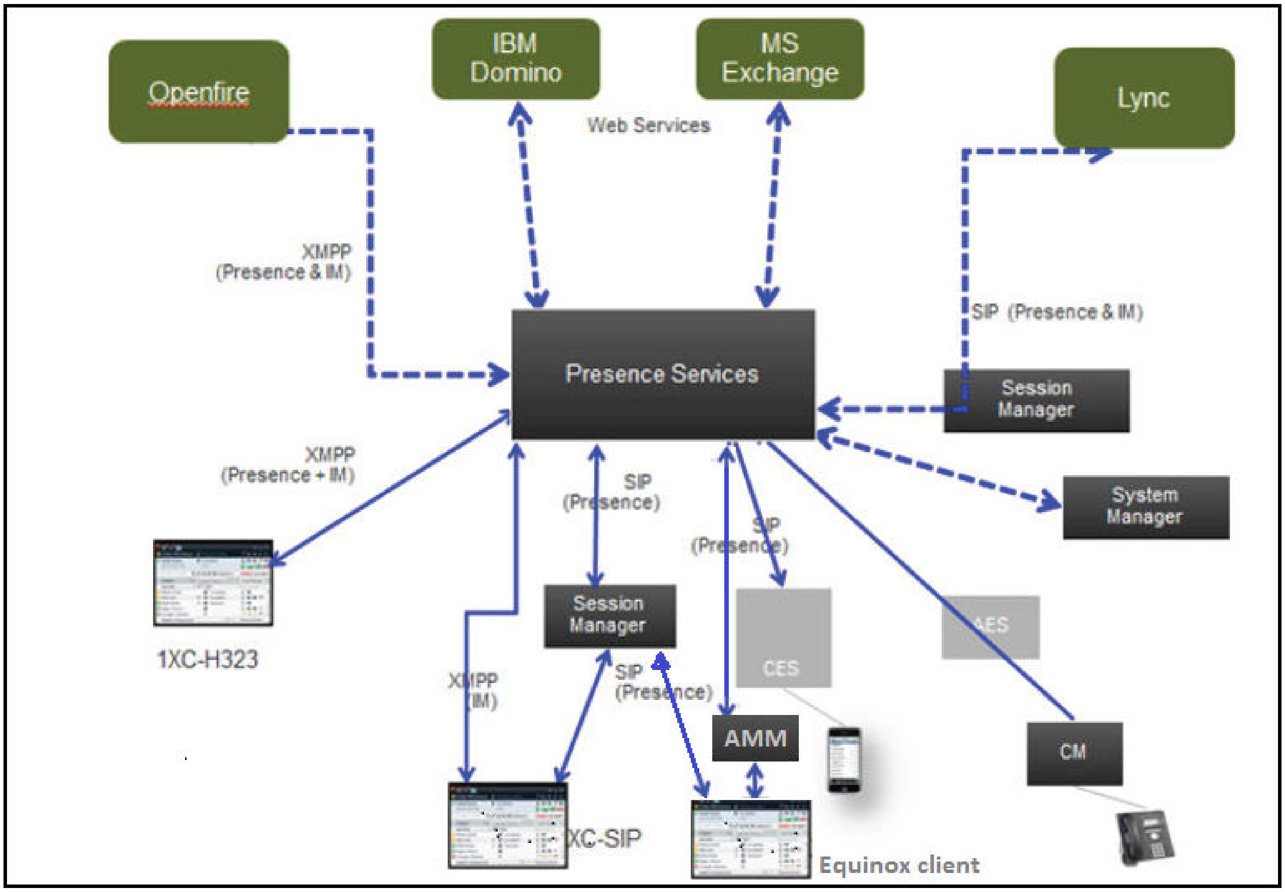


Figure 2: Presence Services snap-in architecture

New in this release 7.1.2

This section provides an overview of the new and enhanced features of Presence Services Release 7.1.2.

Zang federation

Presence Services Release 7.1.2 supports Zang federation. This feature enables:

- Sending IMs as SMS to a mobile user.
- Receiving SMS from a mobile user and deliver it as IM to an Aura user.

Support for generic XMPP federation

Presence Services Release 7.1.2 supports generic federation with other XMPP servers. Any standards based XMPP server is supported using the generic XMPP federation.

Support KVM deployment

Presence Services Release 7.1.2 supports deployment on Kernel-based Virtual Machine (KVM).

KVM is a full virtualization solution for Linux on x86 hardware. Using KVM, you can run multiple virtual machines that run various Avaya Aura components, including Presence Services on Breeze.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

For more information, see *Deploying Avaya Breeze™ on Kernel-based Virtual Machine for Avaya Aura®*..

Support for Interoperability among clients

Presence Services Release 7.1.2 is compatible with existing Avaya endpoints that are used with Presence Services Release 7.x.

Presence/IM capable devices:

- Avaya Equinox 3.0, 3.1, 3.2 & 3.3
- 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

Support for a privileged user

Presence Services Connector Release 7.1.2 supports a Service Attribute “Privileged User”, which will accept the login name of the presence-enabled Avaya Aura user. If you are using Equinox Attendant, then attendant user's login name is accepted.

For Equinox Attendant, ensure that only the attendant user has a service profile associated with Equinox Attendant snap-in.

S4B interoperability with AMM using Federation Relay

Presence Services Release 7.1.2 supports additional routing assistance when AMM is included in Presence Services and Microsoft federation deployments.

If AMM is deployed, then the Session Manager routes IM messages to AMM. Else, Federation Relay will add a new flag “av-msfe-imgw” for IM messages, which will direct the Session Manager to route the IM messages to AMM. The flag allows the Session Manager to identify the Presence and IM messages, and route them to different destinations as required.

Support for self-identity using REST API

Presence Services Release 7.1.2 supports self-identify using the following REST API:

`application/vnd.avaya.presence-im.user-identity.v1+json`

Adding User's ACL Policy to discover server capabilities

Presence Services Release 7.1.2 supports User's ACL Policy , which is dynamic in nature that discovers Presence Services server capabilities.

Support for Microsoft RTC status

Presence Services Release 7.1.2 supports the following:

- Subscribe for status with Microsoft RTC
- Publish status to Microsoft RTC

Supported migration paths

The supported migration paths for Presence Services Release 7.1.2 are:

Release	Requirement
7.0.0.x	Direct upgrade to 7.1.2.
7.0.1.x	Direct upgrade to 7.1.2.
7.1.0	Direct upgrade to 7.1.2.

New in this release

This section provides an overview of the new and enhanced features of Presence Services Release 7.1.

IPv6 Compliance

Presence Services supports dual stack. Therefore, Presence Services supports installation with IPv4 and IPv6 addresses.

Presence Services complies with the IPv6 CEC requirements.

Compliance with DISA security STIGs

Presence Services is now compliant with the security requirements stated in Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG).

Federation with Nextplane

Presence Services supports federation with Nextplane.

Support for Multi User chat with Avaya Multimedia Messaging

Presence Services can interoperate with Avaya Multimedia Messaging (AMM) and an external XMPP federation system, such as Openfire, to support XEP-0045 style Multi-User Chat between AMM-enabled users and external XMPP federation users.

Support for data filtering option

Presence Services implements a data filtering option to support:

- Reduce body size of the NOTIFY requests sent by Presence Services to endpoints.
- Reduce rate of notifications received by subscribing endpoints.

Support for Interoperability among clients

Presence Services Release 7.1 is compatible with existing Avaya endpoints that are used with Presence Services Release 6.2.x and 7.0.x. 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

Presence Services 7.1 is compatible with AMM 3.0, and with the new endpoints that support Rich Messaging.

Supported migration paths

The supported migration paths for Presence Services Release 7.1 are:

Release	Requirement
6.x	Direct upgrade to 7.1.
7.0.0.x	Direct upgrade to 7.1.
7.0.1.x	Direct upgrade to 7.1.

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.
- Presence Services supports up to 2048 characters for XMPP IM.

Feature comparison

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

Feature	6.0	6.1	6.2	7.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

Product compatibility

For the latest and most accurate compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

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 virtual machine (VM) cluster or a multiple VM cluster:

- Single-VM cluster always runs in non-HA mode.
- Multi-VM cluster always runs in HA mode. Non-HA multi-VM clusters are not supported.
- A maximum of 10 VMs are permitted in a cluster. All VMs in the cluster must have the same Avaya Breeze™ profile. Refer to the following tables for possible deployments.
- The number of required VMs depends on the number of presence-enabled users that will be hosted by this cluster. For more information, see *Capacity and scalability specification*.
- Avaya Breeze™ Release 3.3 supports five VM profiles, each with different allocations of CPU, memory and disk space. During Avaya Breeze™ deployment, an Avaya Breeze™ 3.3 profile must be selected. For more information, see *Deploying Avaya Breeze™*. If Presence Services is the only snap-in deployed on the cluster, select the Avaya Breeze™ 3.3 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 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. The planned number of users dictates the minimum Avaya Breeze™ profile required in the initial deployment or the service will not start properly. For example, if the cluster is planned to eventually grow to 40,000 users, the minimum Avaya Breeze™ profile must be profile 5, even if only 5000 users are provisioned on the initial deployment. For information about administering the number of users, see “Configuring System service attributes”.

The following table summarizes the resource allocations of the different Avaya Breeze™ profiles:

Avaya Breeze™ profile	Number of vCPUs	CPU Reservation (Mhz)	Memory (GB)	Disk Space (GB)
2	4	9600	8	80
3	6	14400	10	80
4	8	19200	16	150
5	12	28800	27	300

Note:

Profile 1 cannot be used to deploy Presence Services.

The following table summarizes the possible deployments based around the planned number of users.

Planned Number of user	Number of VMs in a non-HA deployment	Number of VMs in an HA deployment	Minimum Avaya Breeze™ profile
1000	1	2	2
2400	1	2	3
5000	1	2	4
16,000	1	2	5
32,000	Not supported	3	5
48,000	Not supported	4	5
64,000	Not supported	5	5
80,000	Not supported	6	5
96,000	Not supported	8	5
110,000	Not supported	9	5
125,000	Not supported	10	5
250,000	Not supported	20 (two 10-VM clusters)	5

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	

Table continues…

No.	Requirement	Value
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	
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 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 the latest available Avaya Breeze™ on host server.	Deploying Avaya Breeze™ on page 26	
5	Confirm that Avaya Breeze™ successfully replicates with System Manager.	Confirming that Avaya Breeze successfully replicates with System Manager on page 29	
6	Administer Avaya Breeze™ SIP Entity.	Administering Avaya Breeze SIP Entity on page 29	
7	Administer *s* Entity Links between Avaya Breeze™ and Session Managers.	Administering Entity Link between Avaya Breeze and Session Manager on page 29	
8	Administer Presence Services Cluster SIP Entity.	Administering Presence Services Cluster SIP Entity on page 30	
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 30	
10	Administer Avaya Breeze™ server.	Administering Avaya Breeze server on page 31	
11	Administer Avaya Breeze™ cluster and assign Avaya Breeze™ server.	Administering Avaya Breeze cluster on page 32	

Table continues…

No.	Task	Reference	✔
12	Administer Presence Services on Avaya Breeze™ Managed Element.	Administering Presence Services on Avaya Breeze Managed Element on page 33	
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 33	
14	Administer Avaya Breeze™ alarming.	For information, see *Deploying Avaya Breeze™*.	
15	Load Presence Services snap-in.	Loading Presence Services snap-in on page 34	
16	Ensure that at least one routing domain is configured on System Manager.	Configuring Presence/IM routing domain on System Manager on page 264	
17	Install Presence Services snap-in on Avaya Breeze™ cluster.	Installing Presence Services snap-in on page 34	
18	Administer Presence Services System service attributes.	Administering Presence Services System service attributes on page 34	
19	Restart Presence Services.	Restarting Presence Services on page 233	
20	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 301	

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 the latest available Avaya Breeze™. 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 the appropriate Avaya Breeze™ replication group.
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 the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
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 the System Manager web console, click **Elements** > **Avaya Breeze™**.
2. In the navigation pane, click **Service Management** > **Services**.
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 **Number of users** service attribute within the System group is important to optimize performance of the cluster:

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

Note:

A Presence Services restart must be performed after changing this service attribute.

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 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 this service attribute, 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* latest available Avaya Breeze™ instances on *m* host servers.	Deployment of Avaya Breeze on page 26	
5	Confirm that *n* Avaya Breeze™s successfully replicate with System Manager.	Confirming that Avaya Breeze successfully replicates with System Manager on page 29	
6	Administer *n* Avaya Breeze™ SIP Entities.	Administering Avaya Breeze SIP Entity on page 29	

Table continues…

No.	Task	Reference	✔
7	Administer *n*s* Entity Links between Avaya Breeze™ and Session Manager.	Administering Entity Link between Avaya Breeze and Session Manager on page 29	
8	Administer one Presence Services Cluster SIP Entity.	Administering Presence Services Cluster SIP Entity on page 30	
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 30	
10	Administer *n* Avaya Breeze™ servers.	Administering Avaya Breeze server on page 31	
11	Administer one Avaya Breeze™ cluster and assign *n* Avaya Breeze™ servers.	Administering Avaya Breeze cluster on page 32	
12	Administer one Presence Services on Avaya Breeze™ Managed Element.	Administering Presence Services on Avaya Breeze Managed Element on page 33	
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 33	
14	Administer Avaya Breeze™ alarming.	For information, see *Deploying Avaya Breeze™*.	
15	Load Presence Services snap-in.	Loading Presence Services snap-in on page 34	
16	Ensure that at least one routing domain is configured on System Manager.	Configuring Presence/IM routing domain on System Manager on page 264	
17	Install Presence Services snap-in on Avaya Breeze™ cluster.	Installing Presence Services snap-in on page 34	
18	Administer Presence Services System service attributes.	Administering Presence Services System service attributes on page 34	
19	Restart Presence Services.	Restarting Presence Services on page 233	
20	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 301	

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 35	
2	Administer one multi-server Presence cluster in DC-2.	Presence Services multi-server deployment on page 35	
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 40	
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 40	
7	Administer DC-2 as Geo Redundant Cluster of DC-1.	Administering Geographic Redundant Avaya Breeze Cluster to an existing Managed Element on page 41	
8	Administer DC-1 as Geo Redundant Cluster of DC-2.	Administering Geographic Redundant Avaya Breeze Cluster to an existing Managed Element on page 41	
9	Restart Presence Services on both Presence Clusters.	Restarting Presence Services on page 233	
10	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 301	

Table continues…

No.	Task	Reference	✔
11	Administering Aura users for Geographic Redundancy.	Administering Avaya Aura user for Geographic Redundancy on page 42	
12	Administering devices for Geographic Redundancy.	Administration of Avaya Aura devices for Geographic Redundancy on page 42	

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

Upgrading from Presence Services 7.0.x to Presence Services 7.1

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 7.0.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

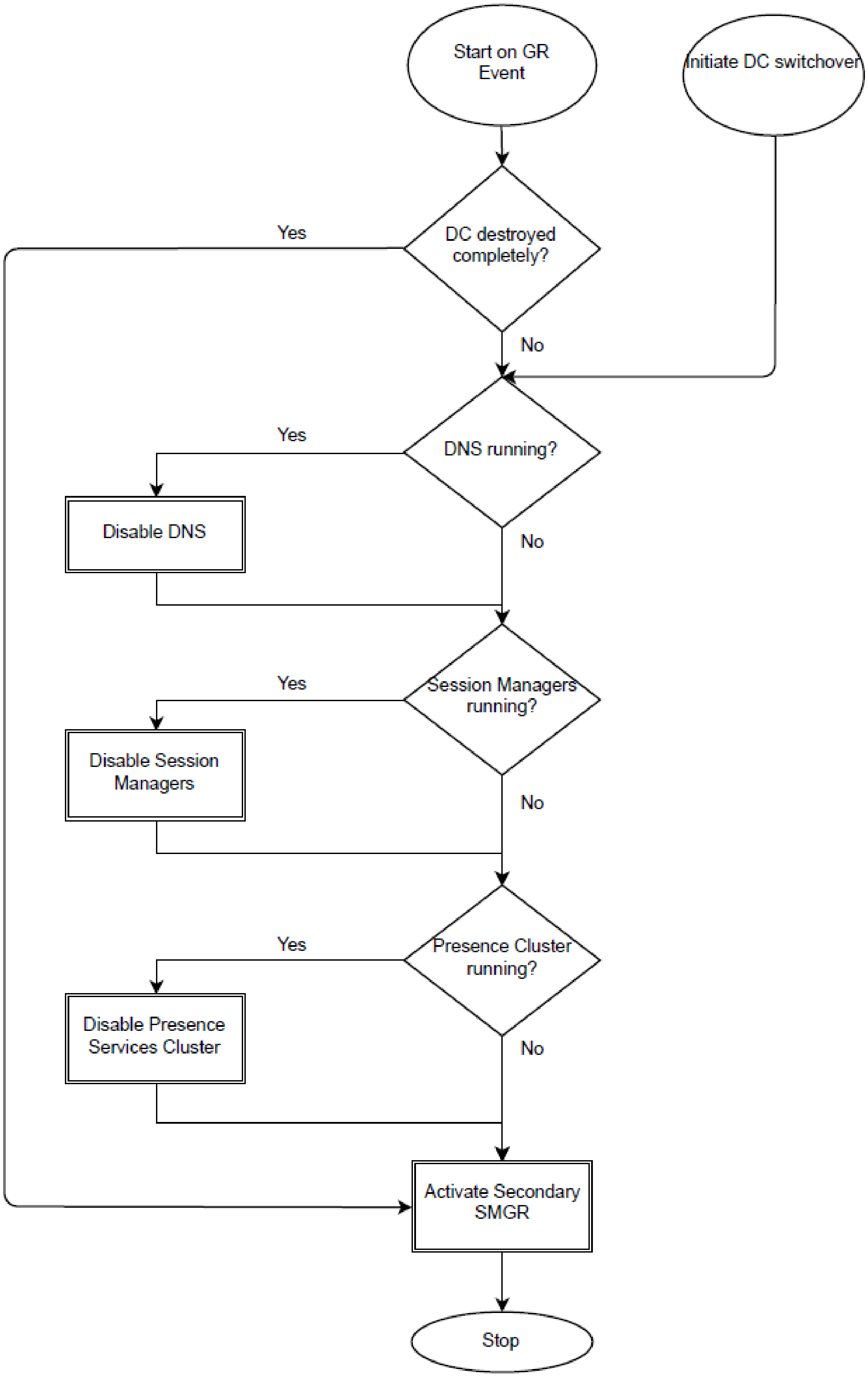
No.	Task	Reference	✔
1	Disable access to DC-1.	Disabling access to a data center on page 47	
2	Perform DC-1 upgrade	Upgrading from Presence Services 7.x to a newer version on page 45	
3	Enable access to DC-1.	Enabling access to a data center on page 49	
4	Disable access to DC-2	Disabling access to a data center on page 47	
5	Perform DC-2 upgrade	Upgrading from Presence Services 7.x to a newer version on page 45	
6	Enable access to DC-2	Enabling access to a data center on page 49	

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
No
Disable DNS
Session Managers running?
Yes
No
Disable Session Managers
Presence Cluster running?
Yes
No
Disable Presence Services Cluster
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**.

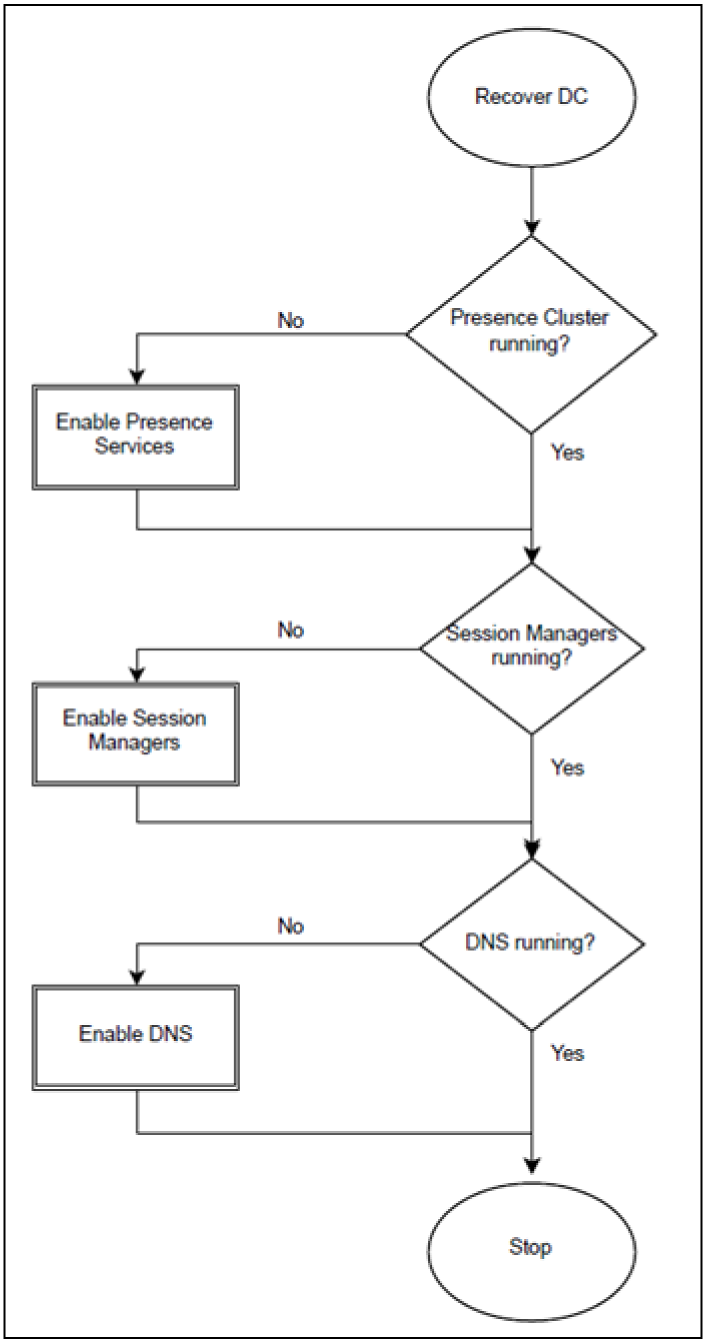
Disabling Avaya Breeze™ cluster running Presence Services

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.

Considerations for upgrading Microsoft Federation deployment to Release 7.1

For upgrading from Microsoft federation deployment Release 7.0.0 or 7.0.1 to Release 7.1, note the following:

- Presence Services configuration attributes earlier in the **Lync Federation** group are replaced with a new **Microsoft Federation** group. You must manually migrate to the new Microsoft Federation group for 7.1.
- Use of the AMM federation relay for Intra-enterprise federation is no longer required or supported.
- Intra-enterprise federation between two different domains is now supported. This federation works directly with the Microsoft Front End server and not the Microsoft Edge server as in previous 7.0.0 and 7.0.1 releases.
- Inter-enterprise federation between two different domains requires use of the at the edge of the Avaya Aura® network.

For more information, see “Microsoft Real Time Communication (RTC) Federation” section.

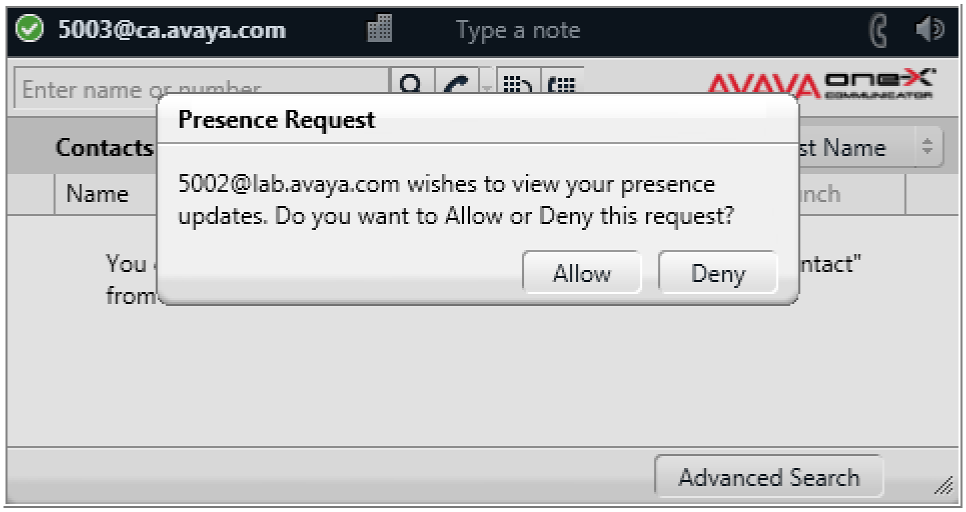
Chapter 7: Administration

Access control policy

Presence Services 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 7.1.

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.



Presence Request

5002@lab.avaya.com wishes to view your presence updates. Do you want to Allow or Deny this request?

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.

AES Collector network routing configuration

AES Collector connects to the AE Server using regular Linux routing rules. As the Avaya Breeze™ platform default network route is associated with the Management Network Interface, outbound connections to the AE Server will use the Management Network Interface by default.

To enable AES Collector to use the Security Module Network Interface, the AE Server must be on the same subnet as the Avaya Breeze™ Security Module Network Interface.

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 supports the following versions of MS Exchange Server:

- 2007
- 2010
- 2010 Service Packs
- 2013

Note:

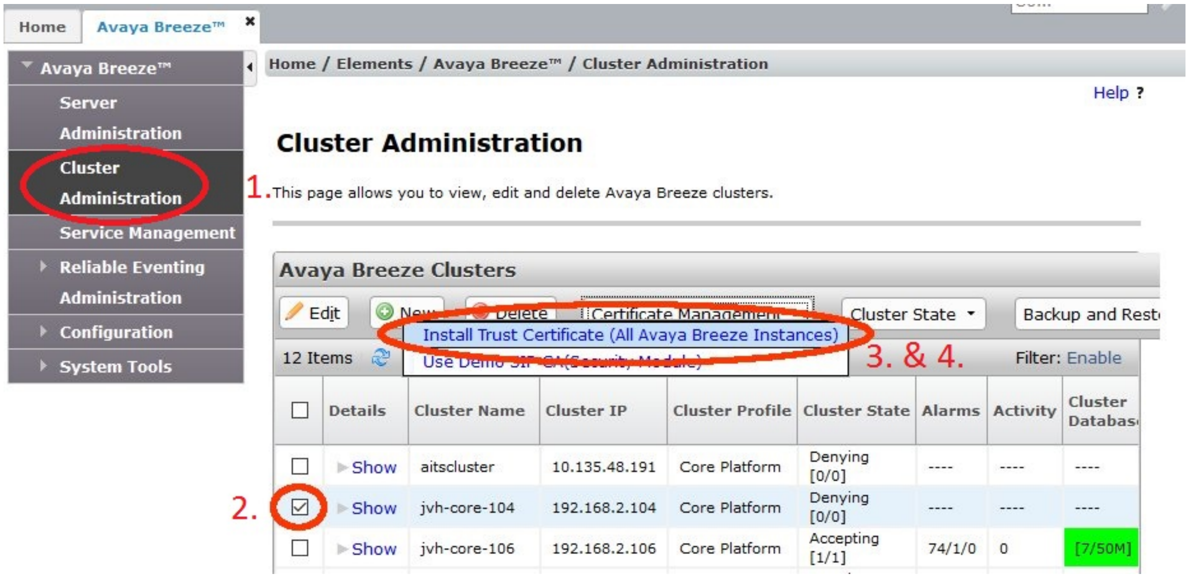
MS Exchange 2010 requires impersonation. However, for MS Exchange 2013, you must run the command **`Add-MailboxPermission -Identity username@domain -user psadmin -AccessRights FullAccess -InheritanceType all`** for all used mailboxes, instead of configuring impersonation. Before you run the command,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

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 installed, as the 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. The following sections will document how to export certificates from Microsoft Exchange server.

Importing certificate in Avaya Breeze™

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
2. Select the Avaya Breeze™ cluster to import the certificate into.
3. Click **Certificate Management**.
4. Select the **Install Trust Certificate (All Avaya Breeze Instances)** option.
5. On the Install Trusted Certificate page, in the **Store Type to install trusted certificate** field, select **ALL**.
6. Click **Browse** and select the certificate file exported earlier.
7. Click **Retrieve Certificate**.
8. Click **Commit**.



Home / Elements / Avaya Breeze™ / Cluster Administration

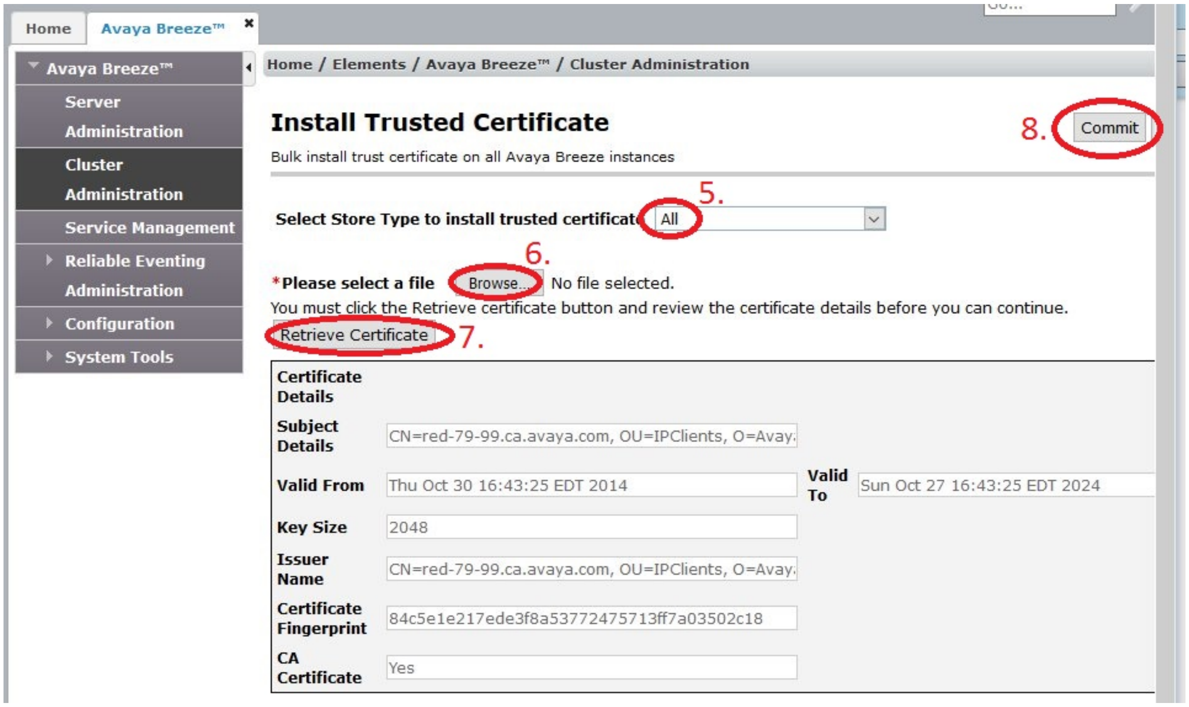
Cluster Administration

This page allows you to view, edit and delete Avaya Breeze clusters.

Avaya Breeze Clusters

12 Items Filter: Enable

☐	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Databas
☐	Show	aitscluster	10.135.48.191	Core Platform	Denying [0/0]	----	----	----
☑	Show	jvh-core-104	192.168.2.104	Core Platform	Denying [0/0]	----	----	----
☐	Show	jvh-core-106	192.168.2.106	Core Platform	Accepting [1/1]	74/1/0	0	[7/50M]



Install Trusted Certificate

Bulk install trust certificate on all Avaya Breeze instances

Select Store Type to install trusted certificate: All

*Please select a file: No file selected.

You must click the Retrieve certificate button and review the certificate details before you can continue.

Certificate Details

Subject Details: CN=red-79-99.ca.avaya.com, OU=IPClients, O=Avay.

Valid From: Thu Oct 30 16:43:25 EDT 2014

Valid To: Sun Oct 27 16:43:25 EDT 2024

Key Size: 2048

Issuer Name: CN=red-79-99.ca.avaya.com, OU=IPClients, O=Avay.

Certificate Fingerprint: 84c5e1e217ede3f8a53772475713ff7a03502c18

CA Certificate: Yes

Exporting certificates from Microsoft Exchange server

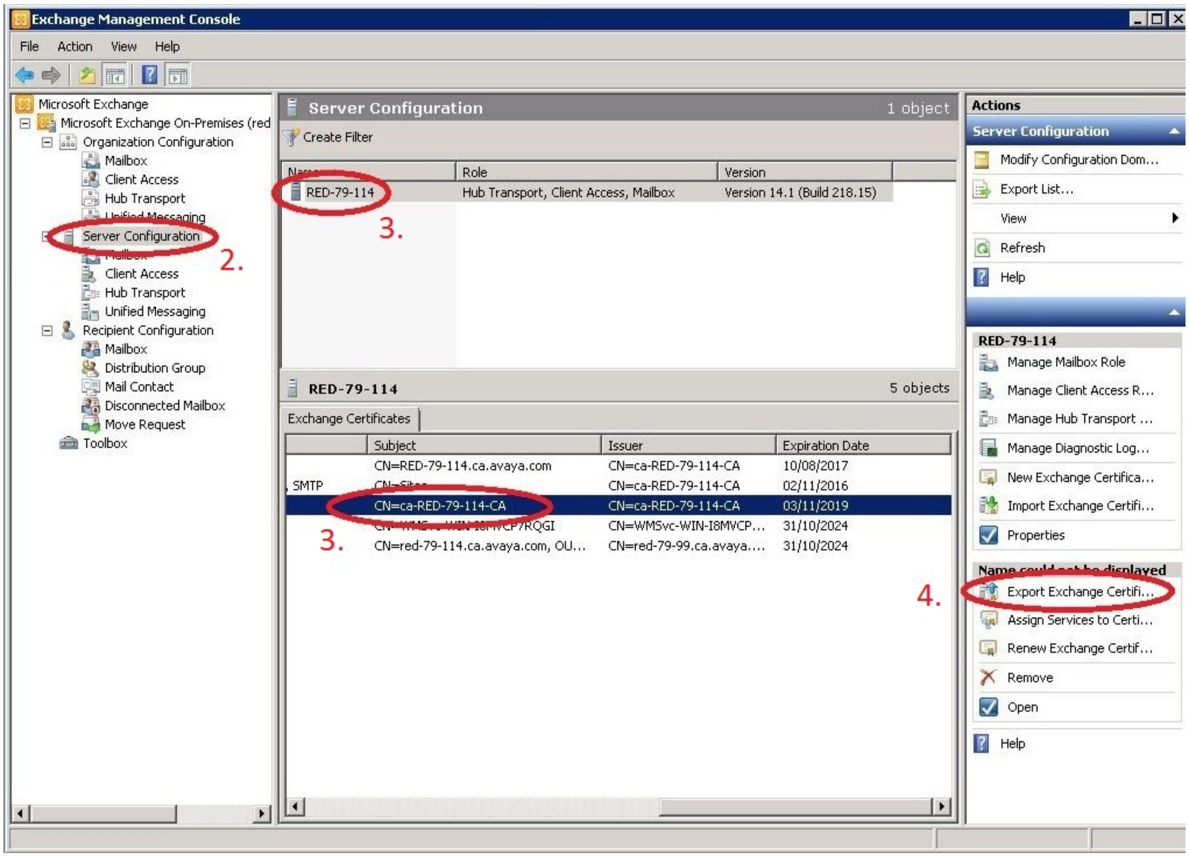
About this task

The following procedure describes how to extract the required certificate from an Exchange 2010 server. For newer versions of Microsoft Exchange, refer to Microsoft Exchange documentation.

Procedure

1. Start the Exchange Management Console.
2. Select **Server Configuration**.
3. Select the Exchange server from the list of servers in the top middle window.

4. Select **Export Exchange Certificate** from the **Action** list.



Name	Role	Version
RED-79-114	Hub Transport, Client Access, Mailbox	Version 14.1 (Build 218.15)

	Subject	Issuer	Expiration Date
	CN=RED-79-114.ca.avaya.com	CN=ca-RED-79-114-CA	10/08/2017
, SMTP	CN=Sites	CN=ca-RED-79-114-CA	02/11/2016
	CN=ca-RED-79-114-CA	CN=ca-RED-79-114-CA	03/11/2019
	CN=WMSvc-WIN-I8MVCP7RQGI	CN=WMSvc-WIN-I8MVCP…	31/10/2024
	CN=red-79-114.ca.avaya.com, OU…	CN=red-79-99.ca.avaya.…	31/10/2024

Repeat this procedure for each Microsoft Exchange server in the Exchange cluster. Alternatively, the CA certificate that was used to sign the certificate for each individual Exchange Server can be imported into the Avaya Breeze™ cluster. This approach reduces the number of certificates that need to be exported from Exchange and imported to the Avaya Breeze™ cluster.

Checklist for integrating Exchange Collector with Presence Services

#	Task	Server	Notes	✔
1	DNS Requirement: Ensure all Client Access Servers (CAS) in the Exchange deployments are resolvable by the Presence server.	Presence server	FQDNs are used internally by Presence Services Exchange web services collector to communicate with MS Exchange server.	

Table continues…

#	Task	Server	Notes	✔
2	*Autodiscover* Service: Ensure that the Presence server can resolve *autodiscover.<yourExchangeDomain>* to one of the CASs configured for autodiscovery.	Presence server	FQDNs are used internally by Presence Services Exchange web services collector to communicate with MS Exchange server.	
3	Add the Microsoft Exchange user handles to System Manager.	Presence server		
4	Create a new Active Directory user to be used as the Presence Services account.	MS Exchange server		
5	Set Full Access Permissions for Exchange Mailboxes.	MS Exchange server		
6	Configure Exchange Services for the autodiscover service on each CAS.	MS Exchange server		

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:
   1. Select the **Override Default** check box.
   2. 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:
   1. Select the **Override Default** check box.
   2. In the **Effective Value** field, set the URI of the Exchange server.

      The URI format must be in the following format `https://`*`<exchange FQDN>`*`/ews/exchange.asmx`.
8. In the **Exchange Server Username** field:
   1. Select the **Override Default** check box.
   2. In the **Effective Value** field, set the user name that the Exchange collector must use when connecting to the Exchange server.

      Enter only the user part, not the domain part.
9. In the **Exchange Server Password** field:
   1. Select the **Override Default** check box.
   2. 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:
    1. Select the **Override Default** check box.
    2. In the **Effective Value** field, set the calendar information collection interval in minutes.
11. In the **Exchange Calendar Request Rate** field:
    1. Select the **Override Default** check box.
    2. 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:
    1. 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.

Exchange Collector network routing configuration

Exchange Collector connects to the Microsoft Exchange server through the Avaya Breeze™ Security Module Network Interface. This implies that the Microsoft Exchange server must either be on the same subnet as the Avaya Breeze™ Security Module Network Interface, or the server must be reachable through the gateway on that subnet.

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 network routing configuration

Domino Collector connects to the Domino server using regular Linux routing rules. As the Avaya Breeze™ platform default network route is associated with the Management Network Interface, outbound connections to the Domino server will use the Management Network Interface by default.

To enable the Domino Collector to use the Security Module Network Interface, the Domino server must be on the same subnet as the Avaya Breeze™ Security Module Network Interface.

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 67	
3	Sign the Domino Calendar web service database.	Domino Server	Signing the Domino Calendar web service database on page 68	
4	Create a new Aura user for Domino Collector.	Domino Server	Creating a Aura user for Domino Collector to authenticate on page 70	

Table continues…

No.	Task	Server	Link	✔
5	Provide access to the Aura user.	Domino Server	Providing reader access to the Aura user for Domino Collector to authenticate on page 78	
6	Add Lotus Notes handle to the Aura user.	Presence Services	Adding Lotus Notes handle to an Aura user on page 82	
7	Configure Domino Collector.	Presence Services	Configuring Domino Collector on page 64	

Installing the Domino Calendar web service database

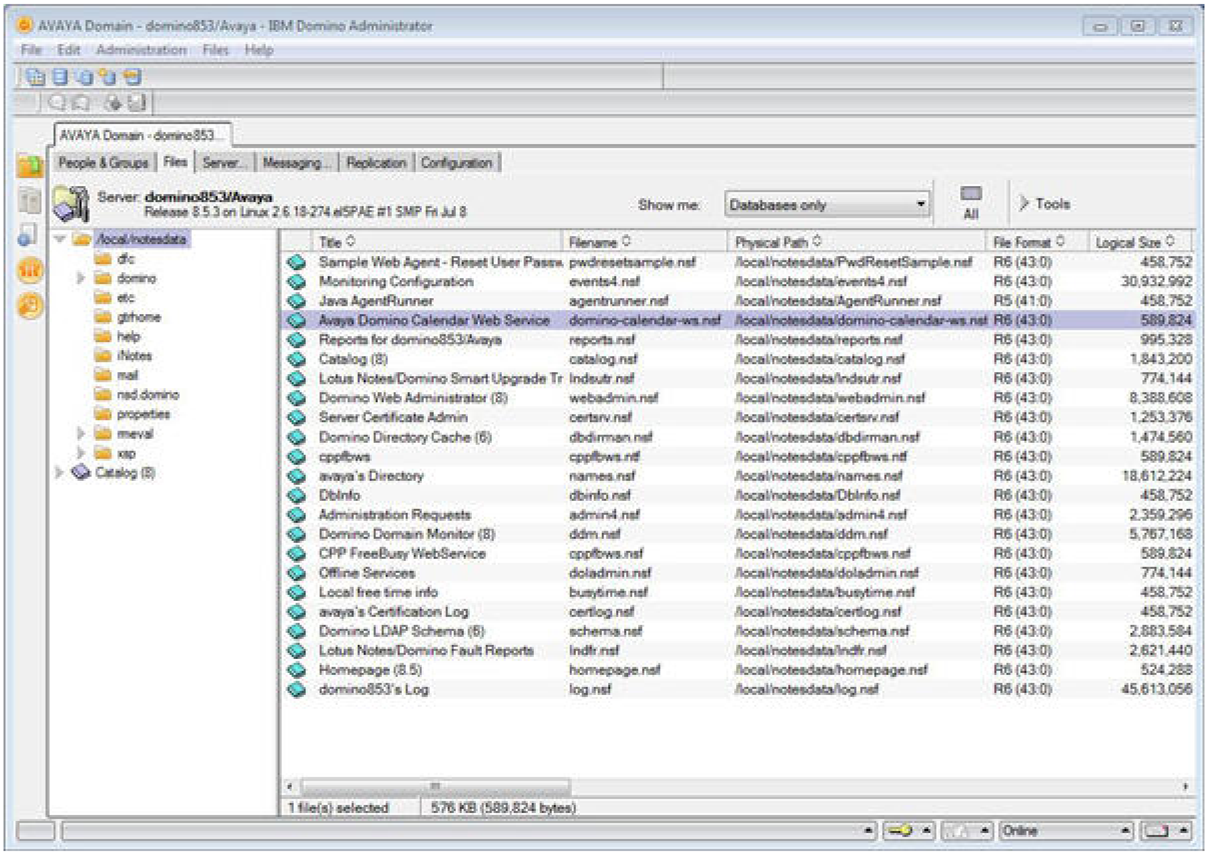
Procedure

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\IBM\Domino\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.



Server: **domino853/Avaya**
Release 8.5.3 on Linux 2.6.18-274.el5PAE #1 SMP Fri Jul 8

Show me: Databases only

Title	Filename	Physical Path	File Format	Logical Size
Sample Web Agent - Reset User Passw	pwdresetsample.nsf	/local/notesdata/PwdResetSample.nsf	R6 (43:0)	458,752
Monitoring Configuration	events4.nsf	/local/notesdata/events4.nsf	R6 (43:0)	30,932,992
Java AgentRunner	agentrunner.nsf	/local/notesdata/AgentRunner.nsf	R5 (41:0)	458,752
Avaya Domino Calendar Web Service	domino-calendar-ws.nsf	/local/notesdata/domino-calendar-ws.nsf	R6 (43:0)	589,824
Reports for domino853/Avaya	reports.nsf	/local/notesdata/reports.nsf	R6 (43:0)	995,328
Catalog (8)	catalog.nsf	/local/notesdata/catalog.nsf	R6 (43:0)	1,843,200
Lotus Notes/Domino Smart Upgrade Tr	lndsutr.nsf	/local/notesdata/lndsutr.nsf	R6 (43:0)	774,144
Domino Web Administrator (8)	webadmin.nsf	/local/notesdata/webadmin.nsf	R6 (43:0)	8,388,608
Server Certificate Admin	certsrv.nsf	/local/notesdata/certsrv.nsf	R6 (43:0)	1,253,376
Domino Directory Cache (6)	dbdirman.nsf	/local/notesdata/dbdirman.nsf	R6 (43:0)	1,474,560
cppfbws	cppfbws.ntf	/local/notesdata/cppfbws.ntf	R6 (43:0)	589,824
avaya's Directory	names.nsf	/local/notesdata/names.nsf	R6 (43:0)	18,612,224
DbInfo	dbinfo.nsf	/local/notesdata/DbInfo.nsf	R6 (43:0)	458,752
Administration Requests	admin4.nsf	/local/notesdata/admin4.nsf	R6 (43:0)	2,359,296
Domino Domain Monitor (8)	ddm.nsf	/local/notesdata/ddm.nsf	R6 (43:0)	5,767,168
CPP FreeBusy WebService	cppfbws.nsf	/local/notesdata/cppfbws.nsf	R6 (43:0)	589,824
Offline Services	doladmin.nsf	/local/notesdata/doladmin.nsf	R6 (43:0)	774,144
Local free time info	busytime.nsf	/local/notesdata/busytime.nsf	R6 (43:0)	458,752
avaya's Certification Log	certlog.nsf	/local/notesdata/certlog.nsf	R6 (43:0)	458,752
Domino LDAP Schema (6)	schema.nsf	/local/notesdata/schema.nsf	R6 (43:0)	2,883,584
Lotus Notes/Domino Fault Reports	lndfr.nsf	/local/notesdata/lndfr.nsf	R6 (43:0)	2,621,440
Homepage (8.5)	homepage.nsf	/local/notesdata/homepage.nsf	R6 (43:0)	524,288
domino853's Log	log.nsf	/local/notesdata/log.nsf	R6 (43:0)	45,613,056

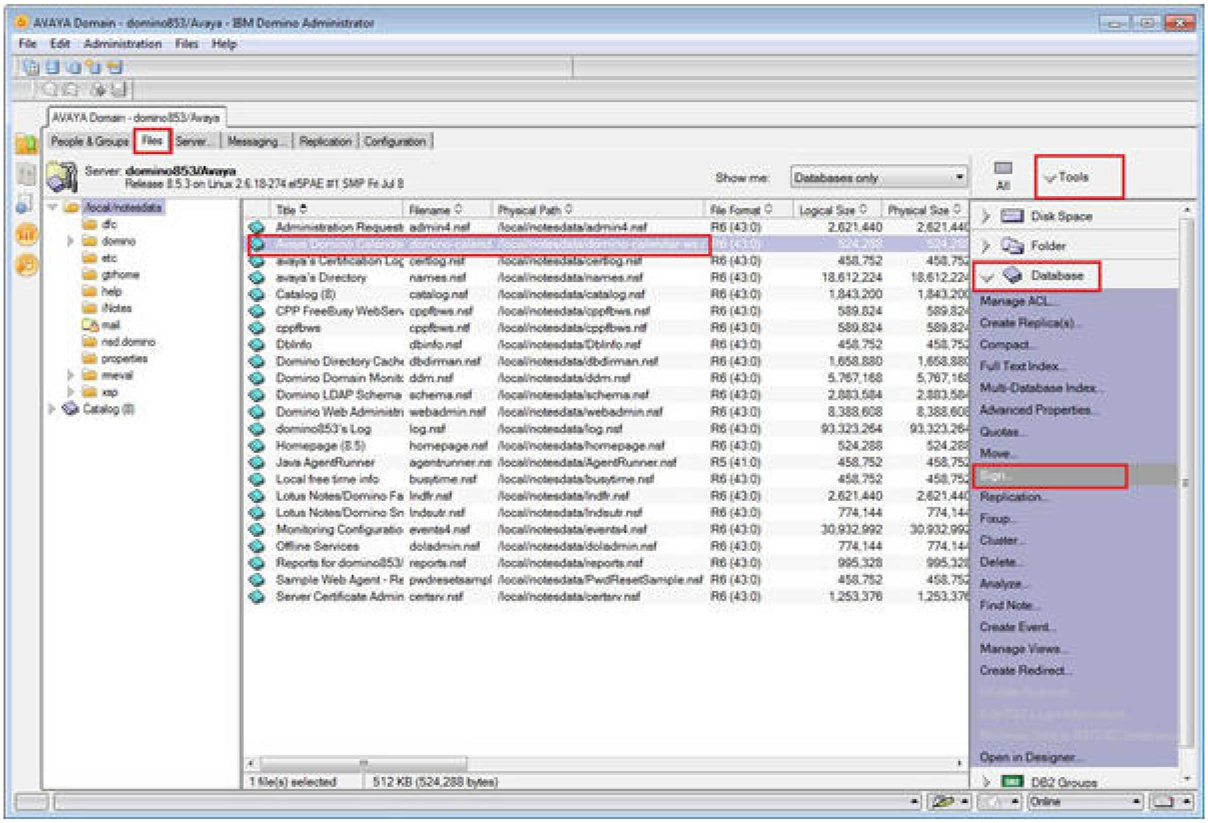
1 file(s) selected 576 KB (589,824 bytes)

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.



Title	Filename	Physical Path	File Format	Logical Size	Physical Size
Administration Request	admin4.nsf	/local/notesdata/admin4.nsf	R6 (43:0)	2,621,440	2,621,440
Avaya Domino Calendar	domino-calend	/local/notesdata/domino-calendar-ws	R6 (43:0)	524,288	524,288
avaya's Certification Log	certlog.nsf	/local/notesdata/certlog.nsf	R6 (43:0)	458,752	458,752
avaya's Directory	names.nsf	/local/notesdata/names.nsf	R6 (43:0)	18,612,224	18,612,224
Catalog (8)	catalog.nsf	/local/notesdata/catalog.nsf	R6 (43:0)	1,843,200	1,843,200
CPP FreeBusy WebServ	cppfbws.nsf	/local/notesdata/cppfbws.nsf	R6 (43:0)	589,824	589,824
cppfbws	cppfbws.ntf	/local/notesdata/cppfbws.ntf	R6 (43:0)	589,824	589,824
DbInfo	dbinfo.nsf	/local/notesdata/DbInfo.nsf	R6 (43:0)	458,752	458,752
Domino Directory Cache	dbdirman.nsf	/local/notesdata/dbdirman.nsf	R6 (43:0)	1,658,880	1,658,880
Domino Domain Monit	ddm.nsf	/local/notesdata/ddm.nsf	R6 (43:0)	5,767,168	5,767,168
Domino LDAP Schema	schema.nsf	/local/notesdata/schema.nsf	R6 (43:0)	2,883,584	2,883,584
Domino Web Administr	webadmin.nsf	/local/notesdata/webadmin.nsf	R6 (43:0)	8,388,608	8,388,608
domino853's Log	log.nsf	/local/notesdata/log.nsf	R6 (43:0)	93,323,264	93,323,264
Homepage (8.5)	homepage.nsf	/local/notesdata/homepage.nsf	R6 (43:0)	524,288	524,288
Java AgentRunner	agentrunner.ns	/local/notesdata/AgentRunner.nsf	R5 (41:0)	458,752	458,752
Local free time info	busytime.nsf	/local/notesdata/busytime.nsf	R6 (43:0)	458,752	458,752
Lotus Notes/Domino Fa	lndfr.nsf	/local/notesdata/lndfr.nsf	R6 (43:0)	2,621,440	2,621,440
Lotus Notes/Domino Sn	lndsutr.nsf	/local/notesdata/lndsutr.nsf	R6 (43:0)	774,144	774,144
Monitoring Configuratio	events4.nsf	/local/notesdata/events4.nsf	R6 (43:0)	30,932,992	30,932,992
Offline Services	doladmin.nsf	/local/notesdata/doladmin.nsf	R6 (43:0)	774,144	774,144
Reports for domino853/	reports.nsf	/local/notesdata/reports.nsf	R6 (43:0)	995,328	995,328
Sample Web Agent - Re	pwdresetsampl	/local/notesdata/PwdResetSample.nsf	R6 (43:0)	458,752	458,752
Server Certificate Admin	certsrv.nsf	/local/notesdata/certsrv.nsf	R6 (43:0)	1,253,376	1,253,376

1 file(s) selected 512 KB (524,288 bytes)

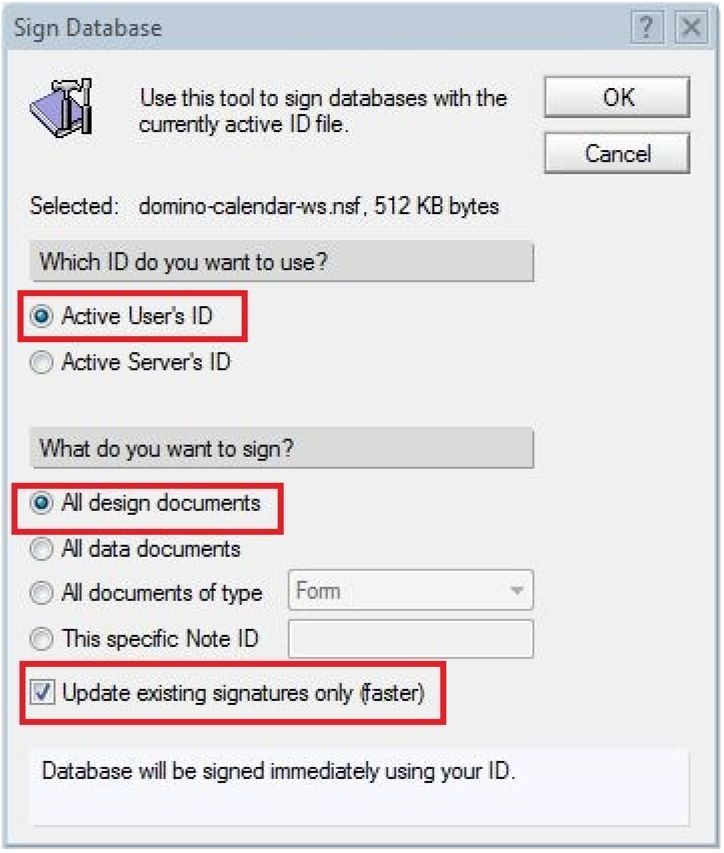
5. Click **Tools** > **Database**.

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.



Use this tool to sign databases with the currently active ID file.

Selected: domino-calendar-ws.nsf, 512 KB bytes

Which ID do you want to use?

● Active User's ID

○ Active Server's ID

What do you want to sign?

● All design documents

○ All data documents

○ All documents of type Form

○ This specific Note ID

☑ Update existing signatures only (faster)

Database will be signed immediately using your ID.

10. Click **OK**.

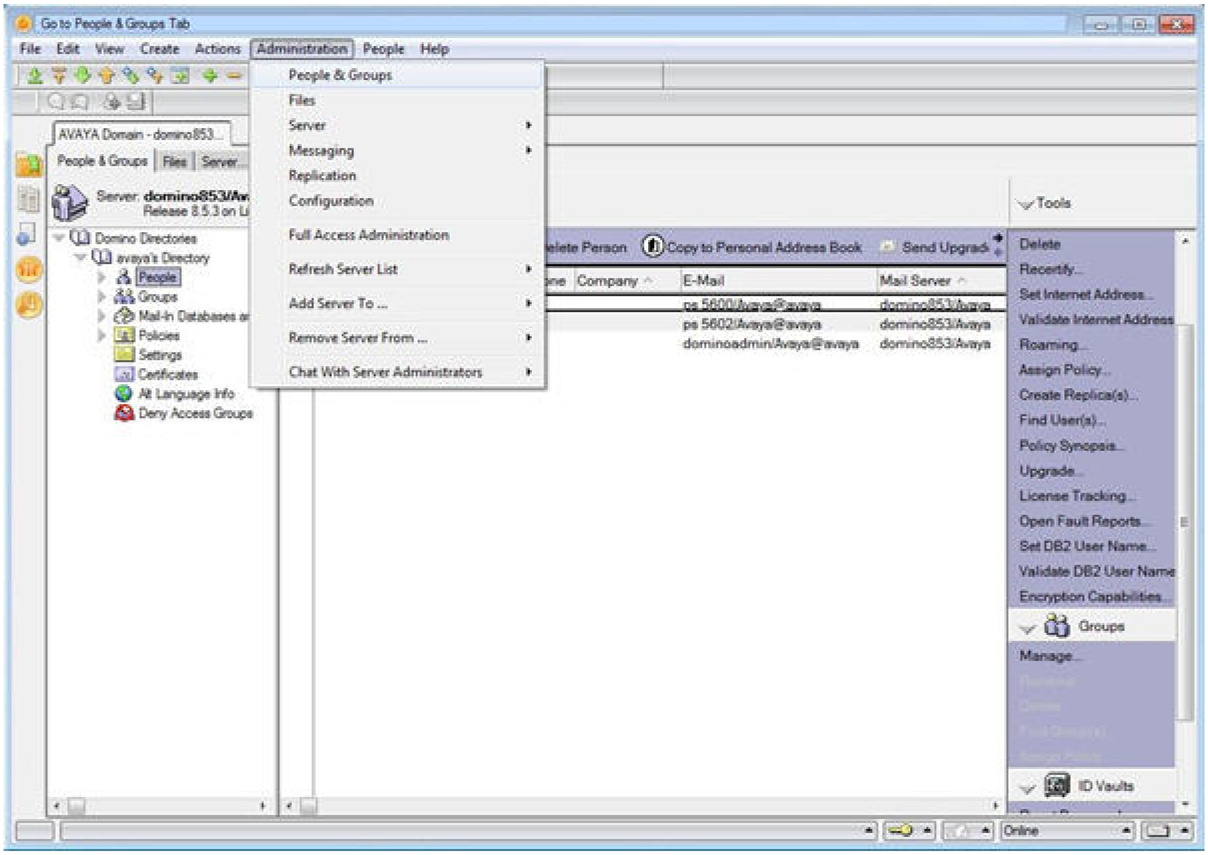
    The system displays the **1 database processed - 0 errors** message.

Creating a Aura user for Domino Collector to authenticate

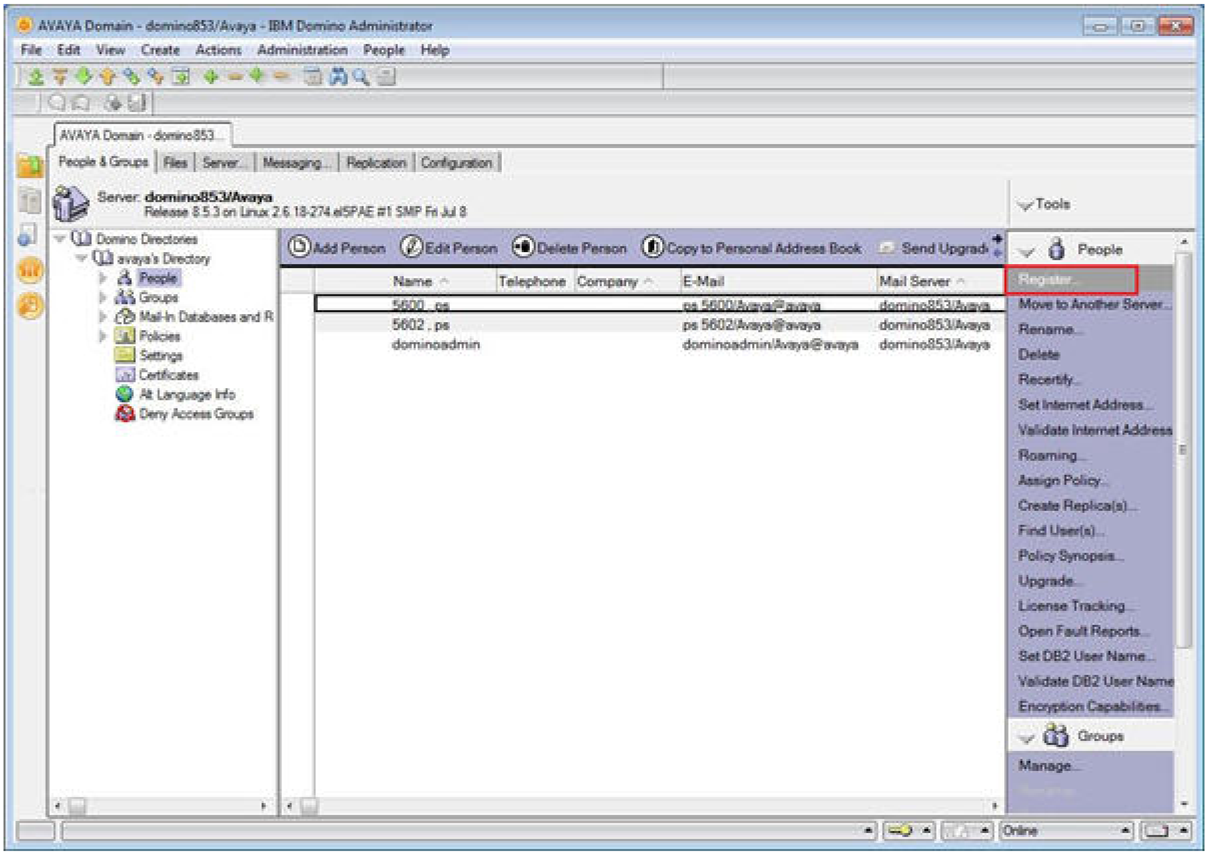
Procedure

1. Log in to the Domino Administrator client.

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



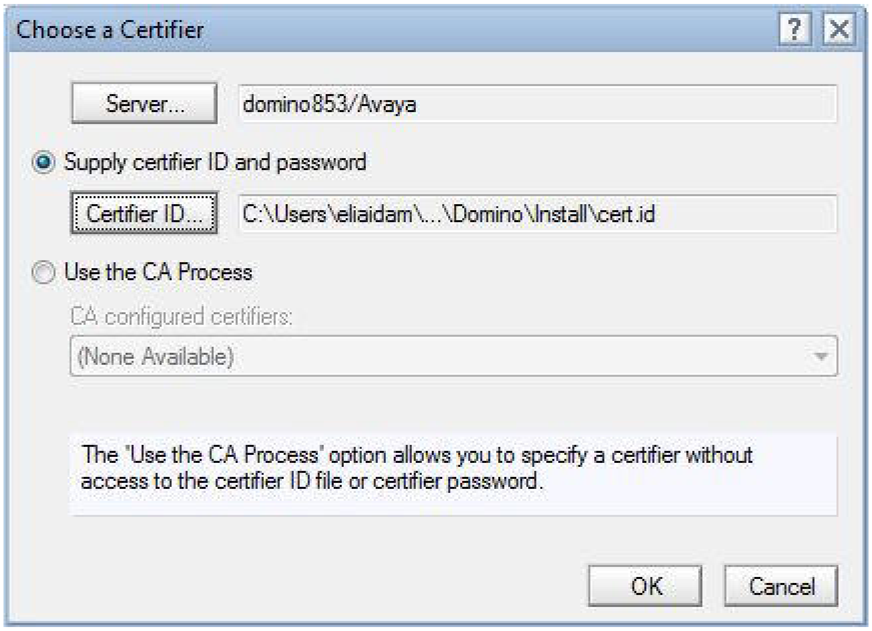
3. Click **Register**.



Server: **domino853/Avaya**
Release 8.5.3 on Linux 2.6.18-274.el5PAE #1 SMP Fri Jul 8

Name	Telephone	Company	E-Mail	Mail Server
5600 , ps			ps 5600/Avaya@avaya	domino853/Avaya
5602 , ps			ps 5602/Avaya@avaya	domino853/Avaya
dominoadmin			dominoadmin/Avaya@avaya	domino853/Avaya

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



Choose a Certifier

Server... domino853/Avaya

● Supply certifier ID and password

Certifier ID... C:\Users\eliaidam\...\Domino\Install\cert.id

○ Use the CA Process

CA configured certifiers:

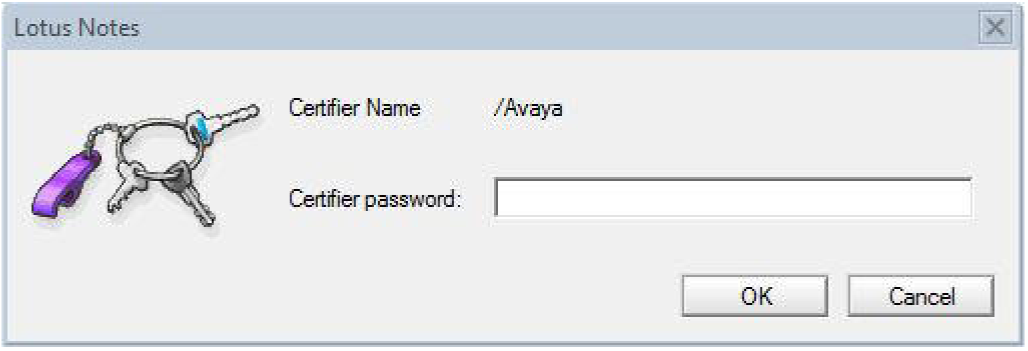
(None Available)

The 'Use the CA Process' option allows you to specify a certifier without access to the certifier ID file or certifier password.

Note:

The Domino server creates the `cert.id` file when the server is installed. This file must be retrieved from the Domino server to the client computer used to run the Domino Administration client software. The `cert.id` file is located in the Domino server default data folder. This is the same folder where the `domino-calendar-ws.nsf` file was copied to in Step 2 of the installation checklist.

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

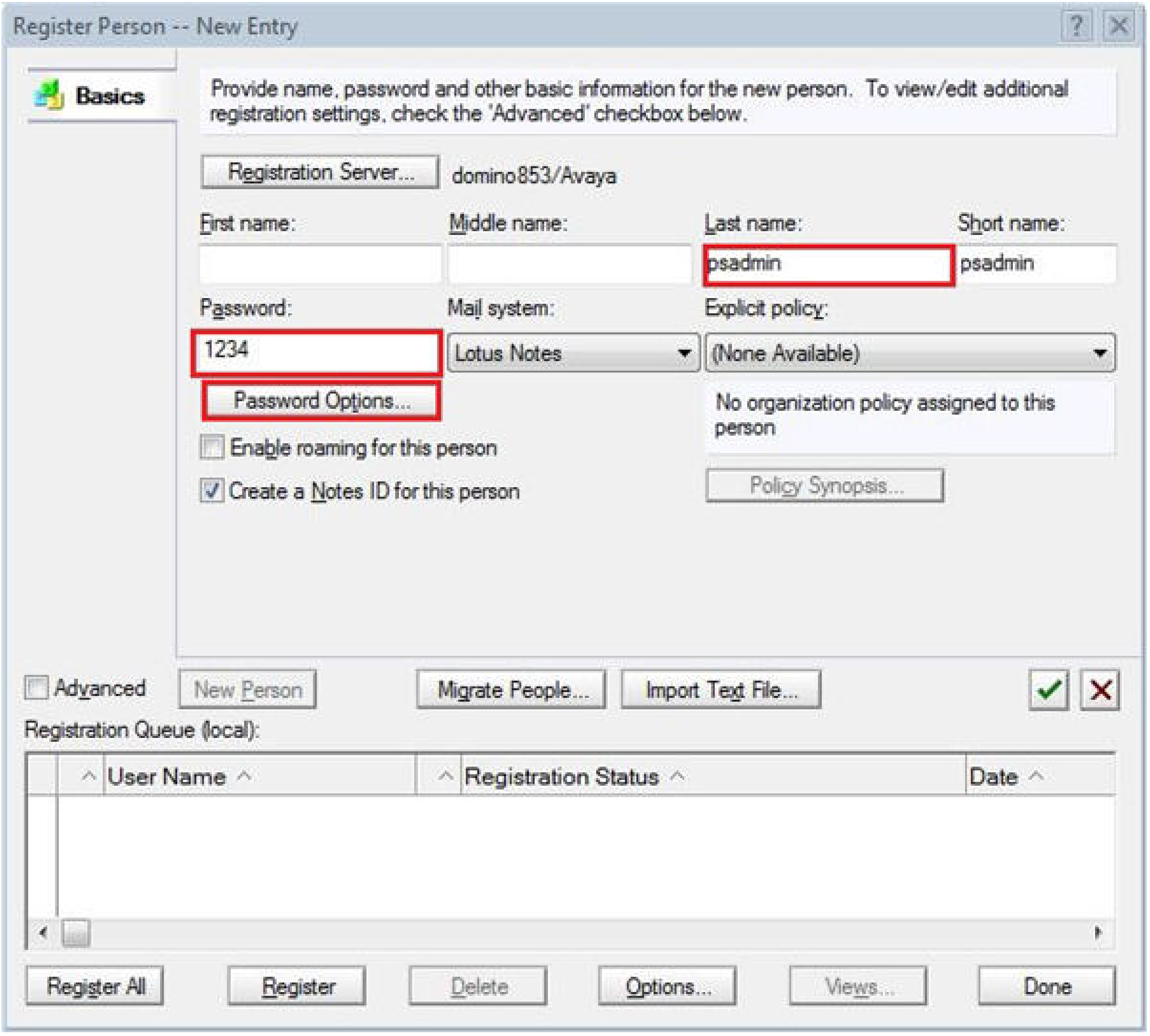


Certifier Name /Avaya

Certifier password:

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

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



Register Person -- New Entry

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

Registration Server... domino853/Avaya

First name:

Middle name:

Last name: psadmin

Short name: psadmin

Password: 1234

Mail system: Lotus Notes

Explicit policy: (None Available)

No organization policy assigned to this person

□ Enable roaming for this person

☑ Create a Notes ID for this person

□ Advanced

Registration Queue (local):

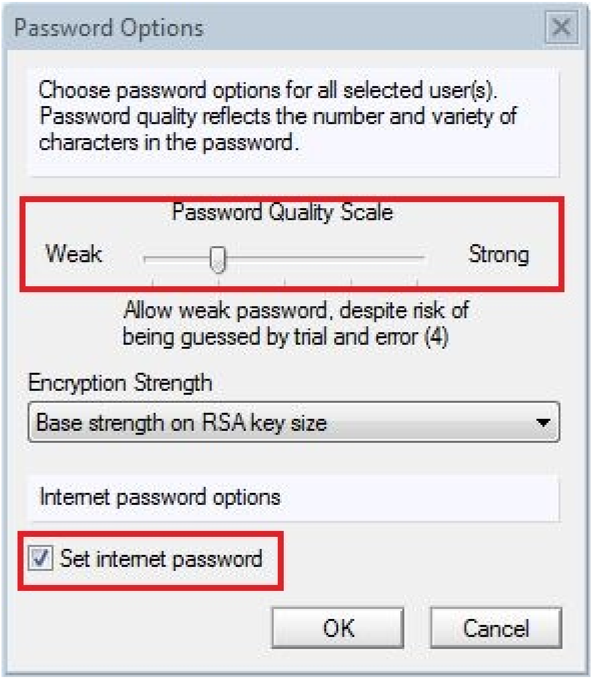
User Name	Registration Status	Date

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**.



Password Options

Choose password options for all selected user(s). Password quality reflects the number and variety of characters in the password.

Password Quality Scale

Weak — Strong

Allow weak password, despite risk of being guessed by trial and error (4)

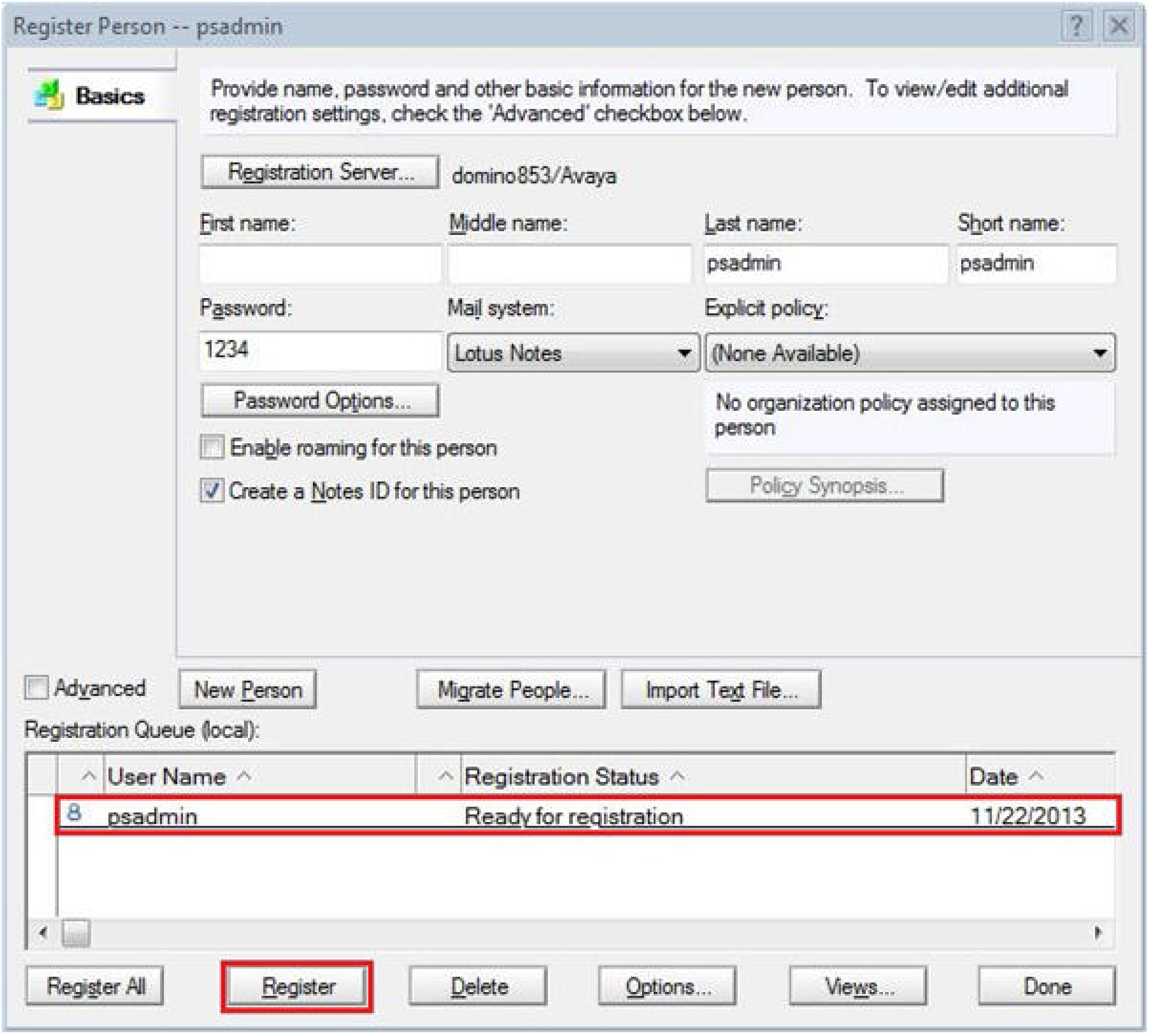
Encryption Strength: Base strength on RSA key size

Internet password options

☑ Set internet password

11. Select the green check mark box.

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



Register Person -- psadmin

Basics

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

Registration Server... domino853/Avaya

First name:

Middle name:

Last name: psadmin

Short name: psadmin

Password: 1234

Mail system: Lotus Notes

Explicit policy: (None Available)

No organization policy assigned to this person

□ Enable roaming for this person

☑ Create a Notes ID for this person

□ Advanced

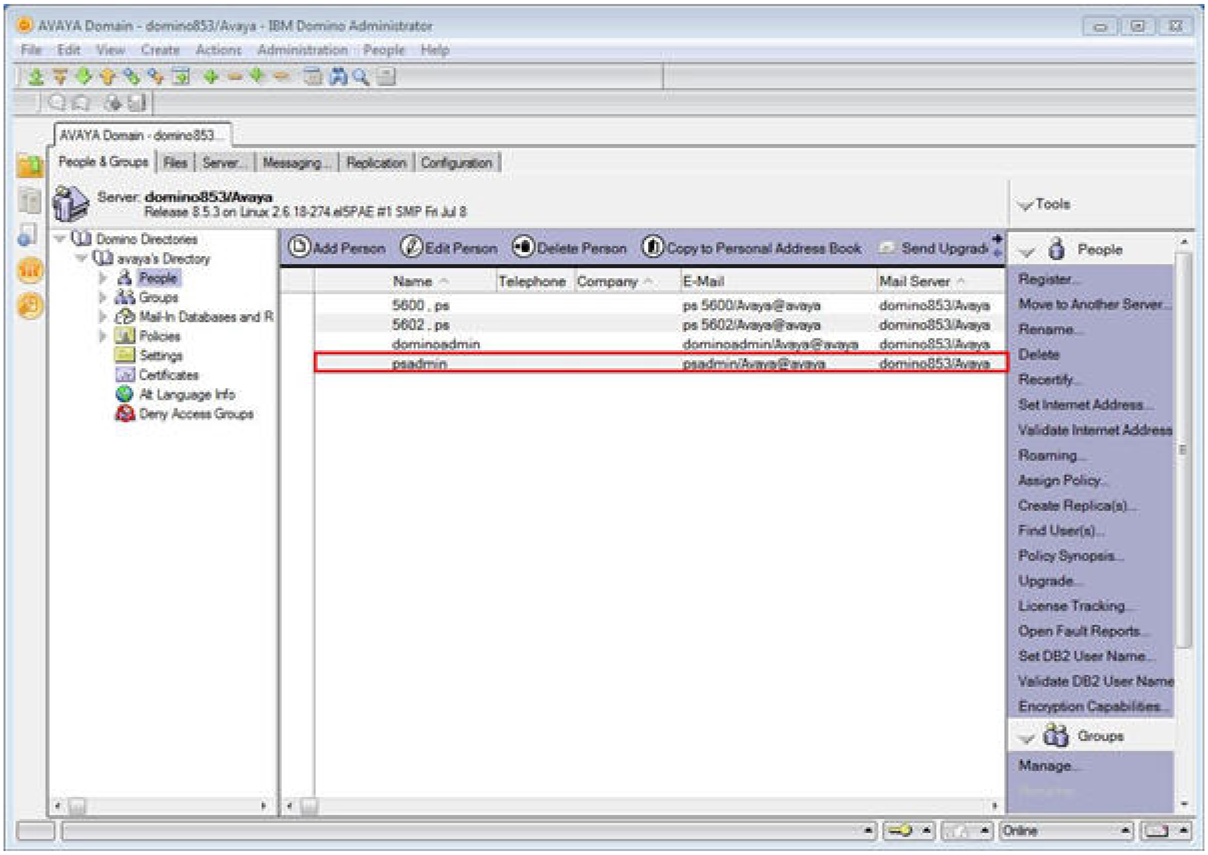
Registration Queue (local):

User Name	Registration Status	Date
psadmin	Ready for registration	11/22/2013

13. Click **OK**.

14. Click **Done**.

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

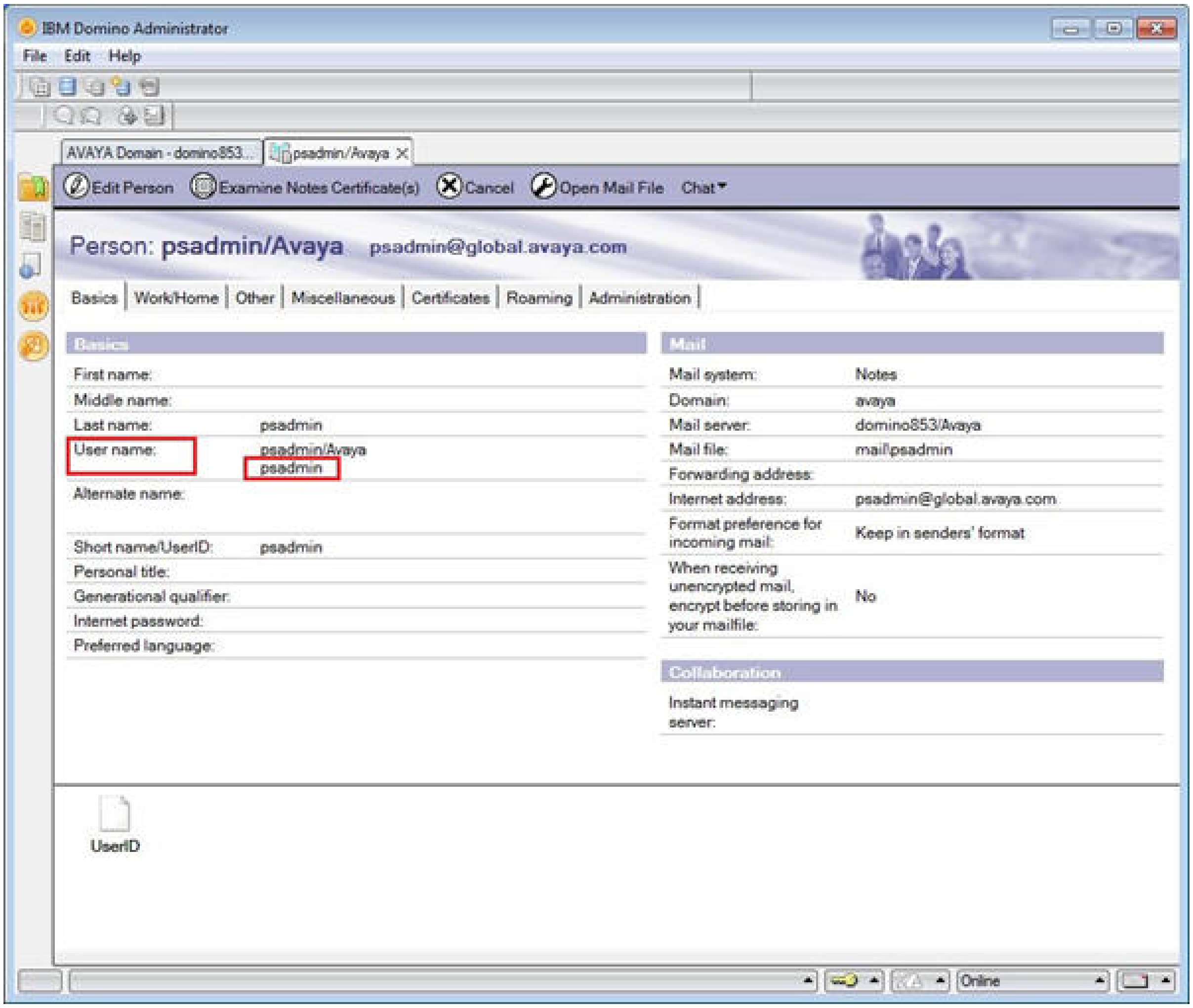


Server: **domino853/Avaya**
Release 8.5.3 on Linux 2.6.18-274.el5PAE #1 SMP Fri Jul 8

Name	Telephone	Company	E-Mail	Mail Server
5600 , ps			ps 5600/Avaya@avaya	domino853/Avaya
5602 , ps			ps 5602/Avaya@avaya	domino853/Avaya
dominoadmin			dominoadmin/Avaya@avaya	domino853/Avaya
psadmin			psadmin/Avaya@avaya	domino853/Avaya

16. Double-click the user to see the information about the user.

Note the entry in the **User name** field.



Person: psadmin/Avaya psadmin@global.avaya.com

Basics

First name:	
Middle name:	
Last name:	psadmin
User name:	psadmin/Avaya psadmin
Alternate name:	
Short name/UserID:	psadmin
Personal title:	
Generational qualifier:	
Internet password:	
Preferred language:	

Mail

Mail system:	Notes
Domain:	avaya
Mail server:	domino853/Avaya
Mail file:	mail\psadmin
Forwarding address:	
Internet address:	psadmin@global.avaya.com
Format preference for incoming mail:	Keep in senders' format
When receiving unencrypted mail, encrypt before storing in your mailfile:	No

Collaboration

Instant messaging server:	

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

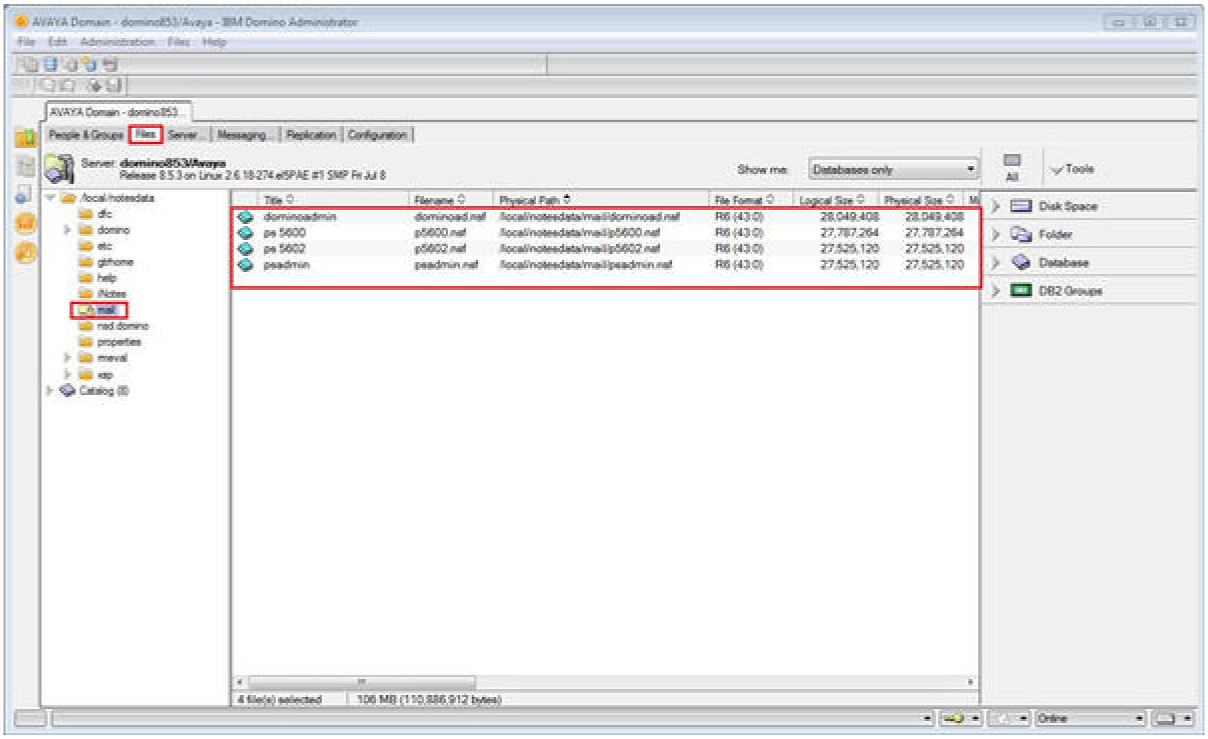
About this task

A Aura 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.



Server: domino853/Avaya
Release 8.5.3 on Linux 2.6.18-274.el5PAE #1 SMP Fri Jul 8

Title	Filename	Physical Path	File Format	Logical Size	Physical Size
dominoadmin	dominoad.nsf	/local/notesdata/mail/dominoad.nsf	R6 (43:0)	28,049,408	28,049,408
ps 5600	p5600.nsf	/local/notesdata/mail/p5600.nsf	R6 (43:0)	27,787,264	27,787,264
ps 5602	p5602.nsf	/local/notesdata/mail/p5602.nsf	R6 (43:0)	27,525,120	27,525,120
psadmin	psadmin.nsf	/local/notesdata/mail/psadmin.nsf	R6 (43:0)	27,525,120	27,525,120

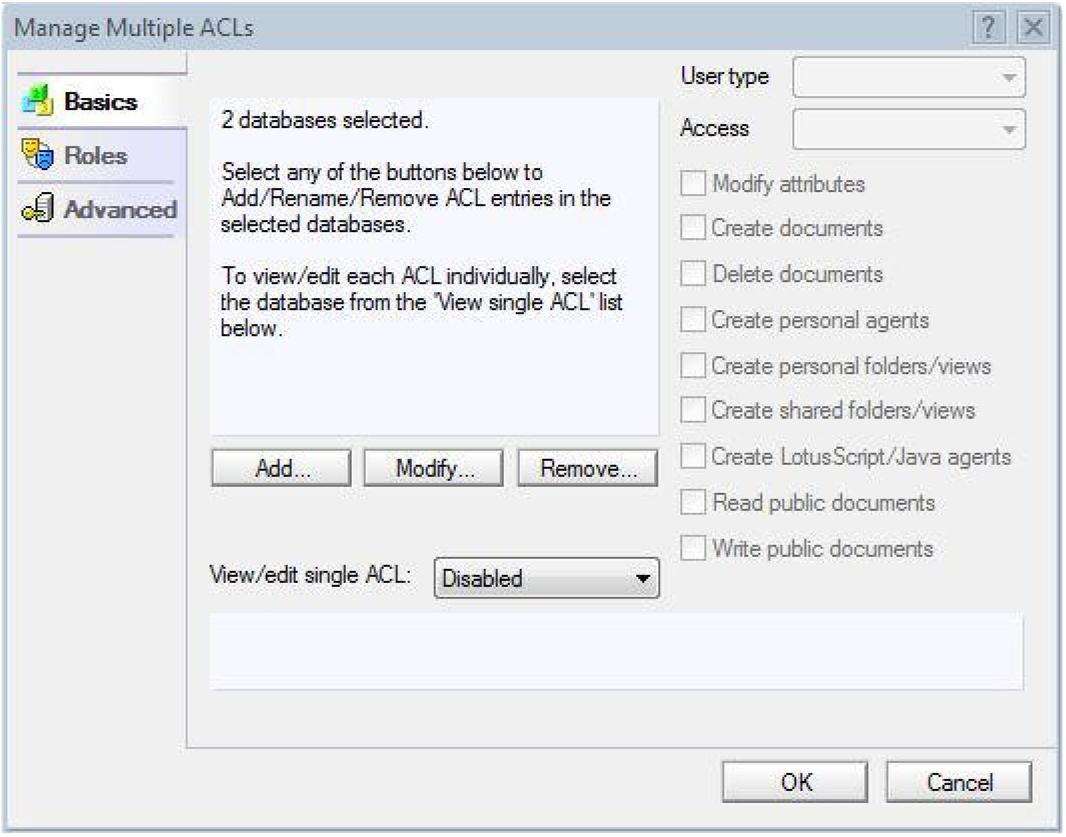
4 file(s) selected 106 MB (110,886,912 bytes)

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**.



Manage Multiple ACLs

2 databases selected.

Select any of the buttons below to Add/Rename/Remove ACL entries in the selected databases.

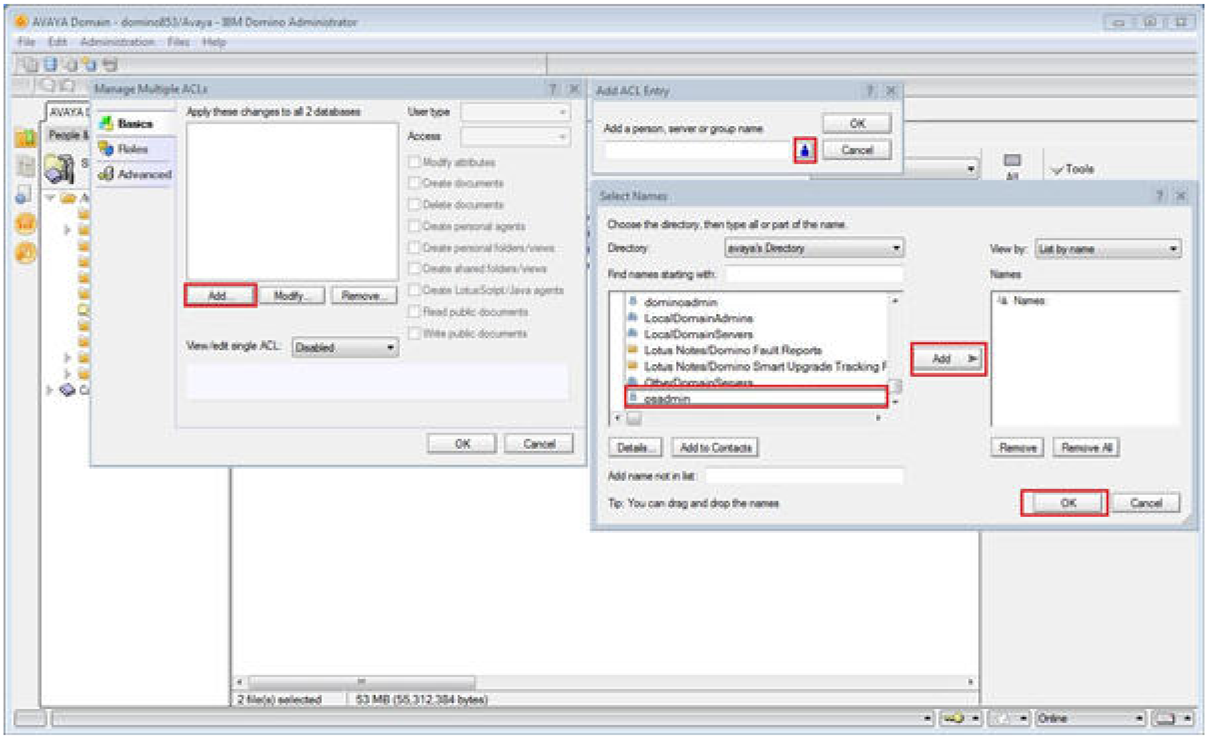
To view/edit each ACL individually, select the database from the 'View single ACL' list below.

View/edit single ACL: Disabled

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

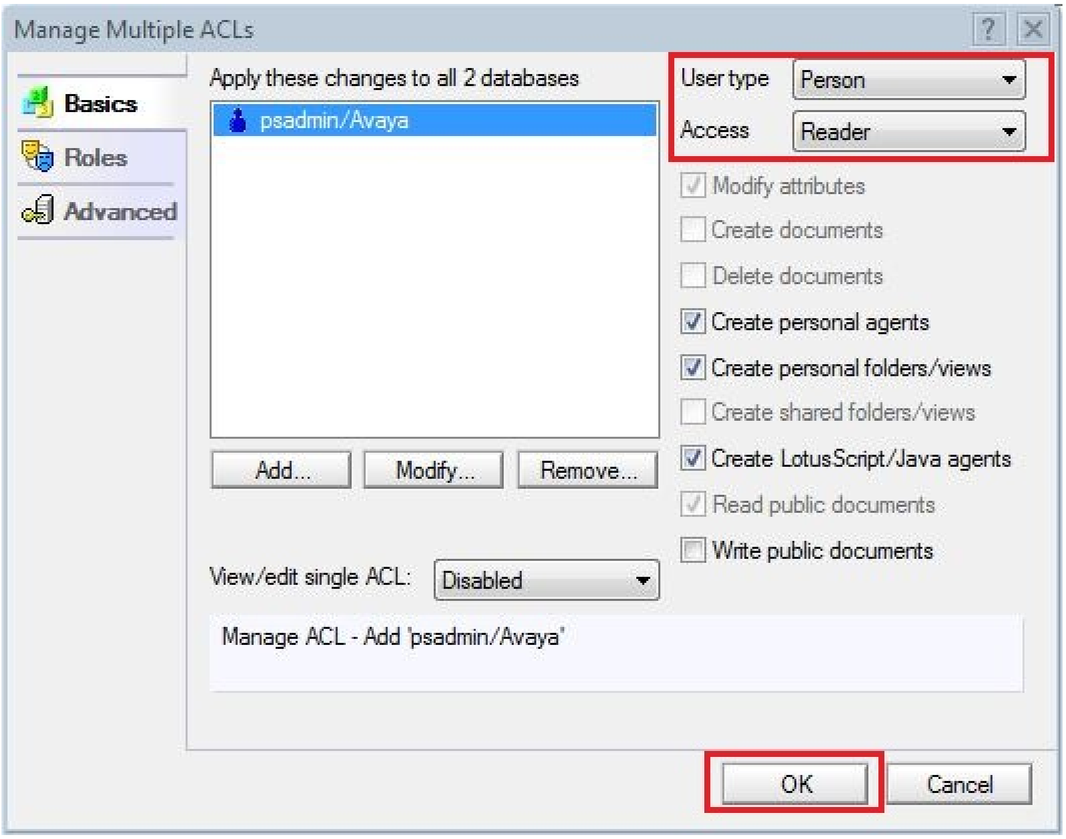
   In the example, `psadmin` is the Aura user.
7. Click **Add**.

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 an Aura 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 Aura 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**.

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.

Any standards based XMPP server is supported using the generic XMPP federation type.

Microsoft Real Time Communication (RTC) 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 RTC 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. Avaya Aura® users can engage in IM conversations with each other through their Avaya Aura® clients. After enabling the Microsoft RTC federation, Presence Services supports:

- Avaya Aura® users, using their Avaya Aura® clients, can IM the other enterprise user colleagues who are using Microsoft Office Communicator (MOC) Lync or Skype clients

- Enterprise users, using Lync or Skype clients, can initiate an IM conversation with their enterprise colleagues who are using Avaya Aura® clients.

Note:

Presence Services Release 7.1.2 supports federation with Skype For Business and Lync 2013 Standard Editions. Enterprise Edition is supported to a limited extent, in that Presence Services will only communicate with a single Microsoft Front End server.

Additionally, an Enterprise user can obtain the overall presence availability of their Avaya Aura® colleagues by adding the Presence/IM communication address or Avaya presence handle of an Avaya Aura® user to their buddy list. The Lync or Skype 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 Microsoft RTC federation when Inter-Tenant Communication Control is enabled on System Manager.

Microsoft RTC federation is supported in two ways for a given user, True federation and Hybrid federation. If a user is administered as both, the Avaya Aura® user and the Microsoft RTC user then the hybrid federation model may be used. It provides an additional feature to Avaya Aura® watchers of the user – namely the aggregation of presence from two sources: Avaya Aura® and Microsoft RTC. For users that are administered in the Microsoft RTC only, the 'True' federation model may be preferred. It offers minimal user administration and does not require additional Avaya Aura® licenses. In both cases, the user is defined in the Microsoft RTC system. A True federation user is not defined in the Avaya Aura® System Manager. A Hybrid federation user is defined in the Avaya Aura® System Manager and is presence enabled

To enable an Aura user as a Hybrid Microsoft RTC 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".

Microsoft RTC federation supports both Internal Enterprise and External Enterprise federation.

Note:

Microsoft RTC Intra-Domain Federation does not support Hybrid users.

Note:

For correct user Presence/IM routing, all Avaya Presence/IM handles must be lowercase. Using uppercase characters might result in the inability 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, modify the handle using lowercase characters.

Note:

The hostname assigned to the Avaya Breeze™ Security Module interface must be constructed using the shortname from the Avaya Breeze™ server manangement hostname with the suffix -sm100. The suffix is not optional.

For example, if the Avaya Breeze™ server management FQDN is *hostA.domainA.com*. Then, the Avaya Breeze™ Security Module FQDN must be: *hostA-sm100.domainB.com*, where *domainA* and *domainB* can be the same.

You must follow this naming convention in the following sections:

- "Configuring DNS A Records"
- "Configuring Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route"
- "Avaya Breeze™ server certificates"

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 Microsoft Federation

Table 7: Checklist for configuring Microsoft Federation

No.	Task	Reference	✔
DNS Configuration:			
1	Configure the DNS A record.	Configuring DNS A Records on page 86	
Front End Server Configuration:			
2	Verify the Front End server certificate.	Verifying the Front End service Certificate on page 87	

Table continues…

No.	Task	Reference	✔
DNS Configuration:			
3	Import the System Manager Default CA certificate into Microsoft Front End server Trust Store.	Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store on page 88	
4	Configure the Microsoft Front End server with Trusted Application Pool, Trusted Application and Static Route	Configuring Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route on page 88	
5	Restart the Front End server service.	Restarting the Front End service on page 90	
Avaya Aura® Configuration:			
6	Configure Avaya Breeze™ server Certificates.	Configuring Avaya Breeze server Trusted Certificate for a single Microsoft Front End server on page 91	
7	Configure SIP Entity and Entity Link to PS Federation Relay service.	Configuring the SIP Entity and Entity Link to PS Federation Relay service on page 93	
8	Configure Avaya Breeze™ Attributes.	Configuring Avaya Breeze attributes on page 94	
9	Configure Avaya Breeze™ nodes to use Microsoft domain DNS server.	Configuring DNS Server Avaya Breeze nodes on page 95	
10	Add or update the existing Communication Manager application.	Adding or updating the existing Communication Manager application on page 96	

Configuring DNS A Records

Procedure

1. For every Avaya Breeze server in the Presence Services cluster, a DNS A Record is required to resolve the Avaya Breeze server Security Module FQDN. The Breeze server Security Module FQDN is constructed from the Breeze server management FQDN short host name plus suffix of -sm100. The IP address is the Breeze server Security Module IP address.

   For example: The Avaya Breeze server management FQDN is sc-8205.avaya.com, the FQDN short host name in this example is sc-8205. The A Record is created as:

   - Host is sc-8205-sm100
   - The FQDN is sc-8205-sm100.avaya.com and
   - The IP address is 10.138.82.6 which is the Breeze Server Security Module IP address

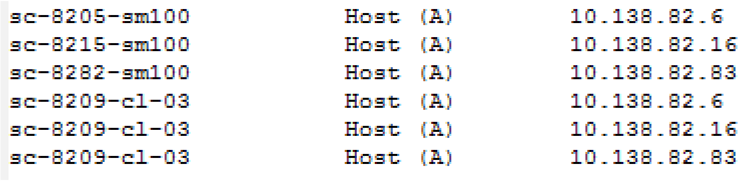
   There is one A Record per Breeze node. For n-nodes cluster, there are n DNS A Records.

2. Create DNS A Record(s) to resolve Presence Services Cluster FQDN. The IP address is the Breeze server Security Module IP address. We need to create multiple A Records to resolve the same Presence Services Cluster FQDN to each Breeze Security Module IP address.

   For example:

   In a three-node cluster, the cluster FQDN must resolve to three Security Module IP addresses. Combining 1 and 2, the screen shot shows the example of 3 nodes cluster A Record(s) under Forward Lookup Zones > domain avaya.com. The example has:

   ```
   Presence Services Cluster FQDN        sc-8209-cl-03.avaya.com
   Breeze server management FQDN(s) and Security Module IP address(es)
   sc-8205.avaya.com    10.138.82.6
   sc-8215.avaya.com    10.138.82.16
   sc-8282.avaya.com    10.138.82.83
   ```

   ```
   sc-8205-sm100          Host (A)        10.138.82.6
   sc-8215-sm100          Host (A)        10.138.82.16
   sc-8282-sm100          Host (A)        10.138.82.83
   sc-8209-cl-03          Host (A)        10.138.82.6
   sc-8209-cl-03          Host (A)        10.138.82.16
   sc-8209-cl-03          Host (A)        10.138.82.83
   ```

   Note:

   When you add New Host (A Record) in DNS, you can select the Create associated pointer (PTR) record check box. This step might eliminate the need to add the machine name to Reverse Lookup Zone if the zone already exists.

Verifying the Front End service Certificate

About this task

Microsoft Front End server deployment requires installation of a certificate in **Deployment Wizard**, **Step 3: Request, Install or Assign Certificates**. To federate with Avaya Aura® system, the installed certificate must support Server and Client Authentication in the Enhanced Key Usage.

Procedure

1. Log in to Front End server.
2. Run **Deployment Wizard**, click **Install** or Update Lync or Skype for Business Server System, and select **Step 3: Request, Install or Assign Certificates**.
3. Click **Run Again** and then click **View the Default Certificate > View Certificate Details**.
4. Verify that the Enhanced Key Usage has the following:

   ```
   Server Authentication(1.3.6.1.5.5.7.3.1)
   Client Authentication(1.3.6.1.5.5.7.3.2)
   ```

5. If not, you need to re-create certificate with Server and Client Authentication and assign to Front End service.

Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store

Procedure

1. Log in to the System Manager web console.
2. Click **Security** > **Certificates** > **Authority** > **CA Structure & CRLs**.
3. Click **Download pem file**.
4. Save the pem file.

   The default downloaded file name is `SystemManagerCA.cacert.pem`
5. Upload the pem file to Microsoft Front End server.
6. Run Microsoft Management Console with Certificate snap-in on Computer account.
7. Click **Console Root** > **Certificates (Local Computer)** > **Trusted Root Certification Authorities Select Certificates** > **All Tasks** > **Import**.
8. In the Certificate Import Wizard, follow the steps of the wizard and select / import the uploaded pem file to the **Trusted Root Certification Authorities.**
9. To verify the imported certificate, click **Console Root** > **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates list**.
10. Select **System Manager CA** from certificate detail page.
11. Verify that the Serial number and the expiratory date of the newly imported certificate matches the System Manager CA.
12. Restart the Front End server services after completing certificate import.

    Refer to the section “Restarting the Front End server service”.

Configuring Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route

About this task

The administrator needs to configure the Presence Services cluster as a trusted application pool that can be referred to in a Front End static route and a trusted application definition.

Procedure

1. On Lync Front End server, run **Lync Server Management Shell** and on Skype for Business Front End server, run Skype for **Business Server Management Shell**.
2. Create a trusted application pool. Use the **`New-CsTrustedApplicationPool`** cmdlet to create a trusted application pool `sc-8209-cl-03.avaya.com` to host trusted application.

   ```
   New-CsTrustedApplicationPool -Identity sc-8209-cl-03.avaya.com  -Registrar
   Registrar:lync2013-fe.bvwlab.com  -Site 1  -ComputerFqdn sc-8205-sm100.avaya.com -
   ThrottleAsServer $true -TreatAsAuthenticated $true -RequiresReplication $false
   ```

For more information, see help of the `New-CsTrustedApplicationPool` cmdlet.

- `Identity` is the FQDN of the new pool and it is the Avaya Breeze™ cluster FQDN.
- `Registrar` is the FQDN of the Front End pool to which this trusted application pool belongs.

You can find the Register parameter with cmdlet **`Get-CsPool | Where-Object {$_.Services -match "Registrar:"}`**.

`-Site` is Site ID to which this trusted application pool belongs; use `Get-CsSite` cmdlet to retrieve the SiteId.

`-ComputerFqdn` defines the FQDN of the first Avaya Breeze™ server Security Module FQDN in the trusted application pool.

3. Add other Avaya Breeze™ node to the trusted application pool for multi-nodes cluster setup. Use the `New-CsTrustedApplicationComputer` cmdlet to add other Avaya Breeze™ server(s) to the trusted application pool.

```
New-CsTrustedApplicationComputer -Identity sc-8215-sm100.avaya.com -Pool sc-8209-
cl-03.avaya.com
```

`-Identity` is Avaya Breeze™ server Security Module FQDNof the 2nd node. (For single node cluster, skip this step).

`-Pool` is the trusted application pool defined in step 2.

By adding all Avaya Breeze™ nodes to the trusted application pool, it provides load-balanced setup for the Presence/IM services from all the hosts.

Repeat this step for each node in a multi-node cluster.

Note:

When creating a trusted application pool (and trusted application computer) in this way, Lync/Skype for Business will issue a warning:

Warning:

Machine xxx from the topology you are publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines.

This warning can be safely ignored as the Avaya Breeze™ nodes are not domain joined in Microsoft Active Directory, and you should answer “Yes” to this warning.

4. Create a trusted application representing Presence Services. Use the **`New-CsTrustedApplication`** cmdlet to create a trusted application represents the Presence Services.

```
New-CsTrustedApplication -ApplicationID edps -TrustedApplicationPoolFqdn sc-8209-
cl-03.avaya.com -Port 5063
```

`-ApplicationID` is friendly identifier for the trusted application.

`-TrustedApplicationPoolFqdn` is the trusted application pool created in step 2.

5. Create a static route for Aura Presence/IM domain routing and associate this route with trusted application pool. Use the New-CsStaticRoute & Set-CsStaticRoutingConfiguration cmdlets to create Static Route associated with global routing table.

   ```
   $newstaticroute = New-CsStaticRoute -TLSRoute -Destination sc-8209-
   cl-03.avaya.com -Port 5063 -MatchUri bvwlab.com -UseDefaultCertificate $true

   Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$newstaticroute}
   ```

   -TLSRoute defines that the static route we are creating will use SIP TLS transport.

   -Destination is the FQDN of the next hop server for routing Presence or IM messages.

   In this example, the routing destination is the Avaya Breeze™ cluster FQDN.

   -Port is the Presence Service port for federation, default is 5063.

   -MatchUri is the domain suffix used to determine if the Presence/IM message is being sent to an Aura user handle by this route. In this example, Lync or Skype client watching Aura client aura-user@bvwlab.com will use the defined static route, sending to destination at FQDN sc-8209-cl-03.avaya.com.

   Note:

   Microsoft Federation supports a shared domain setup, in which the Microsoft domain can be the same as Aura Presence or IM domain. In this shared domain configuration, Lync or Skype for Business will only send Presence or IM requests to Aura client which is not defined as Lync or Skype client. And Microsoft Federation also supports different domains between MS domain and Aura Presence or IM domain. If static routes for additional domains are required, re-run the two cmdlets above, substituting the –MatchUri parameter with desired Aura Presence or IM domain name.

6. Enable the new Topology. Use Enable-CsTopology cmdlet to enable the newly create topology.

   The cmdlet has no passed parameter.

Restarting the Front End service

About this task

After completing DNS changes, install Certificate for the Front End service and configuring trusted applications. It is recommended to restart Front End services.

Procedure

1. On the Microsoft Front End Server, run **Server Manager**, under **SERVICES** section.
2. In Lync system, locate the Lync Server services and in Skype for Business system, locate the Skype for Business Server services.
3. Right-click the selected services, Stop Services then Start Services, or perform single step of Restart Services.

Avaya Breeze™ server certificates

Configuring Avaya Breeze™ server Trusted Certificate for a single Microsoft Front End server

About this task

Use this procedure to install Front End Certificate to Avaya Breeze™ Trusted Certificate store.

Procedure

1. Log in to System Manager web console, select **Inventory** > **Manage Elements**, and select Avaya Breeze™ server.
2. Click **More Actions** > **Manage Trusted Certificates** > **Add**.

   ✱ **Note:**

   The system might display as Configure Trusted Certificates from different System Manager version.
3. In the **Add Trusted Certificate** window, in the **Select Store Type to add trusted certificate** field, select **WEBSPHERE**.
4. Select **Import using TLS** option, enter Front End Server IP Address and port is `5061`.
5. Click **Retrieve Certificate**.
6. Verify the Certificate Details to confirm it is from the Front End Server, click **Commit**.

   There will be an additional certificate entry for WEBSPHERE from Front End server.
7. Click **Done** to complete the Trusted Certificate configuration.
8. Restart Avaya Breeze™ server to make sure certificate change takes effect.

   The Restart operation can be deferred until after finishing both Trusted Certificate and Identity Certificate configurations.

   In multi-node Avaya Breeze™ cluster setup, repeat this procedure for each node.

Configuring Avaya Breeze™ server Trusted Certificate for a pool of Microsoft Front End servers

Procedure

1. In a browser, enter the URL of the Certificate Authority (CA).

   The URL is usually `https://<server-name>/certsrv/`.
2. When prompted, enter the login credentials.
3. Click **Download a CA certificate, certificate chain, or CRL**.
4. Select **Base 64** as the encoding method.
5. Click **Download CA certificate chain**.
6. Click **Save** to download the certificate file.

7. Log in to System Manager web console, select **Inventory** > **Manage Elements**, and select Avaya Breeze™ server.
8. Click **More Actions** > **Manage Trusted Certificates** > **Add**.

   ✱ **Note:**

   The system might display as Configure Trusted Certificates from different System Manager version.
9. In the **Add Trusted Certificate** window, in the **Select Store Type to add trusted certificate** field, select **WEBSPHERE**.
10. Select **Import using file** option.
11. Click **Choose File** and select the certificate you saved in Step 6.
12. Click **Retrieve Certificate**.
13. Verify the Certificate Details and click **Commit**.
14. Click **Done** to complete the Trusted Certificate configuration.
15. Restart Avaya Breeze™ server to make sure certificate change takes effect.

    The Restart operation can be deferred until after finishing both Trusted Certificate and Identity Certificate configurations.

    In multi-node Avaya Breeze™ cluster setup, repeat this procedure for each node.

Configuring Avaya Breeze™ server Identity Certificate

Procedure

1. Log in to System Manager web console, select **Inventory** > **Manage Elements**, and select Avaya Breeze™ server.
2. Click **More Actions** > **Manage Identity Certificates**.

   ✱ **Note:**

   The system might display as Configure Identity Certificates from different System Manager version.
3. In the **Manage Identity Certificates** window, select **WebSphere**, and click **Replace**.
4. Select **Replace this Certificate with Internal Signed Certificate** and enter the following details:
   - **Common Name (CN)**: Select the check box and enter the Avaya Breeze™ server Security Module FQDN. The Avaya Breeze™ server Security Module FQDN is constructed from the Avaya Breeze™ server management FQDN short host name and suffix of -sm100.
   - **Key Algorithm**: Select **RSA**.
   - **Key Size**: Select **2048**.

- **Subject Alternative Name**: DNS Name: Select the check box and enter (1) the same Avaya Breeze™ server Security Module FQDN as in the CN field (2) the Avaya Breeze™ Cluster FQDN separated by a comma.

You can use a third party certificate. The certificate must have the Avaya Breeze™ Security Module FQDN in the Common Name (CN) field and have Subject Alternative Name (SAN) field as described above. You must select the **Import third party certificate** option.

5. Click **Commit**.
6. Click **Done** to complete the Identity Certificate configuration.
7. Restart Avaya Breeze™ server to make sure certificate change takes effect.

   You can defer the Restart operation after finishing both Trusted Certificate and Identity Certificate configurations.

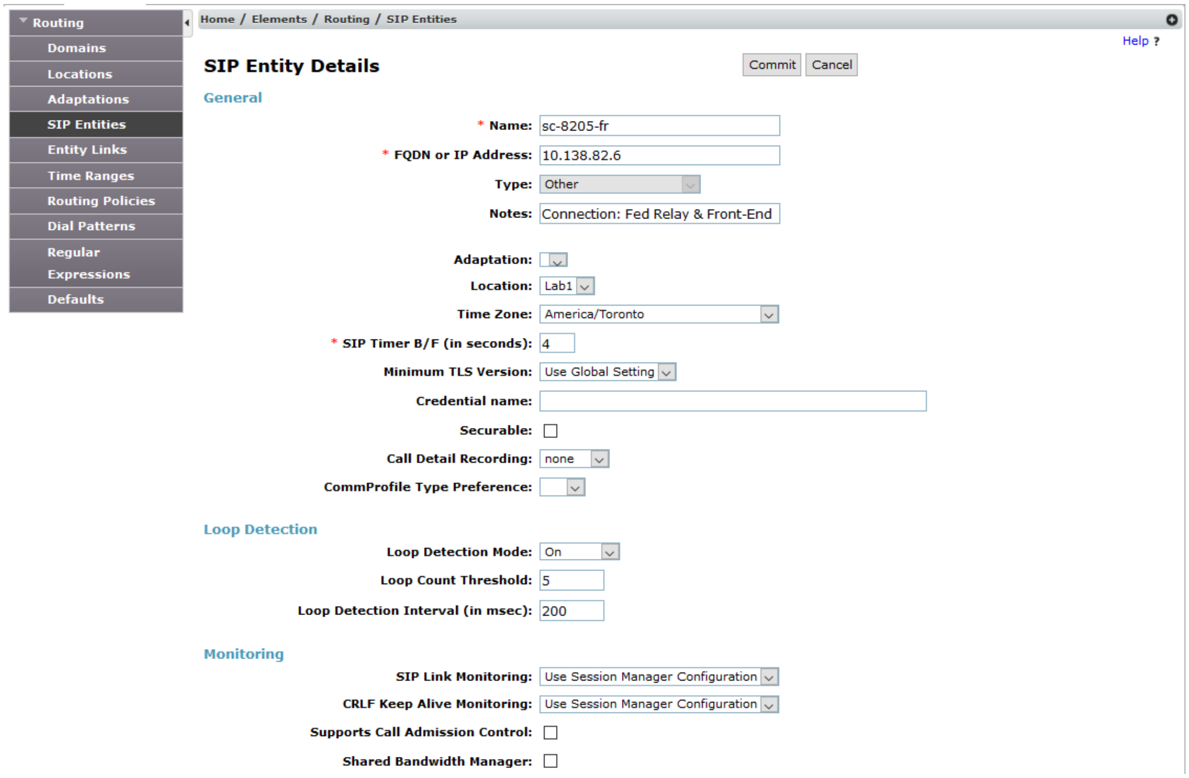
   In multi-node Avaya Breeze cluster setup, repeat this procedure for each node.

Configuring the SIP Entity and Entity Link to PS Federation Relay service

Procedure

1. Log in to System Manager web console.
2. Click **Routing > SIP Entities > New**.
3. Add a new SIP Entity entry represents PS Federation Relay and enter the following fields:
   - **Name**: Enter the name of this SIP Entity.
   - **FQDN or IP Address**: Enter Breeze server Security Module IP address.
   - **Type**: Type `Other`.
   - **SIP Link Monitoring**: Select **Use Session Manager Configuration**.

   Use default values for other fields.



SIP Entity Details

General

* Name:	sc-8205-fr
* FQDN or IP Address:	10.138.82.6
Type:	Other
Notes:	Connection: Fed Relay & Front-End
Adaptation:	
Location:	Lab1
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	none
CommProfile Type Preference:	

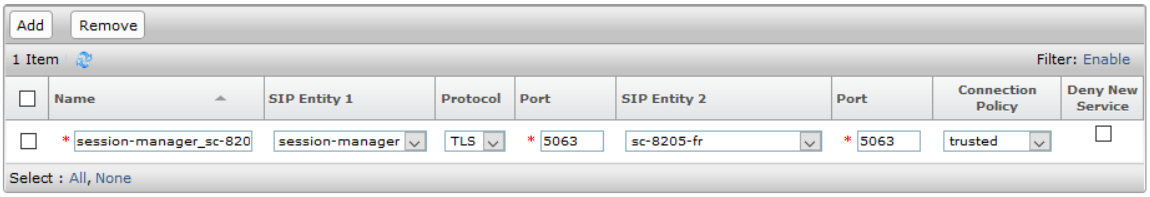
Loop Detection

Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

Monitoring

SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□

4. Click **Commit** to save the SIP Entity configuration.
5. Add Entity Link between Session Manager and the PS Federation Relay service using the following:
   - Protocol TLS and default port 5063.
   - The connection policy must be set to `trusted`.



1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* session-manager_sc-820	session-manager	TLS	* 5063	sc-8205-fr	* 5063	trusted	□

Select : All, None

Note:

In multiple SM setup, create Entity Link from each SM to the same PS Federation Relay service.

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

   Repeat the same procedure for each Breeze server in a multi-node cluster setup.

Configuring Avaya Breeze™ attributes

Procedure

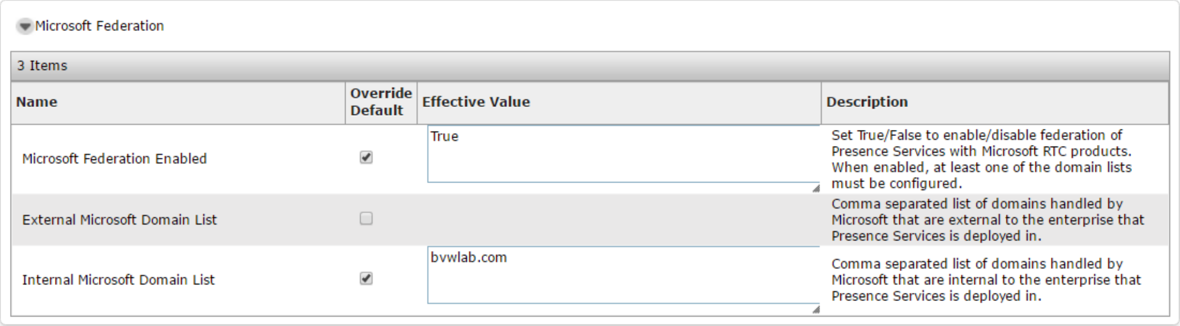
1. On the System Manager web console, click **Elements** > **Avaya Breeze™**.

2. In the navigation pane, click **Configuration** > **Attributes**.
3. Click the Service Clusters tab or Service Globals tab.
   - If Microsoft Federation only applies to one Breeze Cluster, you should use the Service Clusters tab for the Attribute setting.
   - Select the Service Globals tab option if the configuration is for all the Breeze Clusters.
4. In the **Service** field, select the PresenceServices snap-in service.

   The table displays the attributes that you can configure for the service, including a description of each attribute
5. In the Microsoft Federation section:
   a. **Microsoft Federation Enabled**: Select the **Override Default** check box, enter True in the **Efficetive Value** field.

   b. Internal Microsoft Domain List: Select the **Override Default** check box, enter the list of Microsoft domain names, comma separated if there are multiple Microsoft domains.
6. Click **Commit**.

   The following screenshot shows Microsoft Federation Attribute configuration for Microsoft domain bvwlab.com:



Microsoft Federation

3 Items

Name	Override Default	Effective Value	Description
Microsoft Federation Enabled	☑	True	Set True/False to enable/disable federation of Presence Services with Microsoft RTC products. When enabled, at least one of the domain lists must be configured.
External Microsoft Domain List	☐		Comma separated list of domains handled by Microsoft that are external to the enterprise that Presence Services is deployed in.
Internal Microsoft Domain List	☑	bvwlab.com	Comma separated list of domains handled by Microsoft that are internal to the enterprise that Presence Services is deployed in.

Configuring DNS Server Avaya Breeze™ nodes

About this task

The DNS server used by Avaya Breeze™ does not need to be the same as the one used by the Microsoft servers. But in either case, the SRV and A records verified in Step 1, need to be resolvable by the DNS used by all Avaya Breeze™ nodes.

Note:

The DNS configuration can be during Avaya Breeze™ installation, or can be adjusted later using the CLI command `CEnetSetup`.

Procedure

1. Verify DNS SRV Record representing Microsoft domain service locator and verify Front End server FQDN to IP address resolution using Linux cli command..

In the Microsoft RTC, Lync or Skype for Business configuration, it should have this `_sipinternaltls._tcp` SRV Record defined. The SRV record provides service location for Lync or Skype client to locate the service from Front End server. The same SRV Record is also used by Presence Service to locate the Front End server for Presence/IM service.

```
$ nslookup -querytype=srv _sipinternaltls._tcp.bvwlab.com 10.138.82.42
Server    :         10.138.82.42
Address    :        10.138.82.42#53
_sipinternaltls._tcp.bvwlab.com service = 1 100 5061 sip.bvwlab.com
$ nslookup sip.bvwlab.com
Server    :         10.138.82.42
Address    :        10.138.82.42#53
Name        :   sip.bvwlab.com
Address    : 10.138.82.43
```

In this example, the DNS Server IP address is 10.138.82.42 and `_sipinternaltls._tcp` SRV Record for domain `bvwlab.com` points to Front End server FQDN of `sip.bvwlab.com` and Front End FQDN `sip.bvwlab.com` is revolved to IP address `10.138.82.43`.

2. Restart Presence Service Snap-in after modifying Breeze DNS resolver configuration file.

Adding or updating the existing Communication Manager application

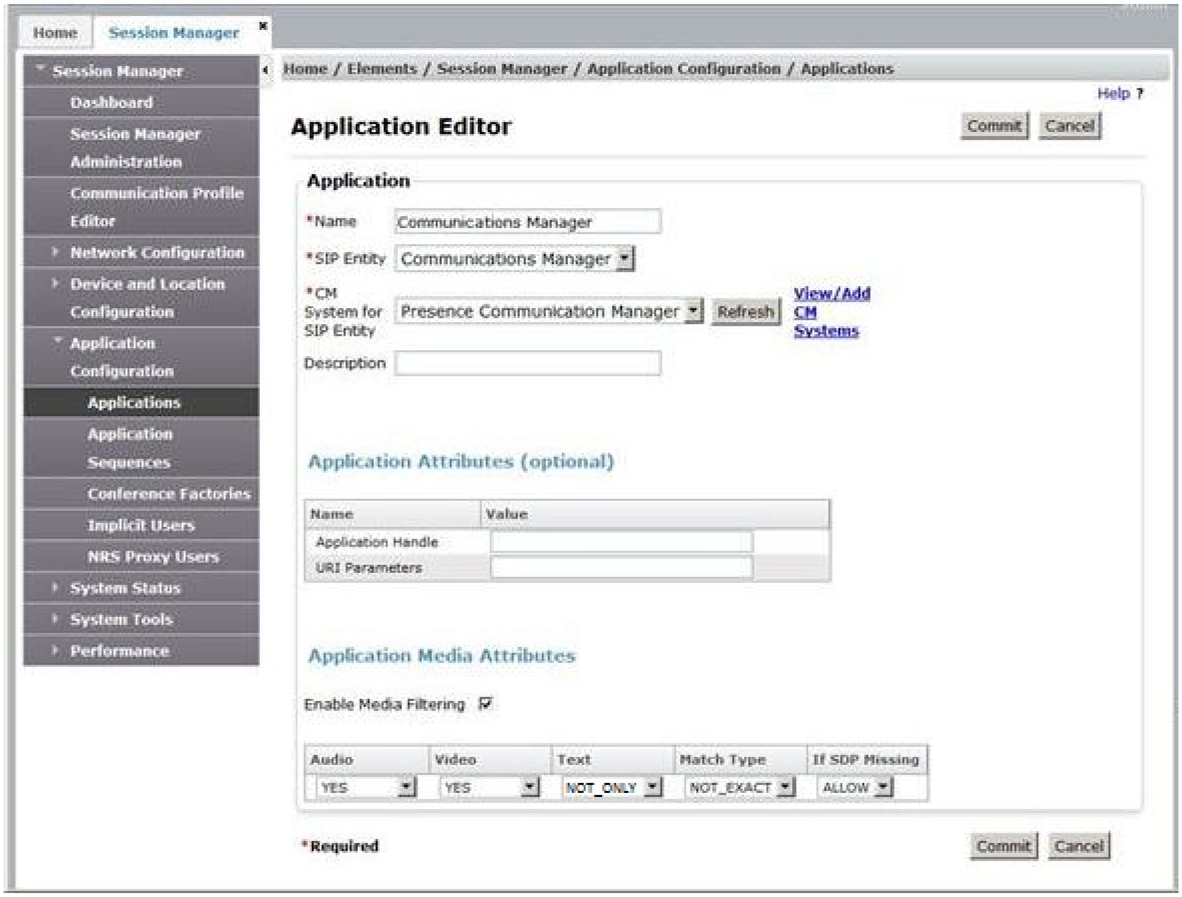
About this task

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**.



Application Editor

Application

*Name	Communications Manager
*SIP Entity	Communications Manager
*CM System for SIP Entity	Presence Communication Manager
Description	

Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

Application Media Attributes

Enable Media Filtering ☑

Audio	Video	Text	Match Type	If SDP Missing
YES	YES	NOT_ONLY	NOT_EXACT	ALLOW

*Required

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

Subscribe for status with Microsoft RTC and Publish status to Microsoft RTC

Presence Services Release 7.1.2 supports the following:

- Subscribe for status with Microsoft RTC
- Publish status to Microsoft RTC

The subscriptions are associated with Hybrid federation user. If configured with Microsoft SIP handle, a presence enabled Avaya Aura® user is a Hybrid federation user. For more information about configuring a Hybrid federation user, see *Adding Microsoft SIP user handles to System Manager*.

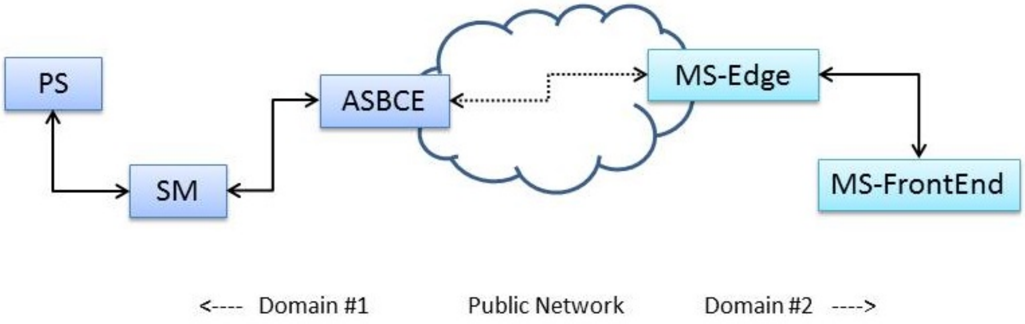
To enable the functionality, you must configure the Microsoft Real Time Communication (RTC) Federation.

- **Subscribe for status with Microsoft RTC federation**: When enabled, Avaya Aura® Hybrid User presence status is the aggregation of presence states from two sources: Avaya Aura®, and Microsoft RTC Client. By default, it is enabled. You can override to disable the functionality.

- **Publish status to Microsoft RTC**: When enabled, Avaya Aura® Hybrid User call state is published to Microsoft RTC to allow presence status aggregation in Microsoft RTC Client. By default, it is disabled. You can override to enable the functionality.

Microsoft federation with external domains

The following diagram illustrates the message flow and server connections of the different components required to deploy External Domain federation:



Checklist for configuring Microsoft Federation with External Domains

No.	Task	Reference	✔
DNS Configuration			
1	Add a DNS A record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server.	Adding a DNS A record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server on page 103	

Table continues…

No.	Task	Reference	✔
2	Add a DNS reverse pointer record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server.	Adding a DNS reverse pointer record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server on page 103	
Avaya Session Border Controller for Enterprise Configuration			
1	Create and install the identity certificate used by Avaya Session Border Controller for Enterprise.	Creating and installing the identity certificate used by Avaya Session Border Controller for Enterprise on page 106	
2	Retrieve the Microsoft Edge CA certificate.	Retrieving the Microsoft Edge CA certificate on page 107	
3	Configure a TLS Client Profile used to connect to the Microsoft Edge.	Configuring a TLS Client Profile used to connect to the Microsoft Edge on page 108	
4	Configure a TLS Client Profile used to connect to the Session Manager.	Configuring a TLS Client Profile used to connect to the Session Manager on page 109	

Table continues…

No.	Task	Reference	✔
5	Configure a TLS Server Profile used to receive connections from the Microsoft Edge.	Configuring a TLS Server Profile used to receive connections from the Microsoft Edge on page 110	
6	Configure a TLS Server Profile used to receive connections from the Session Manager.	Configuring a TLS Server Profile used to receive connections from the Session Manager on page 111	
7	Configure the Microsoft Edge external Signaling Interface.	Configuring the Microsoft Edge external Signaling Interface on page 112	
8	Configure the Session Manager internal Signaling Interface.	Configuring the Session Manager internal Signaling Interface on page 113	
9	Configure the Media Interfaces.	Configuring the Media Interfaces on page 114	
10	Configure the Server Interworking Profiles.	Configuring the Server Interworking Profiles on page 115	
11	Configure the End Point Policy Groups.	Configuring the End Point Policy Groups on page 120	

Table continues…

No.	Task	Reference	✔
12	Configure the Server Configuration Profiles.	Configuring the Server Configuration Profiles on page 116	
13	Configure the Routing Profiles.	Configuring the Routing Profiles on page 121	
14	Configure the DNS server used by Avaya Session Border Controller for Enterprise.	Configuring the DNS server used by the Avaya Session Border Controller for Enterprise on page 123	
15	Enable External Topology Hiding.	Enabling External Topology Hiding on page 124	
16	Enable Internal Topology Hiding.	Enabling Internal Topology Hiding on page 125	
17	Set up the Microsoft Edge Border Rule.	Setting up the Microsoft Edge Border Rule on page 126	
18	Create a Signaling Manipulation Script.	Creating a Signaling Manipulation Script on page 127	
19	Create the End Point flows.	Creating endpoint flows on page 128	
Microsoft Edge Server SIP Federated Domain Configuration			

Table continues…

No.	Task	Reference	✔
1	Configure the SIP Federated Domain.	Configuring the SIP federated domain on page 131	
Routing between Session Manager and Avaya Session Border Controller for Enterprise Configuration			
1	Set up the required certificates for Session Manager.	Setting up required certificates for Session Manager on page 133	
2	Set up the Avaya Session Border Controller for Enterprise Entity and Entity Link.	Setting up the Avaya Session Border Controller for Enterprise Entity and Entity Link on page 133	
3	Set up the Session Manager Routing Policy.	Setting up the Session Manager Routing Policy on page 135	
4	Set up the Session Manager Regular Expression.	Setting up the Session Manager Regular Expression on page 136	
Presence Services Microsoft Federation Attributes Configuration			
1	Set up the cluster attributes for External Domain Microsoft Federation.	Setting up cluster attributes for External Domain Microsoft Federation on page 137	
Communication Manager configuration			

Table continues…

No.	Task	Reference	✔
1	Add or update the existing Communication Manager application.	Adding or updating the existing Communication Manager application on page 96	

DNS configuration

The DNS server used by the Avaya Aura® components does not need to be the same as the one used by the Microsoft servers. However, if not, the Microsoft Edge and Avaya Session Border Controller for Enterprise fully qualified domain names (FQDN) must be resolvable by the DNS used by the Avaya Session Border Controller for Enterprise server.

The following DNS entries must be made on the DNS server used by the Microsoft Edge and Avaya Session Border Controller for Enterprise:

1. Add a DNS A record so that the FQDN of the Avaya Session Border Controller for Enterprise external interface is resolvable by the Microsoft Edge server.
2. Add a DNS reverse pointer for the Avaya Session Border Controller for Enterprise external interface IP address to resolve the Avaya Session Border Controller for Enterprise external interface FQDN.

Adding a DNS A record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server

Procedure

1. Log in to the Microsoft DNS server as an administrator.
2. In the Forward Lookup Zones section, create the domain for Avaya Session Border Controller for Enterprise, if it does not exist.
3. Right-click the correct domain and select **New Host (A)**.
4. In the New Host dialog box, enter the Avaya Session Border Controller for Enterprise host name and IP address.
5. Click **Add Host** > **OK**, and then click **Done**.

   Note:

   When adding a new Host (A) record, you can select the **Create associated pointer (PTR) record** check box. This setting might eliminate the need to add the host name to **Reverse Lookup Zone**, if the zone already exists.

Adding a DNS reverse pointer record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server

Procedure

1. Log in to the Microsoft DNS server as an administrator.

2. In the navigation pane, click **Reverse Lookup Zones** > **New Zone**.
3. On the Action menu, click **New Zone**.
4. Select **Primary zone and store the zone** in Active Directory.
5. Click **Next**.
6. Click **To all DNS servers in the Active Directory domain** .
7. Click **Next**.
8. Enter the Network ID portion of the IP address corresponding to the Avaya Session Border Controller for Enterprise external interface, and click **Next**.
9. Select **Allow both non-secure and secure dynamic updates**, and click **Next**.
10. Click **Finish**.
11. Right-click the created zone and select **New Pointer (PTR)**.
12. In the **Host IP number** field, enter the Avaya Session Border Controller for Enterprise external IP address.
13. In the **Host Name** field, enter the FQDN of the Avaya Session Border Controller for Enterprise external interface.
14. Click **OK**.

Configuring Avaya Session Border Controller for Enterprise

About this task

A session border controller is a device used to exert control over incoming and outgoing signaling and media streams in an enterprise Avaya Aura® solution. It is typically deployed at the edge of a corporate network and used to control inbound and outbound sessions.

In the Presence Services to Microsoft external domain federation deployment, the Avaya Session Border Controller for Enterprise is used to isolate the Aura servers from the public network.

In addition to the configuration described in *Administering Avaya Session Border Controller for Enterprise*, the following must be configured and or executed to setup federation:

Note:

It is strongly recommended that TLS 1.2 be used in all TLS Client and Server Profiles.

Procedure

1. Generate Avaya Session Border Controller for Enterprise identity certificate to be used in the TLS Client Profiles. This certificate will be used in creating TLS client connections to the Microsoft Edge server and also to the Session Manager in the internal Avaya Aura® network/domain.
2. Retrieve the CA certificate from the Microsoft Edge server to import into the Avaya Session Border Controller for Enterprise.
3. Retrieve the CA certificate from the Session Manager to import into the Avaya Session Border Controller for Enterprise. If the System Manager is used as the CA, the Session

Manager CA can be downloaded from the System Manager via the Services; Security; Certificates; Authority; CA Structure & CRLs page.

4. Create two TLS Client Profiles for the outgoing connections to the Microsoft Edge and Session Manager.
5. Create two TLS Server Profiles for the incoming connections from the Microsoft Edge and Session Manager.
6. Configure an external Signaling Interface using the external TLS Server Profile.
7. Configure an internal Signaling Interface using the internal TLS Server Profile.
8. Create internal and external Media Interfaces.
9. Create Server Interworking Profiles for both the Session Manager and Microsoft Edge.
10. Create Server Configuration Profiles for both the Session Manager and Microsoft Edge.
11. Default Application Rules can be used, as there is no customization required.
12. Default Media Rules can be used, as there is no customization required.
13. Default Signaling Rules can be used, as there is no customization required.
14. Create two End Point Policy Groups for the Microsoft Edge and the Session Manager.
    a. The Microsoft Edge End Point Policy Group requires a Border Rule.
    b. The Session Manager End Point Policy Group uses defaults, as there is no customization required.
15. Create two Routing Profiles for the Microsoft Edge and the Session Manager. Each Routing Profiles will use the specific Server Configuration Profile created for Microsoft Edge and Session Manager.
16. Avaya Session Border Controller for Enterprise specific configuration for System Manager to Microsoft federation:
    a. The DNS server used by the Avaya Session Border Controller for Enterprise needs to be able to resolve the FQDN of the Microsoft Edge server.
    b. Enable topology hiding in both directions. Only enable topology hiding for the following headers: Via, SDP, and Record-Route. Specifically not Request-Line, To or From. This is required to enable back-to-back SIP dialogs between the Microsoft Edge and the Session Manager using FQDNs for Record Routes and Contact URIs.
    c. Setup a Border Rule for the Microsoft Edge End Point Policy Group. This changes the contact in the initial SUBSCRIBE message sent from the System Manager to use an FQDN instead of an IP address. This is required to enable the Microsoft Edge to properly send NOTIFYs back to System Manager.
    d. Create a Signaling Manipulation Rule to remove the GSID request URI parameter from the in-dialog SUBSCRIBEs sent from System Manager to the Microsoft Edge. This is required, since the Edge will not accept the modified in-dialog SUBSCRIBE request URI.

17. Create two End Point Flows. End Point Flows associate the various configuration profiles and options together to control signaling messages that flow thru the Avaya Session Border Controller for Enterprise.

Creating and installing the identity certificate used by Avaya Session Border Controller for Enterprise

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **TLS Management** > **Certificates**.
3. Click **Generate CSR**, and enter the following details:
    a. The certificate **Common Name** field should be set to the FQDN of the Avaya Session Border Controller for Enterprise.

    b. The certificate **Subject Alt Name** fields should have the following included: **DNS**:`<FQDN-of-Avaya Session Border Controller for Enterprise>`, **IPAddress**:`<IP Address of the external interface>`, **IPAddress**:`<IP Address of the internal interface>`.

    c. **Client and Server authentication** enabled.

    d. **Key usage** set to Digital Signature and Key Encipherment.

    e. Set and confirm the passphrase.
4. Download the CSR and private key file and use your Certificate Authority (CA) to sign the request and generate the identity certificate.

    For example, the Session Manager CA can be used to achieve this.
5. In **TLS Management**; **Certificates**, click **Install** to import the Avaya Session Border Controller for Enterprise identity certificate and private key file.
6. The CA certificate used to sign the CSR and identity certificate must be loaded into each server that will receive client connections from the Avaya Session Border Controller for Enterprise. This allows those servers (that is, Microsoft Edge and Session Manager) to authenticate incoming TLS client connections from the Avaya Session Border Controller for Enterprise.
7. For Standalone Avaya Session Border Controller for Enterprise, after installing the certificate, the following CLI command must be executed to sync the private key with the certificate:
    a. Log in to the Avaya Session Border Controller for Enterprise through SSH using a tool like putty.

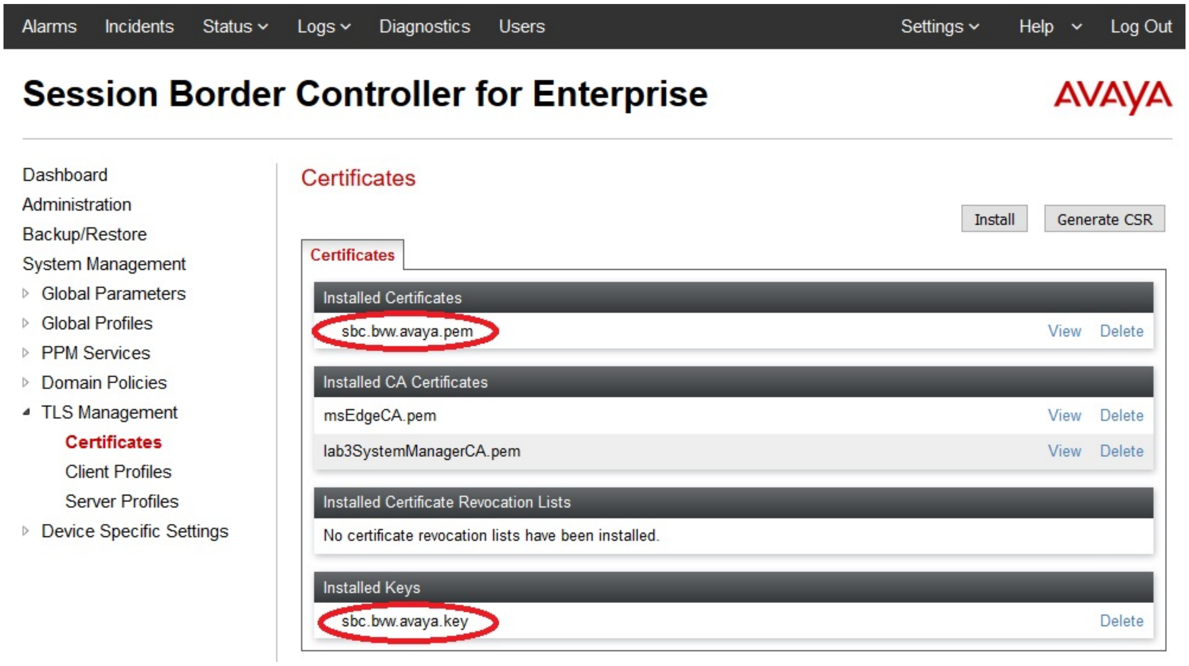
    b. Change to the directory: `/usr/local/ipcs/cert/key`.

    c. Execute the command: `enc_key <private-key-file-name> <passphrase> .`

    ```
    # cd /usr/local/ipcs/cert/key
    ```

    ```
    # enc_sbc.bvw.avaya.key avaya123
    ```

8. Using System Management, select **Restart Application** to restart the Avaya Session Border Controller for Enterprise.



Certificates

Installed Certificates

sbc.bvw.avaya.pem

Installed CA Certificates

msEdgeCA.pem

lab3SystemManagerCA.pem

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Keys

sbc.bvw.avaya.key

Retrieving the Microsoft Edge CA certificate

Procedure

1. Log in to the Microsoft Edge server as the administrator.
2. Start the Microsoft Lync or Skype for Business Deployment wizard.
3. Click **Install or Update Skype for Business Server System**.
4. Click **Run Again** in Step 3.

   The system displays the Certificate Wizard.
5. In the Certificate Wizard, select the **External Edge Certificate (public Internet)** group.
6. Click **view**.
7. Click **View Certificate Details**.

   The system displays the Microsoft Edge identity certificate.
8. Select **Certification Path**.
9. Select the CA certificate and click **View Certificate**.

   The system displays the Microsoft Edge CA certificate.
10. Click the **Details** tab; and click **Copy to File…**.
11. Select **Base-64 encoded X.509 (.CER)**.
12. Click **Next**.

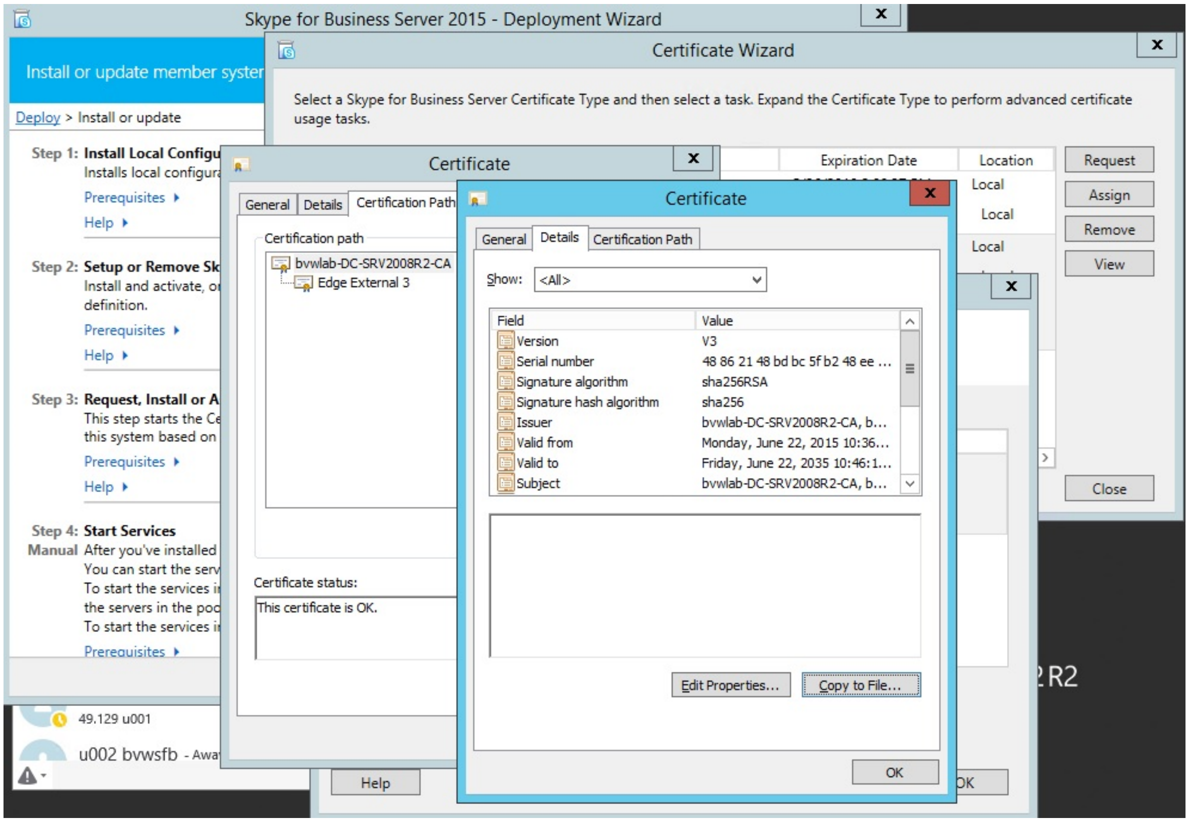
13. Enter a filename for the CA certificate file, and click **Next**.

    For example, `msEdgeCA`.

14. Click **Finish** to save the file.
15. Click **OK** to close the Export was successful dialog box.

    The exported CA certificate file will be used in client and server profiles created in subsequent procedures.

16. Rename the certificate file from `msEdgeCA.cer` to `msEdgeCA.pem`.



Select a Skype for Business Server Certificate Type and then select a task. Expand the Certificate Type to perform advanced certificate usage tasks.

Certification path: bvwlab-DC-SRV2008R2-CA > Edge External 3

Certificate status: This certificate is OK.

Show: <All>

Field	Value
Version	V3
Serial number	48 86 21 48 bd bc 5f b2 48 ee ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	bvwlab-DC-SRV2008R2-CA, b...
Valid from	Monday, June 22, 2015 10:36...
Valid to	Friday, June 22, 2035 10:46:1...
Subject	bvwlab-DC-SRV2008R2-CA, b...

Configuring a TLS Client Profile used to connect to the Microsoft Edge

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **TLS Management** > **Client Profiles**.
3. Click **Add** and name the profile.

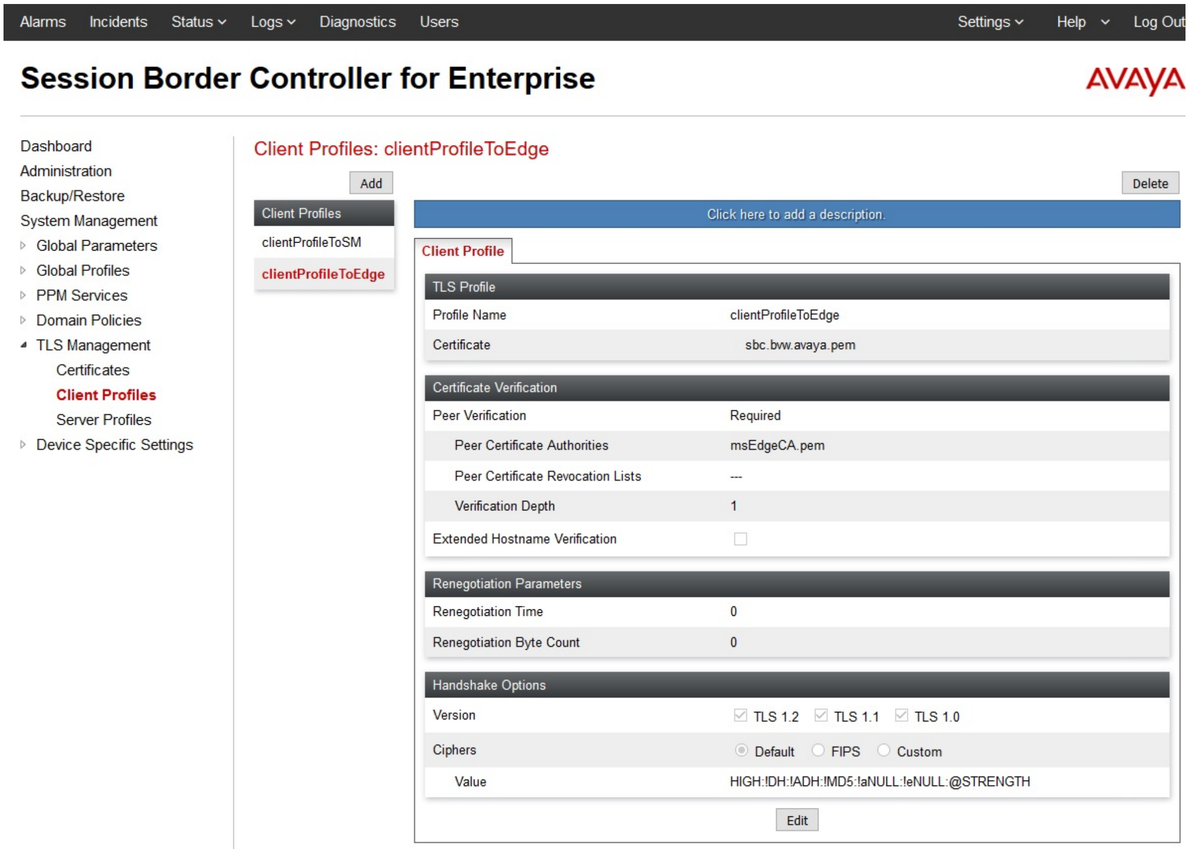
   For example: `clientProfileToEdge`.

4. Select the Avaya Session Border Controller for Enterprise identity certificate created in the earlier procedure from the certificate menu.
5. Configure Peer Verification as shown in the following figure:

6. Select the peer CA certificate and a verification depth of `1`.
7. To load the peer CA, click **TLS Management** > **Certificates** > **Install** > **CA certificate**.
8. Browse to the certificate file and click **upload**.

   In the following example, the peer CA is `msEdgeCA.pem`, which was used to sign the Microsoft Edge identity certificate.
9. Select the versions of TLS required.

   It is recommended to use TLS 1.2.
10. Customize the encryption ciphers as required.



Session Border Controller for Enterprise

Client Profiles: clientProfileToEdge

TLS Profile	
Profile Name	clientProfileToEdge
Certificate	sbc.bw.avaya.pem
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	msEdgeCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 ☑ TLS 1.1 ☑ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Configuring a TLS Client Profile used to connect to the Session Manager

Procedure

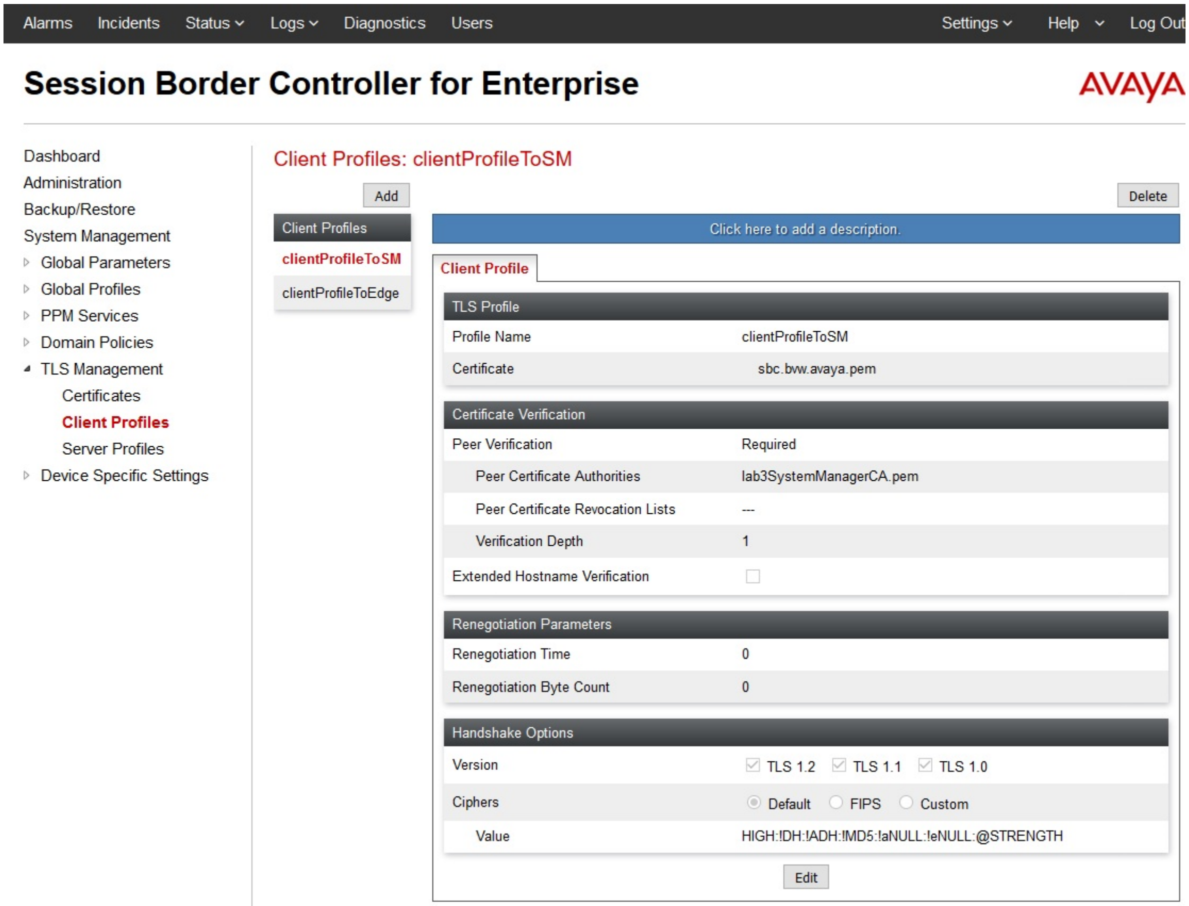
1. Repeat the earlier procedure to create a similar client profile used to connect to the Session Manager.

   For more information, see “Configuring a TLS Client Profile used to connect to the Microsoft Edge”.
2. Assign a name to the profile appropriately.

   For example: `clientProfileToSM`.

3. Configure Peer Verification using the peer Session Manager CA certificate.
4. Select the versions of TLS required.

   It is recommended to use TLS 1.2.
5. Customize the encryption ciphers as required.



Client Profiles: clientProfileToSM

TLS Profile	
Profile Name	clientProfileToSM
Certificate	sbc.bw.avaya.pem
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	lab3SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 ☑ TLS 1.1 ☑ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Configuring a TLS Server Profile used to receive connections from the Microsoft Edge

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **TLS Management** > **Server Profiles**.
3. Click **Add** and assign a name to the profile.

   For example: `serverProfileExternal`.
4. Select the Avaya Session Border Controller for Enterprise identity certificate created earlier.
5. If peer certificate verification is desired, enable **Peer Verification**, and select the peer CA certificate.

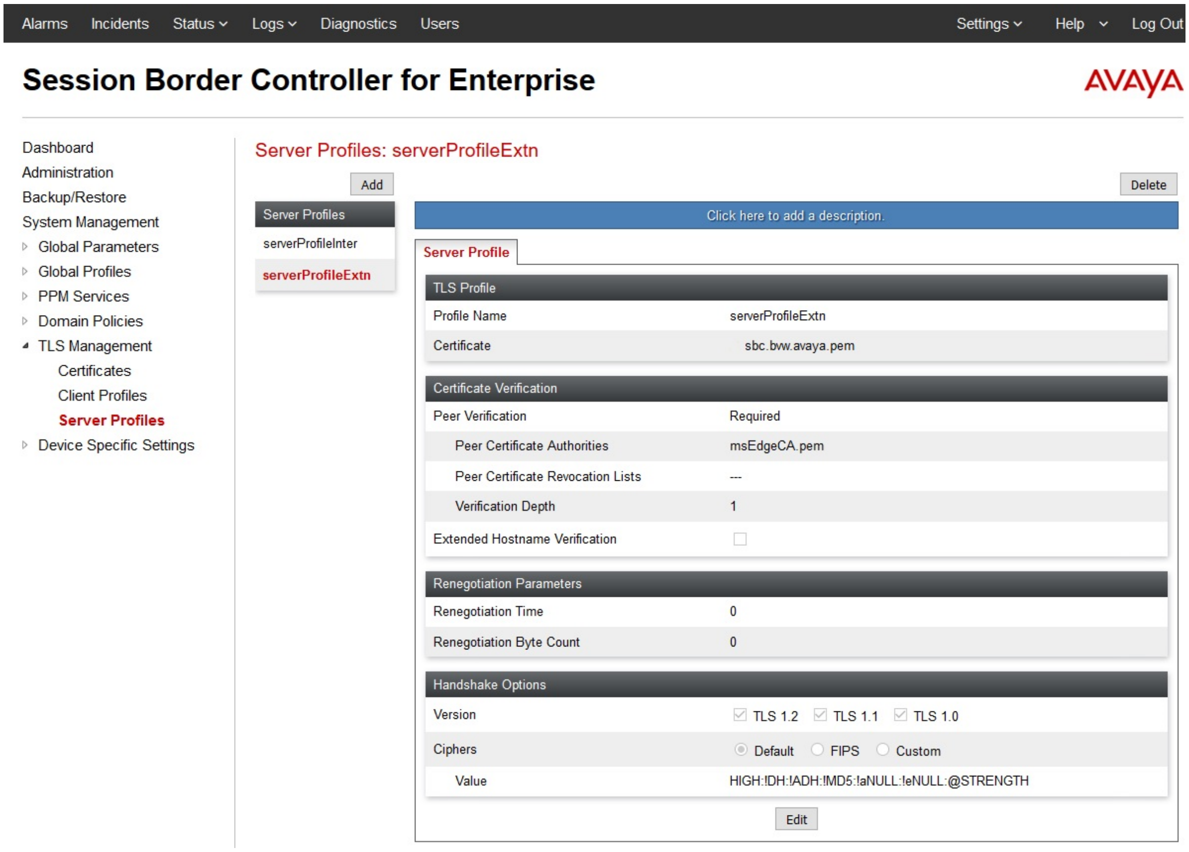
This CA can be loaded from **TLS Management** > **Certificates** > **Install** > **CA certificate** page.

In the following figure below, the peer CA is `msEdgeCA.pem`. This is the CA certificate that was used to sign the Microsoft Edge’s identity certificate.

6. Select the versions of TLS required.

   It is recommended to use TLS 1.2.

7. Customize the encryption ciphers as required.



Session Border Controller for Enterprise

Server Profiles: serverProfileExtn

TLS Profile	
Profile Name	serverProfileExtn
Certificate	sbc.bw.avaya.pem

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	msEdgeCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.2 ☑ TLS 1.1 ☑ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Configuring a TLS Server Profile used to receive connections from the Session Manager

Procedure

1. Repeat the earlier procedure to create a similar server profile used by the Session Manager.

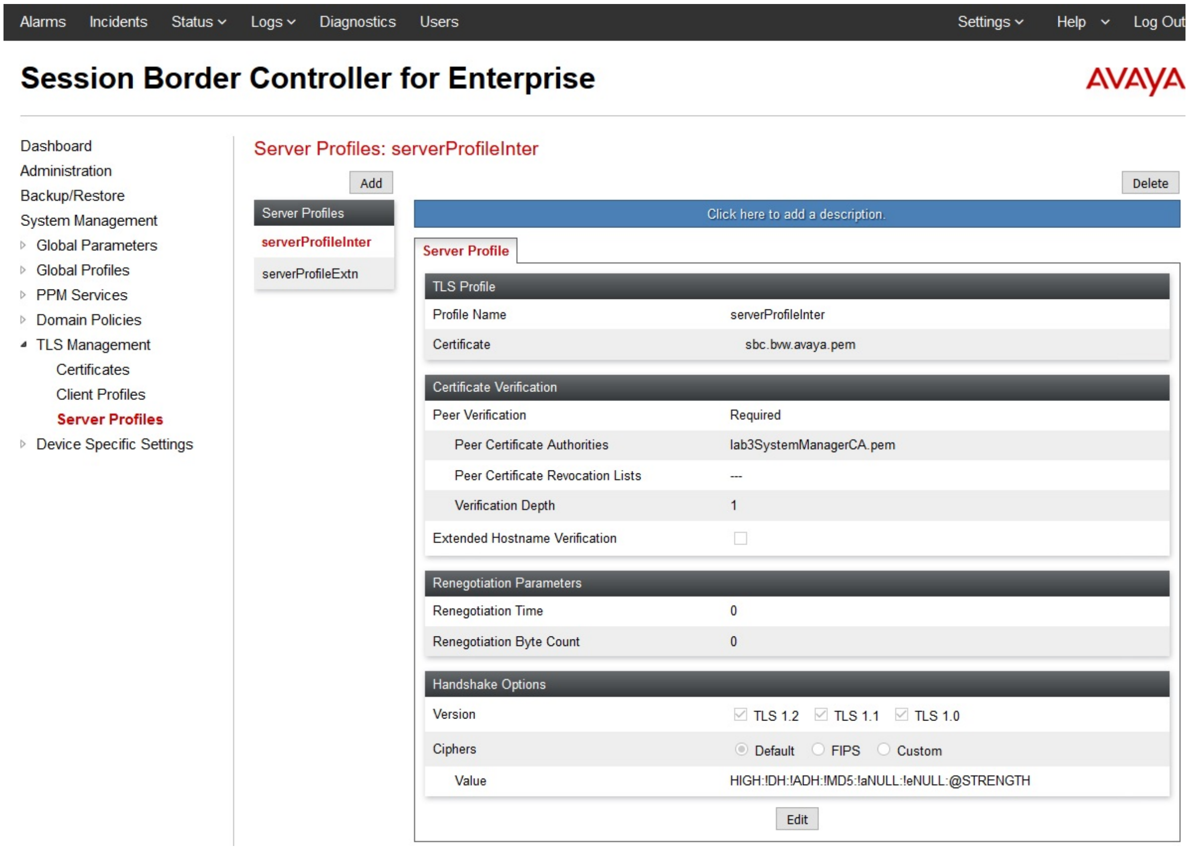
   For more information, see “Configuring a TLS Server Profile used to receive connections from the Microsoft Edge”.

2. Assign a name to the profile appropriately.

   For example: `serverProfileInternal`.

3. If Peer Verification is required, enable Peer Verification and select the peer Session Manager CA certificate.
4. Select the versions of TLS required.

   It is recommended to use TLS 1.2.
5. Customize the encryption ciphers as required.



TLS Profile	
Profile Name	serverProfileInter
Certificate	sbc.bvw.avaya.pem
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	lab3SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	☑ TLS 1.2 ☑ TLS 1.1 ☑ TLS 1.0
Ciphers	● Default ○ FIPS ○ Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

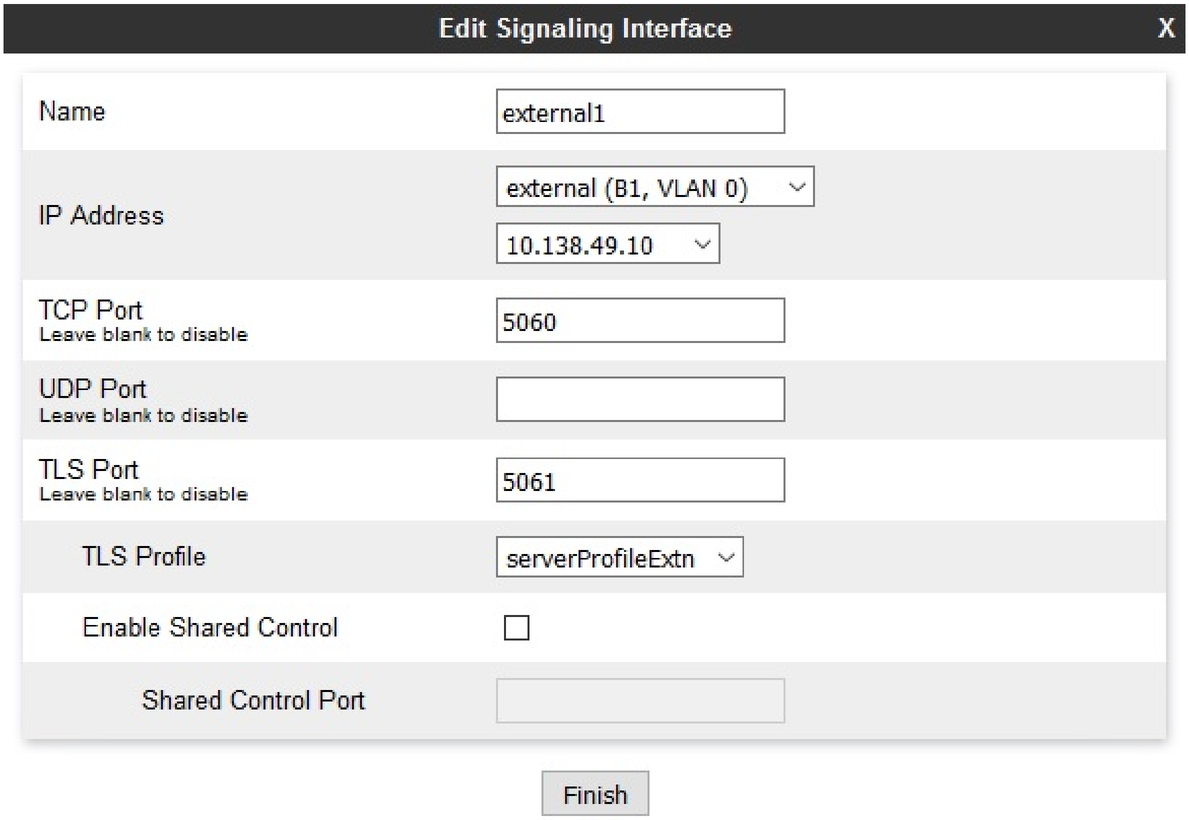
Configuring the Microsoft Edge external Signaling Interface

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Device Specific Settings** > **Signaling Interface**.
3. Click **Add** and name the interface.

   For example: `external1`.
4. Select the interface and IP Address that is connected to the public network where the Microsoft Edge is accessible.
5. Enable TLS by specifying port `5061` and assign the previously created external TLS Server Profile.

   Typically, TCP and UDP are disabled.



Edit Signaling Interface

Name	external1
IP Address	external (B1, VLAN 0) 10.138.49.10
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	serverProfileExtn
Enable Shared Control	□
Shared Control Port	

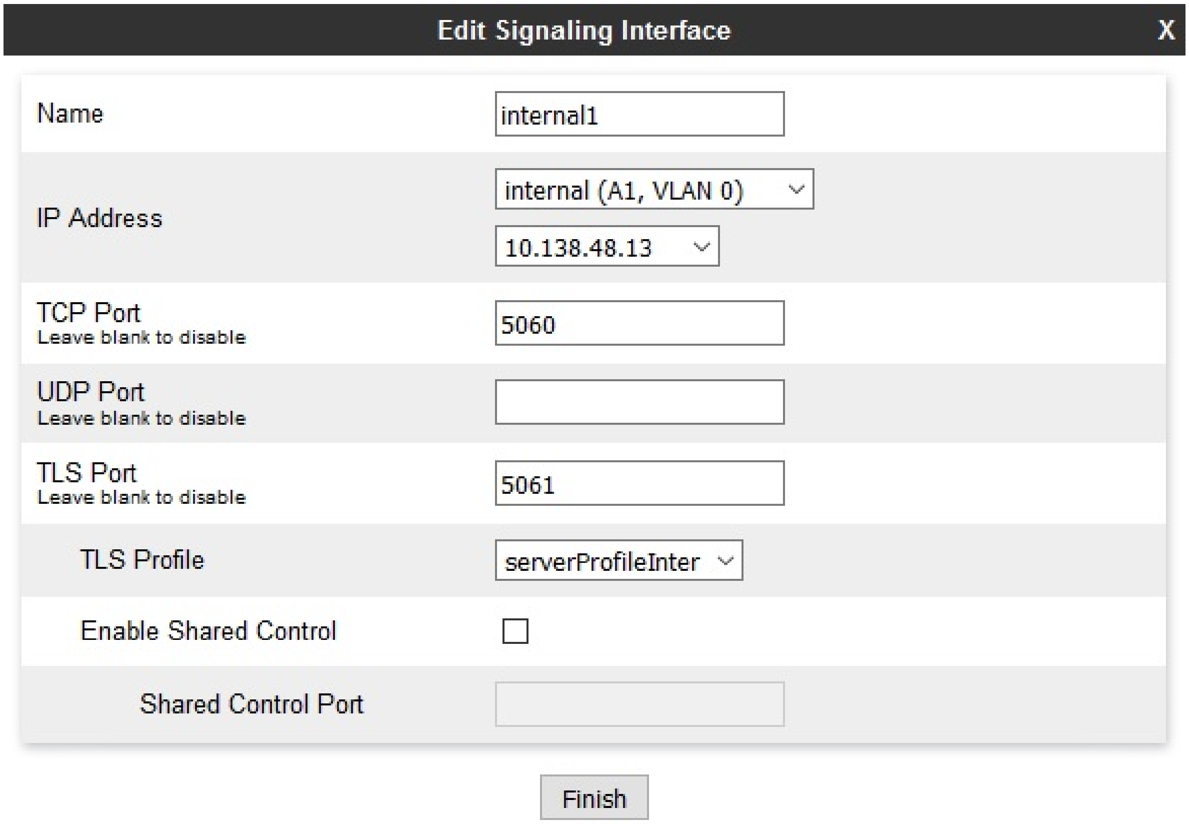
Configuring the Session Manager internal Signaling Interface

Procedure

1. Repeat the earlier procedure to create a similar internal Signaling Interface to be used by Session Manager.
2. Assign a name to the interface appropriately.

   For example: `internal1`.

3. Set the IP Address, ports, and internal TLS Server Profile.



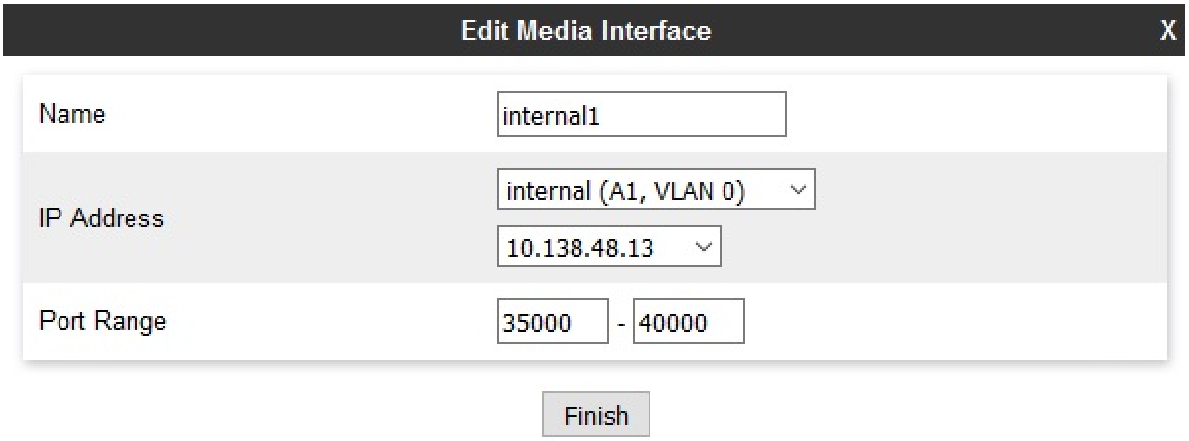
Name	internal1
IP Address	internal (A1, VLAN 0) 10.138.48.13
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	serverProfileInter
Enable Shared Control	□
Shared Control Port	

Configuring the Media Interfaces

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Device Specific Settings** > **Media Interface**.
3. Click **Add** to create the internal Media Interface.
4. Select the internal IP address.

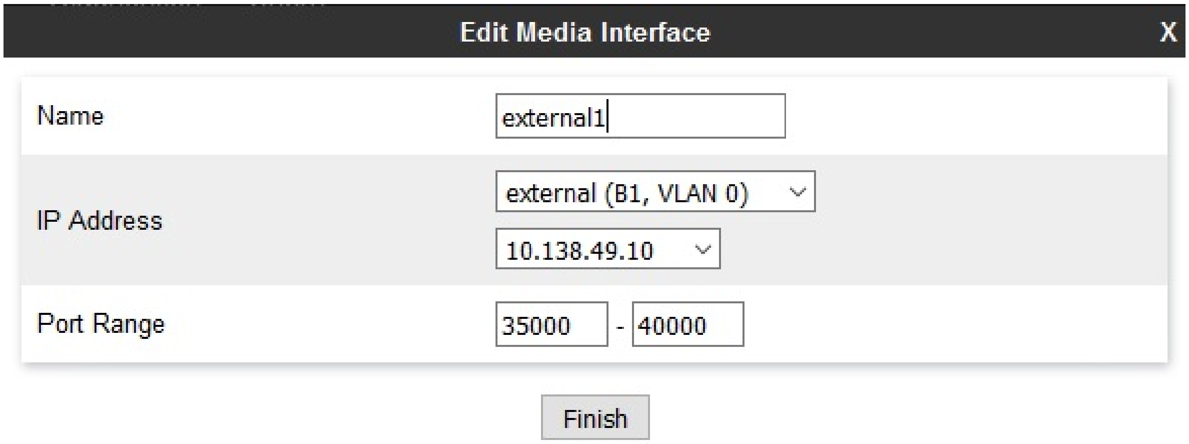
5. Verify that the default Port ranges are acceptable.



Edit Media Interface

Name	internal1
IP Address	internal (A1, VLAN 0) 10.138.48.13
Port Range	35000 - 40000

6. Similarly, click **Add** to create the external Media Interface using the external IP address.



Edit Media Interface

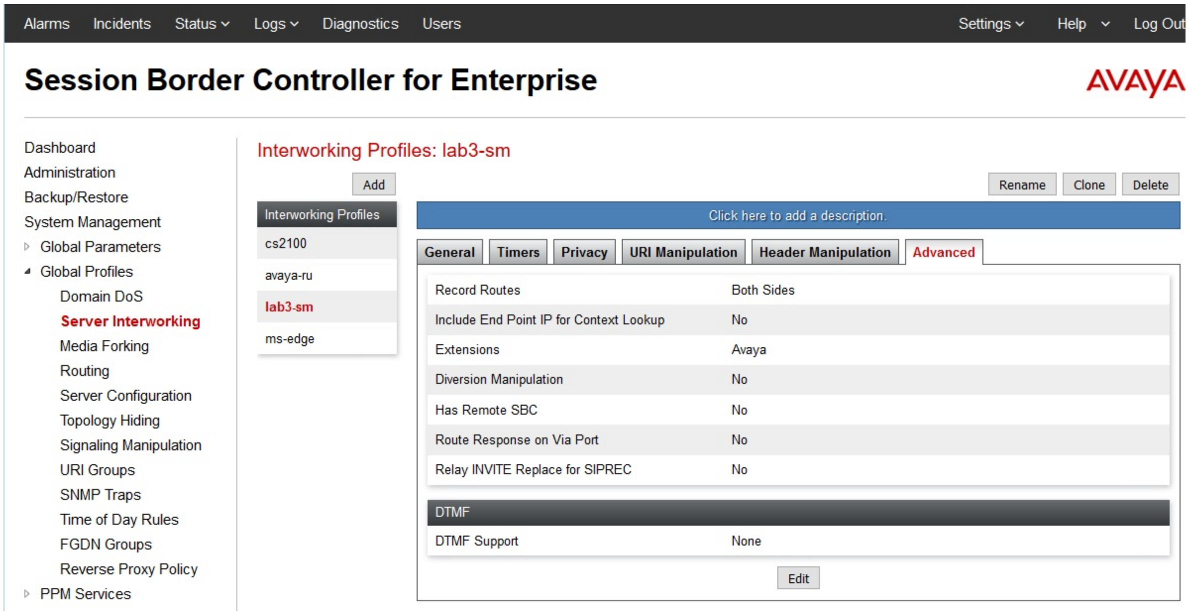
Name	external1
IP Address	external (B1, VLAN 0) 10.138.49.10
Port Range	35000 - 40000

Configuring the Server Interworking Profiles

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Global Profiles** > **Server Interworking**.
3. Click **Add** and assign a name to the profiles.

   For example: `lab3-sm` and `ms-edge`.
4. Use the default settings except for the **Advanced** section.
5. In the **Advanced** section for the **lab3-sm** profile:
   1. Set **Record Routes** to Both Sides.
   2. Set **Extensions** to Avaya.



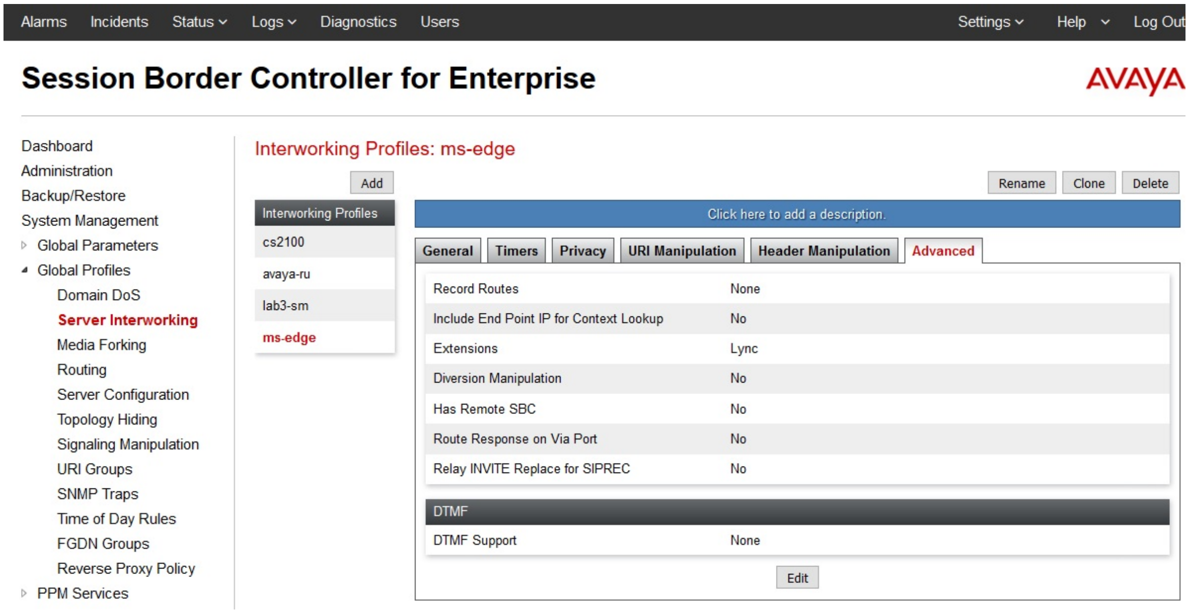
Interworking Profiles: lab3-sm

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	No
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

DTMF

DTMF Support	None

6. In the **Advanced** section for the **ms-edge** profile:
    a. Set **Record Routes** to None.
    b. Set **Extensions** to Lync.



Interworking Profiles: ms-edge

Record Routes	None
Include End Point IP for Context Lookup	No
Extensions	Lync
Diversion Manipulation	No
Has Remote SBC	No
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

DTMF

DTMF Support	None

Configuring the Server Configuration Profiles

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Global Profiles** > **Server Configuration**.

3. Click **Add** and assign a name to the Server Configuration Profiles.

   For example: `lab3-sm` and `ms-edge`.

4. In the **General** tab, set the following:

   a. **Server Type**: `Call Server`

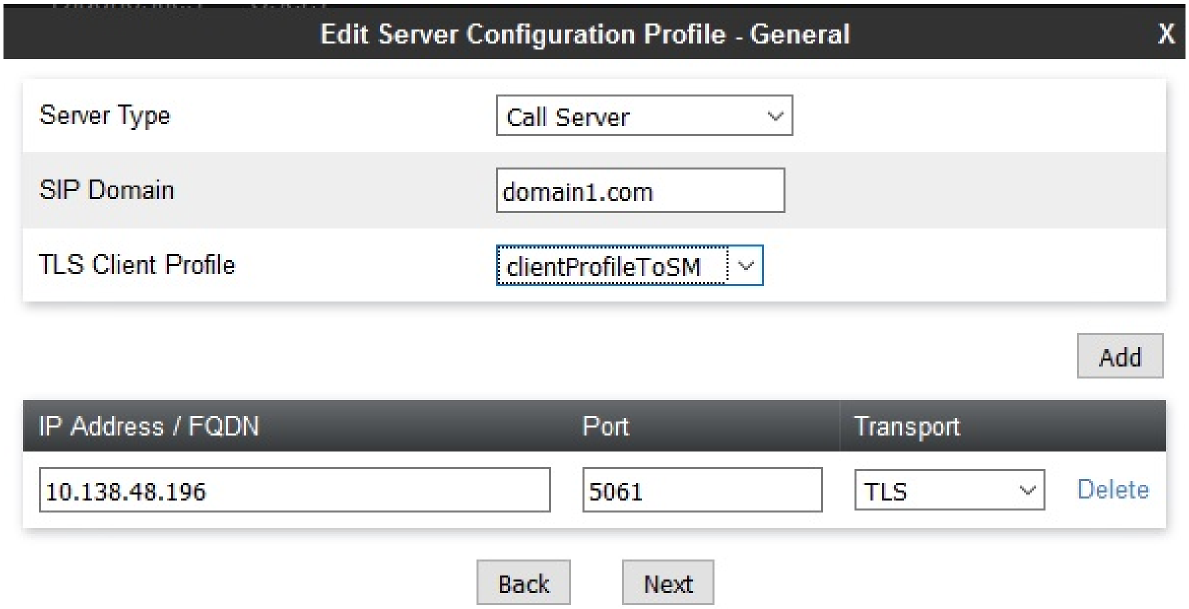
   b. **SIP Domain**: `Aura Presence/IM domain`

   c. **IP Address**: IP Address of the Session Manager Asset Interface

   d. **Port**: `5061`

   e. **Transport**: `TLS`

   f. **TLS Client Profile**: TLS Client Profile to the Session Manager



Edit Server Configuration Profile - General

Server Type	Call Server
SIP Domain	domain1.com
TLS Client Profile	clientProfileToSM

IP Address / FQDN	Port	Transport	
10.138.48.196	5061	TLS	Delete

5. Click **Next**.

   Authentication is disabled.

6. Click **Next**.

   Enable Heartbeat is disabled.

7. Click **Next**.

8. In the **Advanced** tab, set the following:

   a. **DoS Protection**: `disabled`

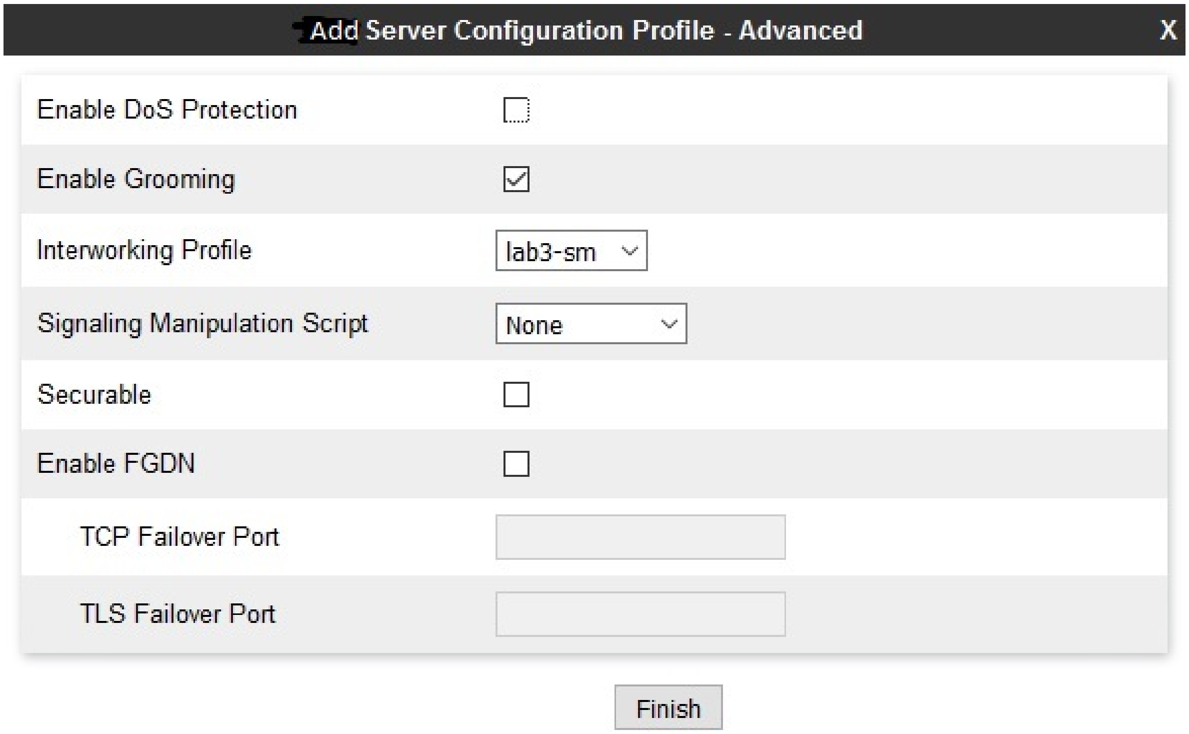
   b. **Grooming**: `enabled`

   c. **Interworking Profile**: Session Manager Interworking Profile.

      For example, `lab3-sm`.

   d. **Signaling Manipulation Script**: `none`
   e. **Securable**: `disabled`
   f. **FGDN**: `disabled`

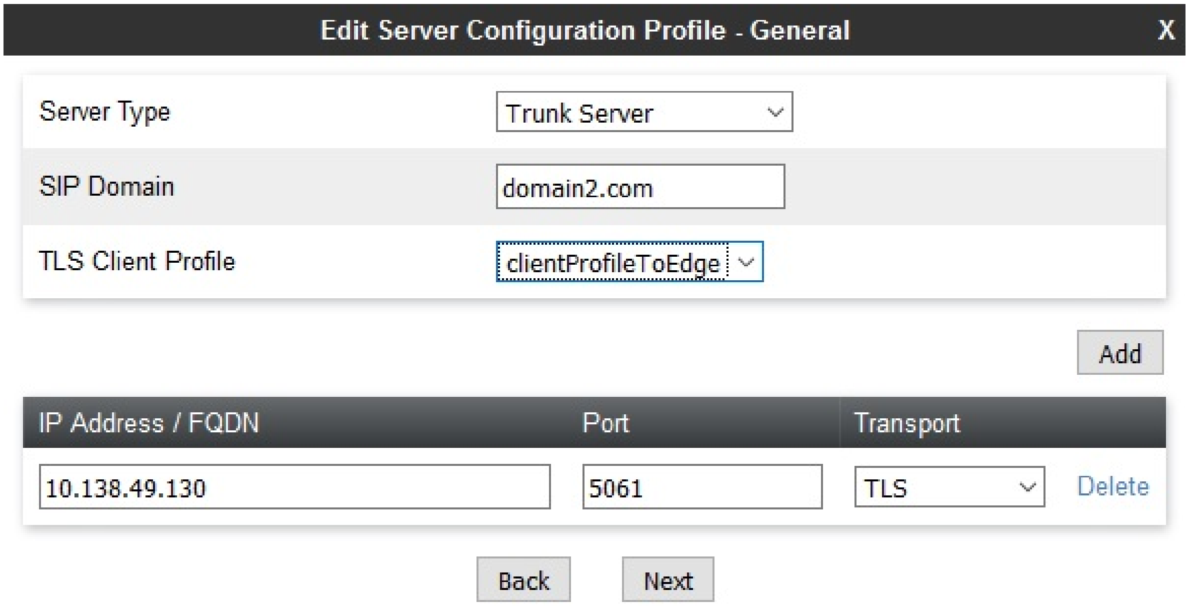
9. Click **Finish** to commit the changes.



[redacted] Add Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	lab3-sm
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	

10. Similarly, click **Add** again to create the Server Configuration Profile for the Microsoft Edge.
11. Assign a name to the profile ms-edge.
12. In the **General** tab, set the following:
    a. **Server Type**: `Trunk Server`
    b. **SIP Domain**: `Microsoft domain`
    c. **IP Address**: IP Address of the Edge server
    d. **Port**: `5061`
    e. **Transport**: `TLS`
    f. **TLS Client Profile**: TLS Client Profile to the Edge



Edit Server Configuration Profile - General

Server Type	Trunk Server
SIP Domain	domain2.com
TLS Client Profile	clientProfileToEdge

IP Address / FQDN	Port	Transport	
10.138.49.130	5061	TLS	Delete

13. Click **Next**.

    Authentication is disabled.

14. Click **Next**.

    Enable Heartbeat is disabled.

15. Click **Next**.

16. In the **Advanced** tab, set the following:

    a. **DoS Protection**: `disabled`

    b. **Grooming**: `enabled`

    c. **Interworking Profile**: Session Manager Interworking Profile.

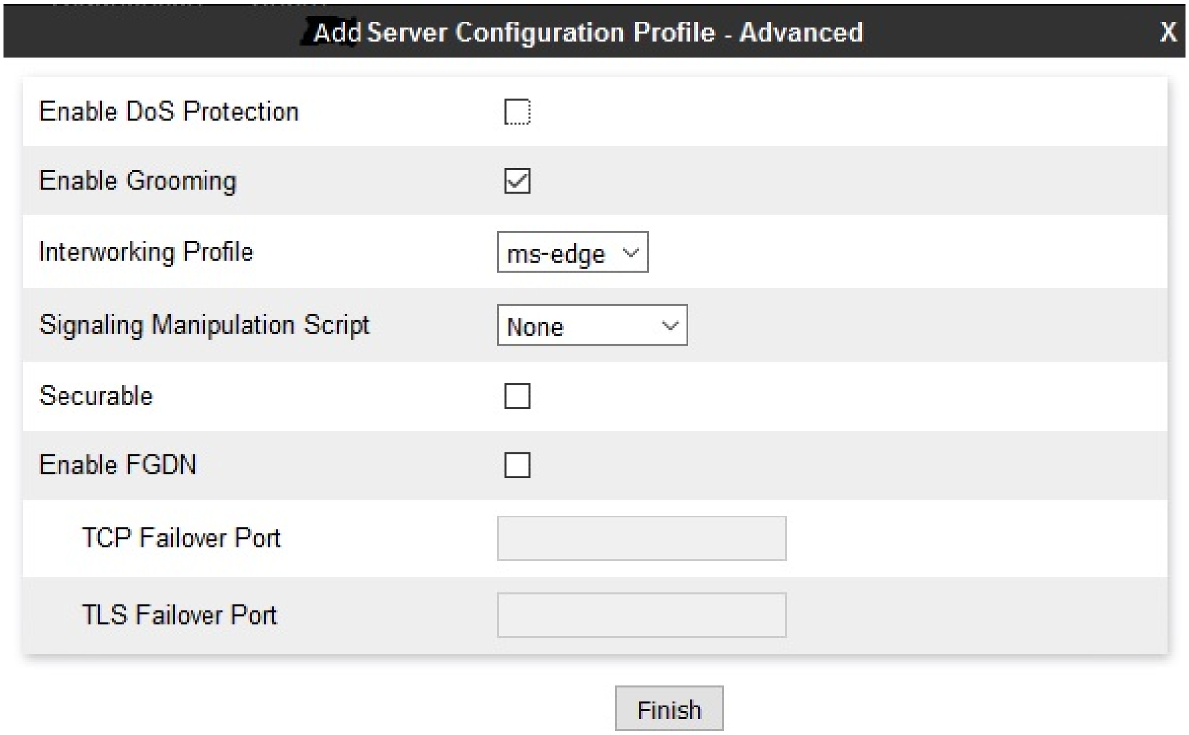
       For example, `ms-edge`.

    d. **Signaling Manipulation Script**: `none`

    e. **Securable**: `disabled`

    f. **FGDN**: `disabled`

17. Click **Finish** to commit the changes.



Add Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	ms-edge
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	

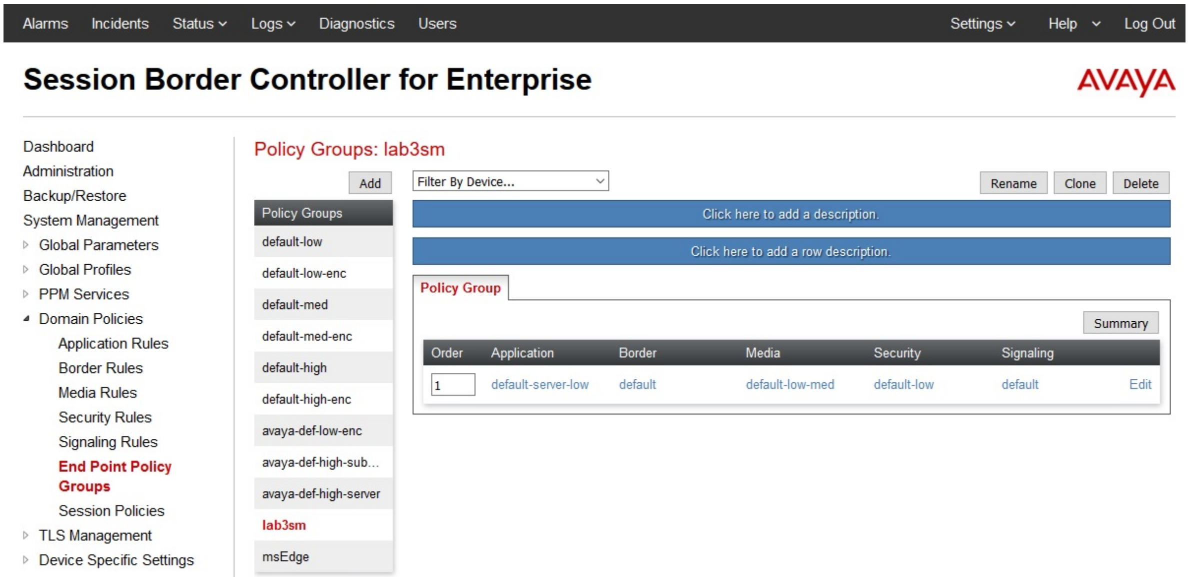
Configuring the End Point Policy Groups

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Domain Policies** > **End Point Policy Groups**.
3. Click **Add** and assign a name to the Policy Groups.

   For example: `lab3sm` and `msEdge`.

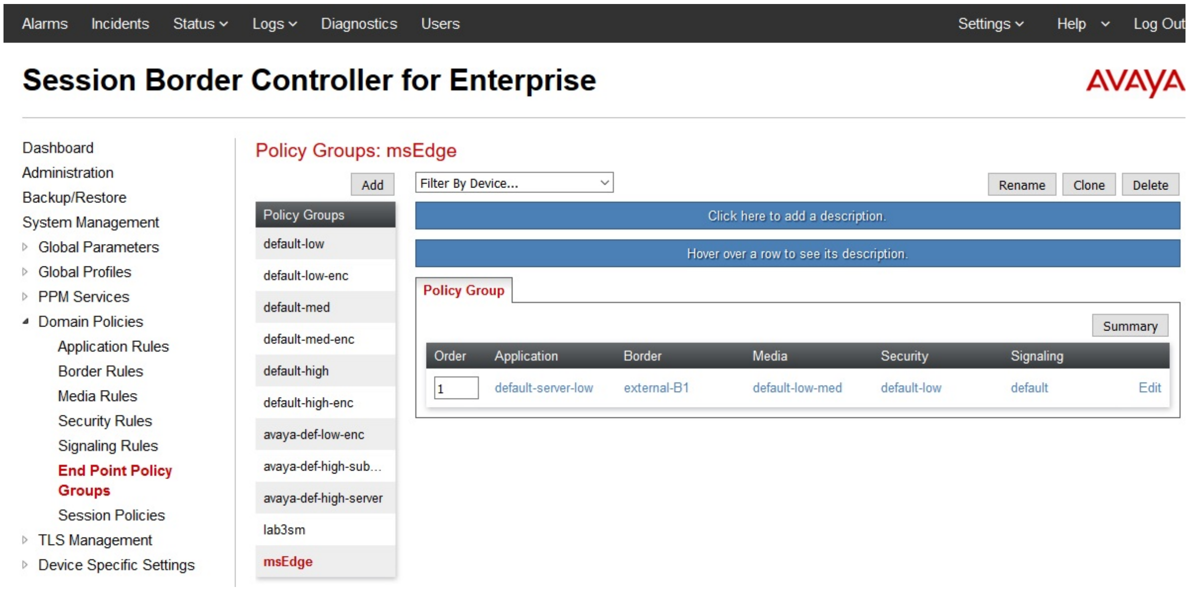
4. For the **lab3sm** Policy Group, use the default settings as show in the following figure:



Order	Application	Border	Media	Security	Signaling	
1	default-server-low	default	default-low-med	default-low	default	Edit

5. For the msEdge Policy Group, use the default settings except for Border. Configure a specific border rule for the Microsoft Edge.

   As shown in the following figure, the Border Rules is named `external-B1`. Refer to the following Border Rule creation procedure.



Order	Application	Border	Media	Security	Signaling	
1	default-server-low	external-B1	default-low-med	default-low	default	Edit

Configuring the Routing Profiles

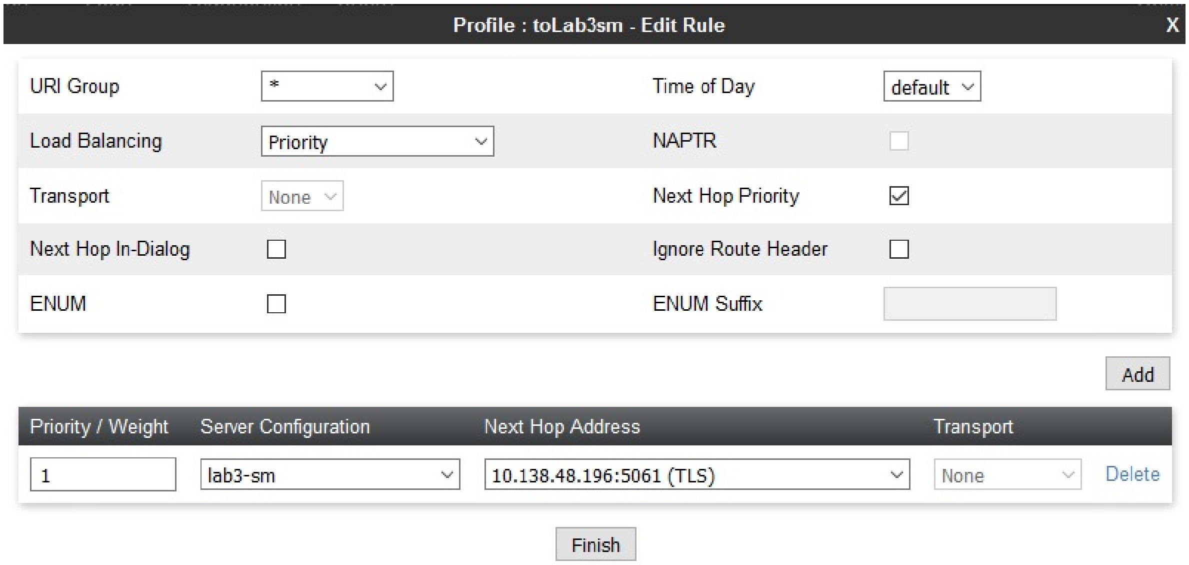
Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Global Profiles** > **Routing**.

3. Click **Add** and assign a name to the Routing Profiles.

   For example: `toLab3sm` and `toMSEdge`.

4. For the **toLab3sm** profile use the default settings, adding the lab3-sm Server Configuration as the Next Hop Address as show in the following figure:

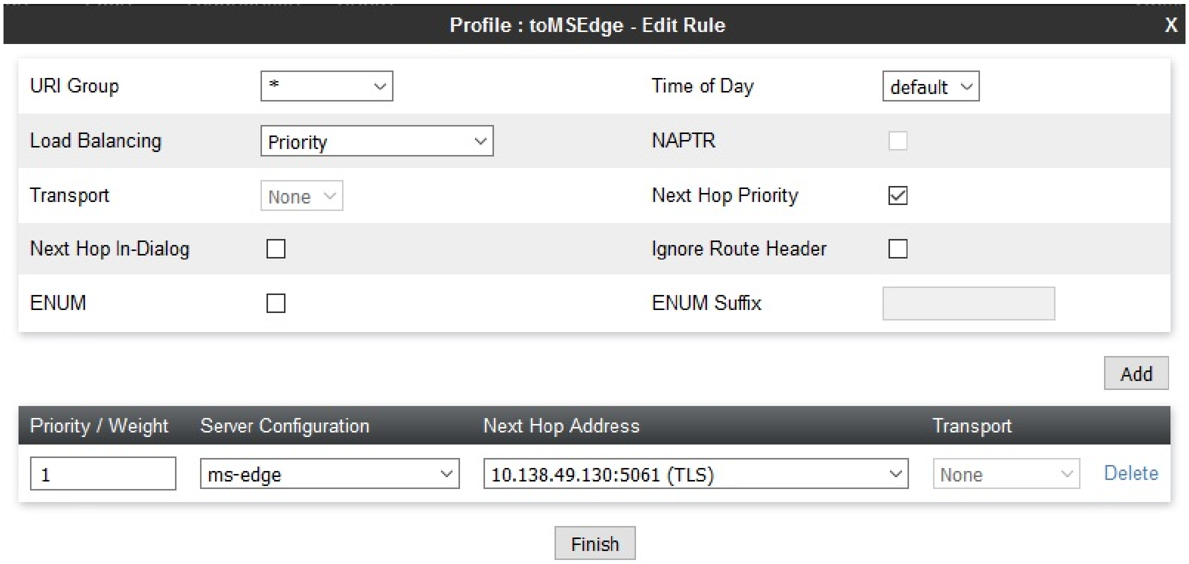


Profile : toLab3sm - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	lab3-sm	10.138.48.196:5061 (TLS)	None	Delete

5. For the **toMSEdge** profile use the default settings, adding the ms-edge **Server Configuration** as the **Next Hop Address** as show in the following figure:



Profile : toMSEdge - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	□	Ignore Route Header	□
ENUM	□	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	ms-edge	10.138.49.130:5061 (TLS)	None	Delete

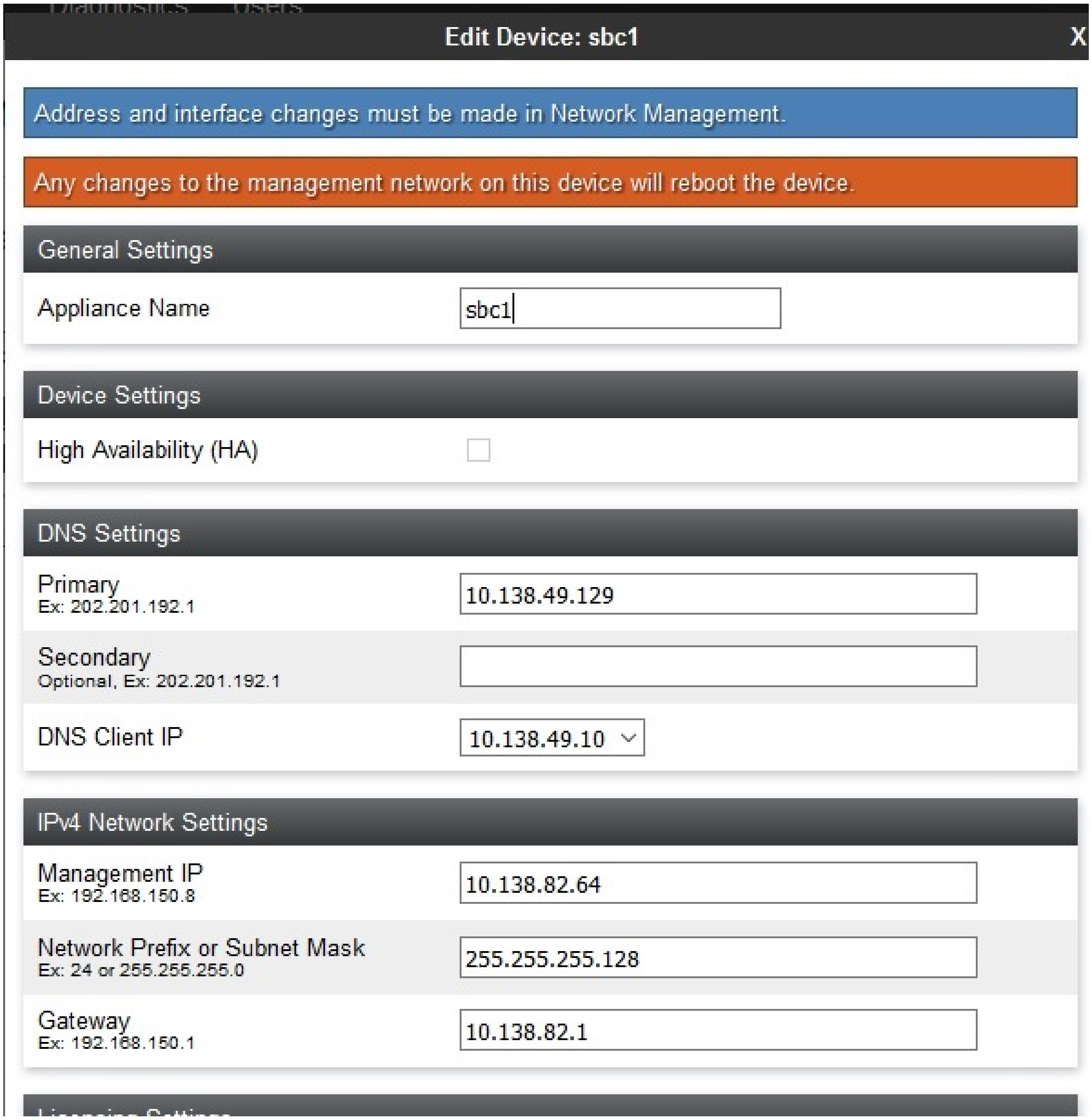
Configuring the DNS server used by the Avaya Session Border Controller for Enterprise

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **System Management**.
3. In the **Device** tab, click the **Edit** link for the Avaya Session Border Controller for Enterprise device.
4. In the **DNS Settings** section, fill in the **Primary** and **Secondary** IP Addresses for the DNS servers.

   In the example below, the DNS primary address is a Microsoft DNS server in the Microsoft domain.
5. Enter an appropriate Client IP that is able to connect to the DNS servers.

6. Using System Management, select **Restart Application** to restart the Avaya Session Border Controller for Enterprise.



Edit Device: sbc1

Address and interface changes must be made in Network Management.

Any changes to the management network on this device will reboot the device.

General Settings

Appliance Name	sbc1

Device Settings

High Availability (HA)	□

DNS Settings

Primary Ex: 202.201.192.1	10.138.49.129
Secondary Optional, Ex: 202.201.192.1	
DNS Client IP	10.138.49.10

IPv4 Network Settings

Management IP Ex: 192.168.150.8	10.138.82.64
Network Prefix or Subnet Mask Ex: 24 or 255.255.255.0	255.255.255.128
Gateway Ex: 192.168.150.1	10.138.82.1

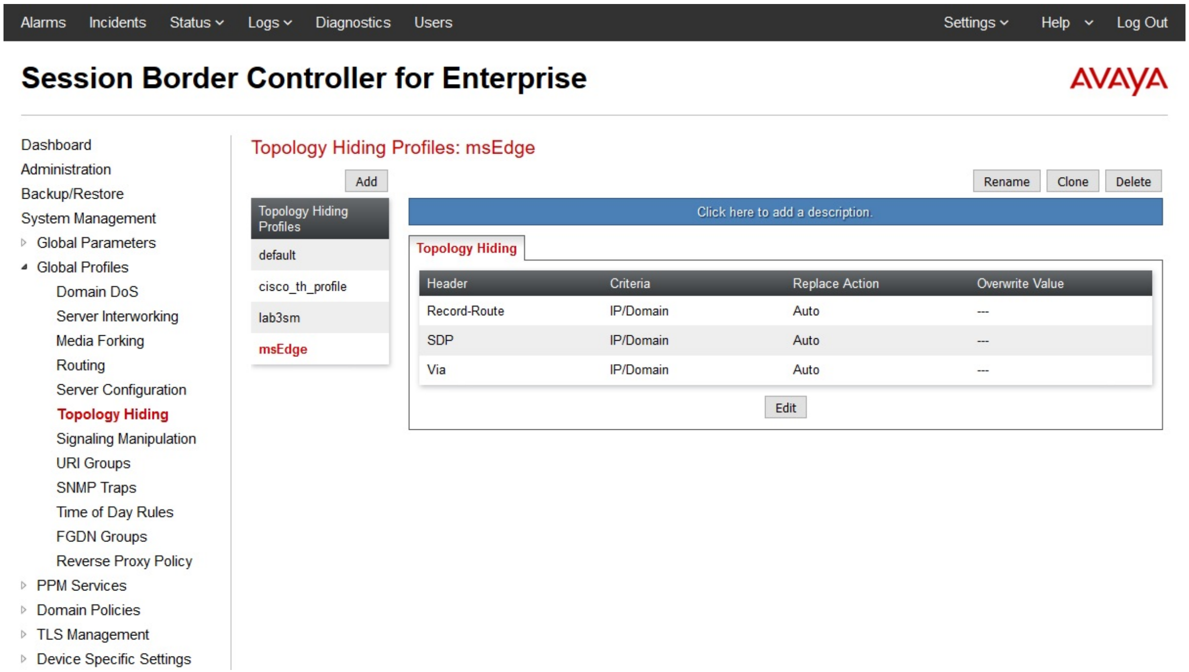
Enabling External Topology Hiding

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Global Profiles** > **Topology Hiding**.
3. Click **Add** and assign a name to the profile.

   For example: `msEdge`.

4. Add the following three headers:
    a. **Record-Route** with **replace action** set to `auto`.
    b. **SDP** with **replace action** set to `auto`.
    c. **Via** with **replace action** set to `auto`.



Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

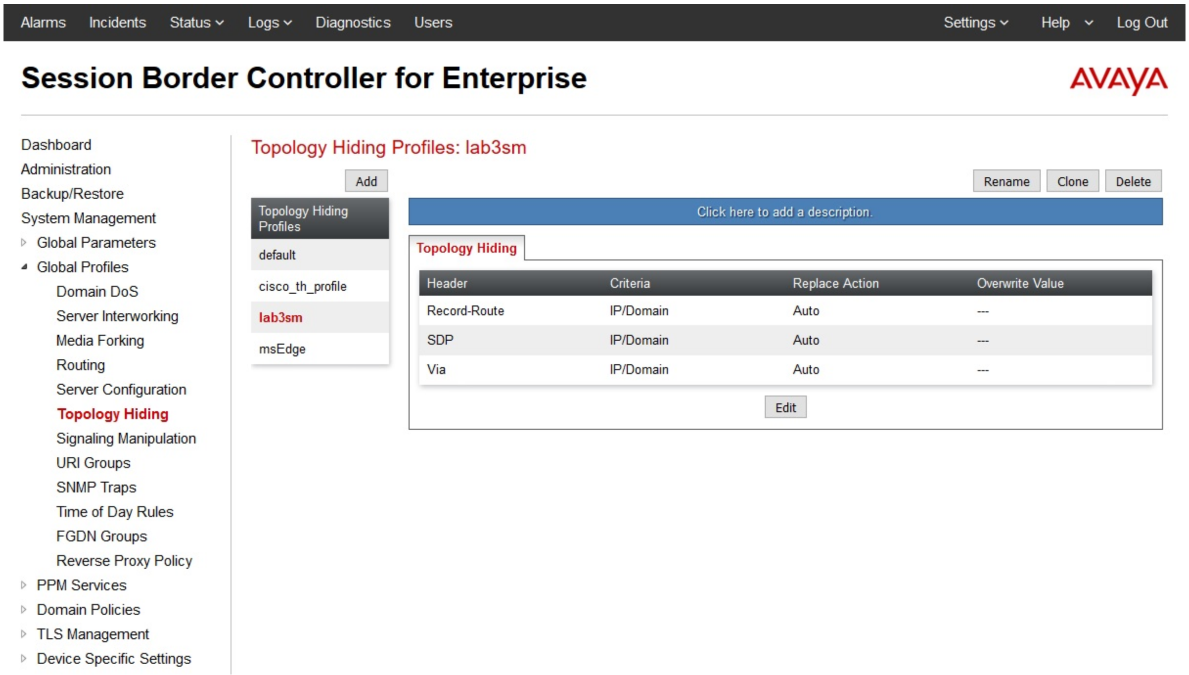
Enabling Internal Topology Hiding

Procedure

1. Repeat the earlier procedure to create a similar Topology Hiding Profile used by the Session Manager.
2. Assign a name to the profile appropriately.

    For example: `lab3sm`.

3. Add the same three headers as in the External Topology Profile.



Topology Hiding Profiles: lab3sm

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

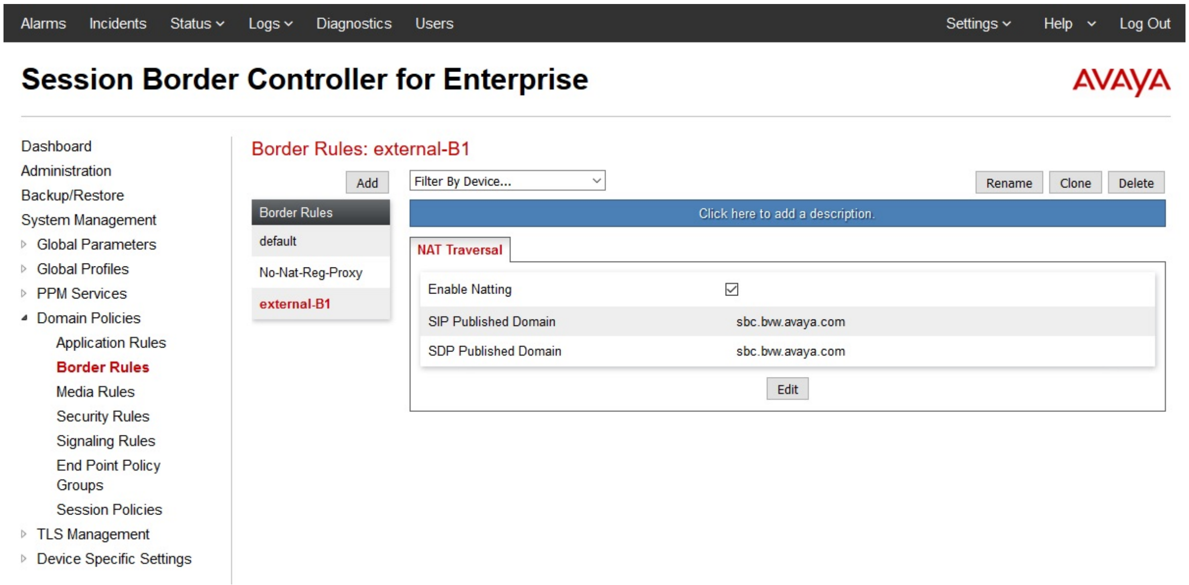
Setting up the Microsoft Edge Border Rule

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Domain Policies** > **Border Rules**.
3. Click **Add** and assign a name the rule.

   For example: `external-B1`.
4. Enable **Natting**.
5. Enable SIP Published IP and set the SIP Published Domain to the FQDN of the Avaya Session Border Controller for Enterprise.

6. Enable SDP Published IP and set the SDP Published Domain to the FQDN of the Avaya Session Border Controller for Enterprise.



Border Rules: external-B1

Enable Natting	☑
SIP Published Domain	sbc.bw.avaya.com
SDP Published Domain	sbc.bw.avaya.com

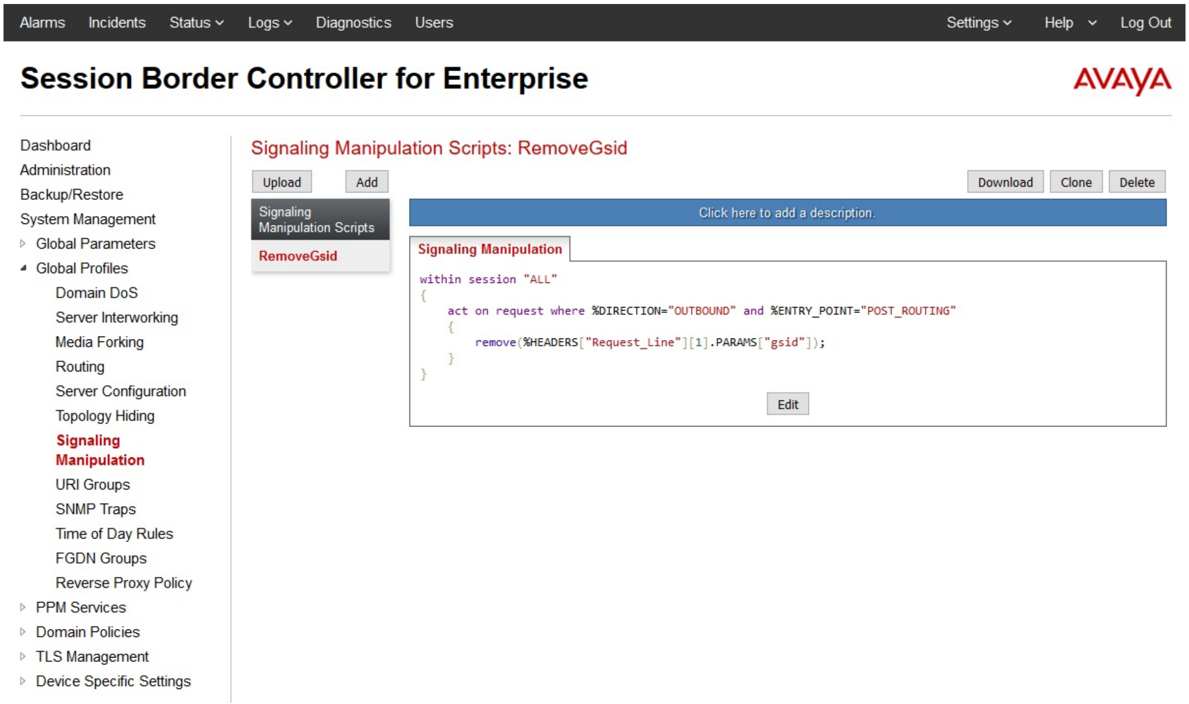
Creating a Signaling Manipulation Script

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Global Profiles** > **Signaling Manipulation**.
3. Click **Add**, set the title to `RemoveGsid` and add the following script:

```
within session "ALL"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        remove(%HEADERS["Request_Line"][1].PARAMS["gsid"]);
    }
}
```

4. Click **Save** to save the script file.



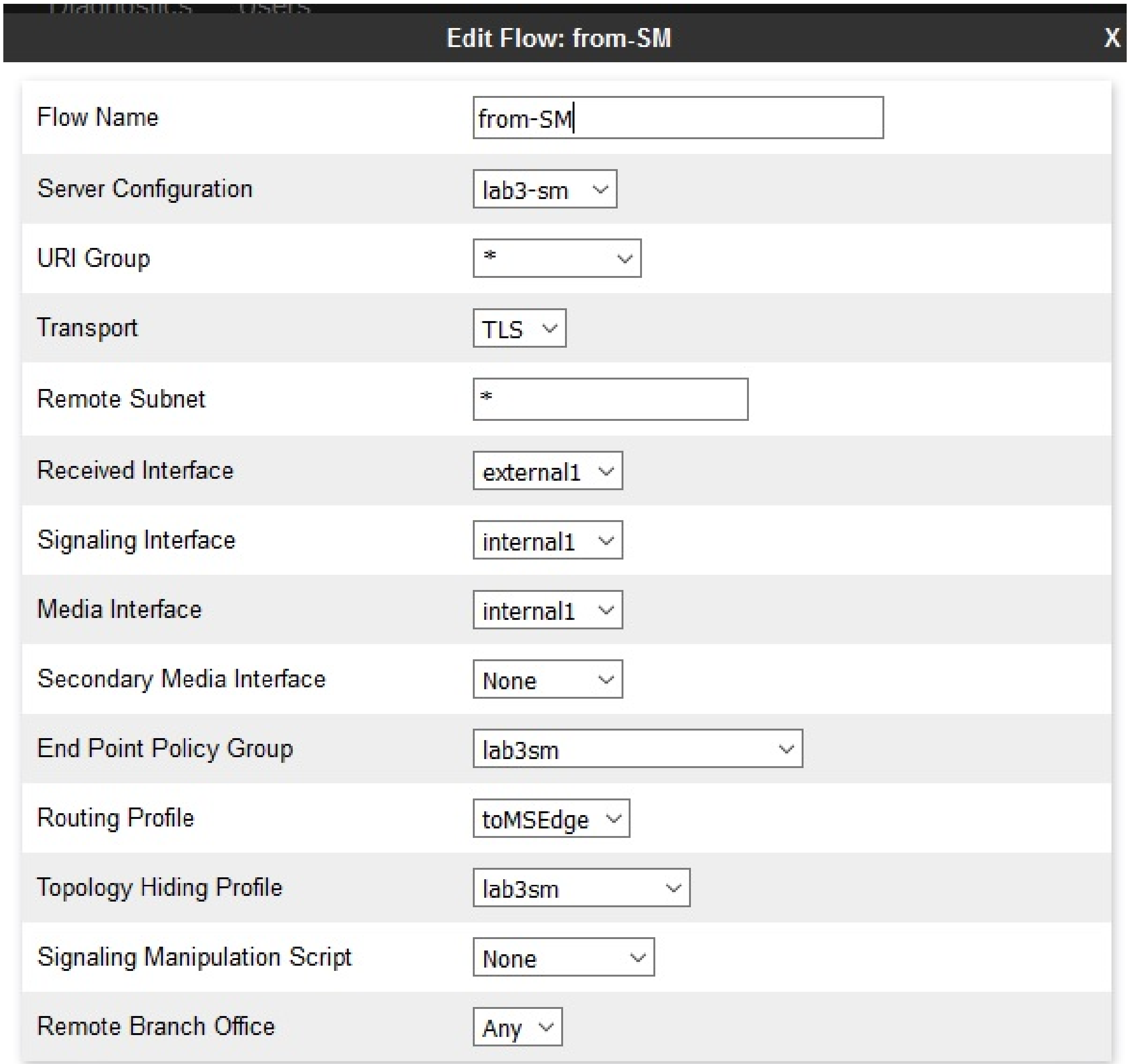
```
within session "ALL"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        remove(%HEADERS["Request_Line"][1].PARAMS["gsid"]);
    }
}
```

Creating End Point Flows

Procedure

1. Log in to the Avaya Session Border Controller for Enterprise server as the administrator.
2. Click **Device Specific Settings** > **End Point Flows** > **Server Flows**.
3. Click **Add** to create the End Point Flow for the Session Manager.
4. Set the name of the flow to `from-SM`.

5. Set up the options and profiles create above as show in the following figure:

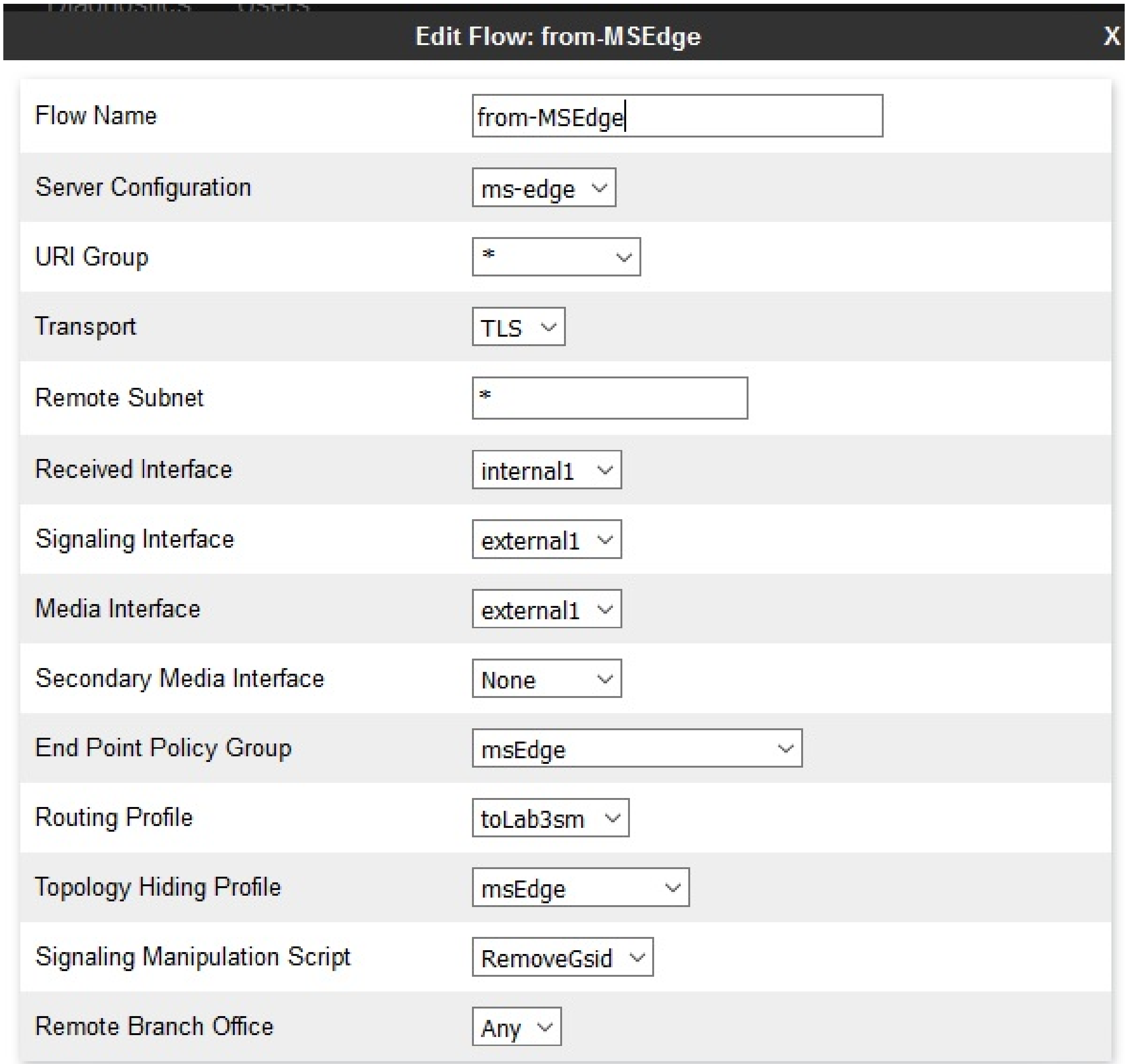


Flow Name	from-SM
Server Configuration	lab3-sm
URI Group	*
Transport	TLS
Remote Subnet	*
Received Interface	external1
Signaling Interface	internal1
Media Interface	internal1
Secondary Media Interface	None
End Point Policy Group	lab3sm
Routing Profile	toMSEdge
Topology Hiding Profile	lab3sm
Signaling Manipulation Script	None
Remote Branch Office	Any

6. Click **Add** to create the End Point Flow for the Microsoft Edge.
7. Set the name of the flow to from-Edge.
8. Setup the options and profiles created above as shown in the following figure:

Note:

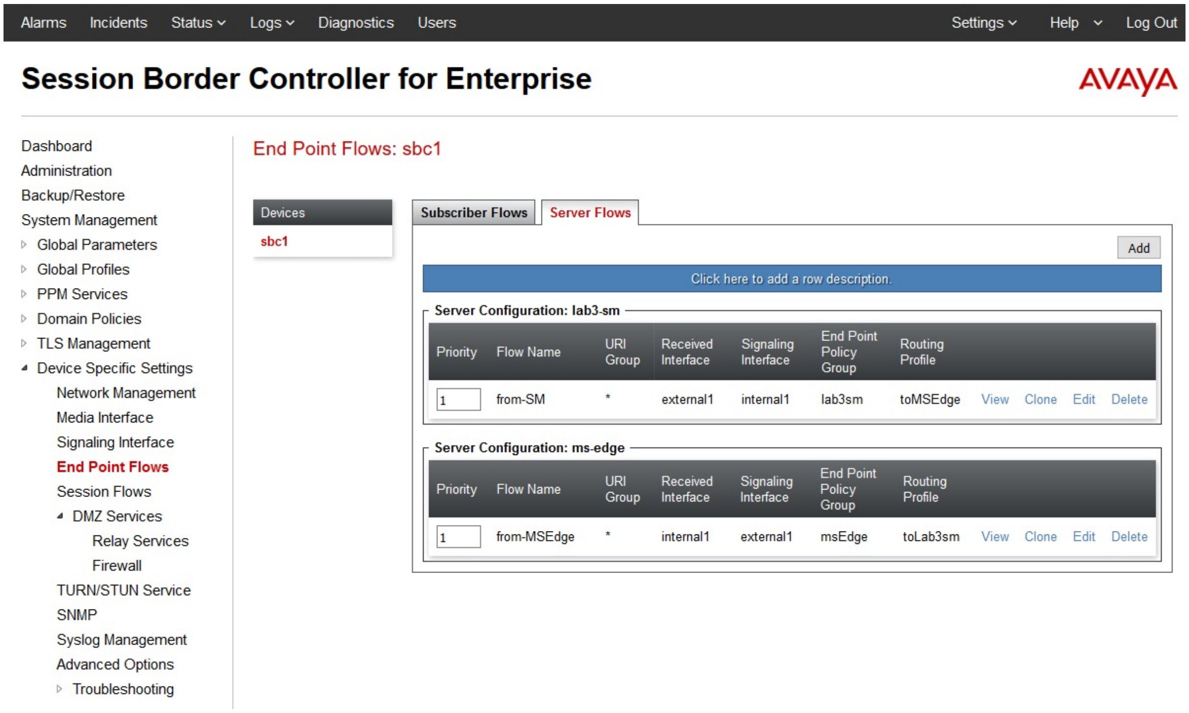
The Edge flow has the **RemoveGsid** Signaling Manipulation Script configured.



Edit Flow: from-MSEdge

Flow Name	from-MSEdge
Server Configuration	ms-edge
URI Group	*
Transport	TLS
Remote Subnet	*
Received Interface	internal1
Signaling Interface	external1
Media Interface	external1
Secondary Media Interface	None
End Point Policy Group	msEdge
Routing Profile	toLab3sm
Topology Hiding Profile	msEdge
Signaling Manipulation Script	RemoveGsid
Remote Branch Office	Any

9. The following shows the two End Point Flows: from-SM and from-MSEdge.



End Point Flows: sbc1

Server Configuration: lab3-sm

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	from-SM	*	external1	internal1	lab3sm	toMSEdge	View	Clone	Edit	Delete

Server Configuration: ms-edge

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	from-MSEdge	*	internal1	external1	msEdge	toLab3sm	View	Clone	Edit	Delete

10.

Microsoft edge server SIP federated domain configuration

A federated domain must be configured on the Microsoft Lync or Skype for Business system to allow signaling messages to be routed to the Avaya Session Border Controller for Enterprise from the Microsoft Edge server.

Configuring the SIP federated domain

Procedure

1. Log in to the Microsoft Front End server as the administrator.

   Note:

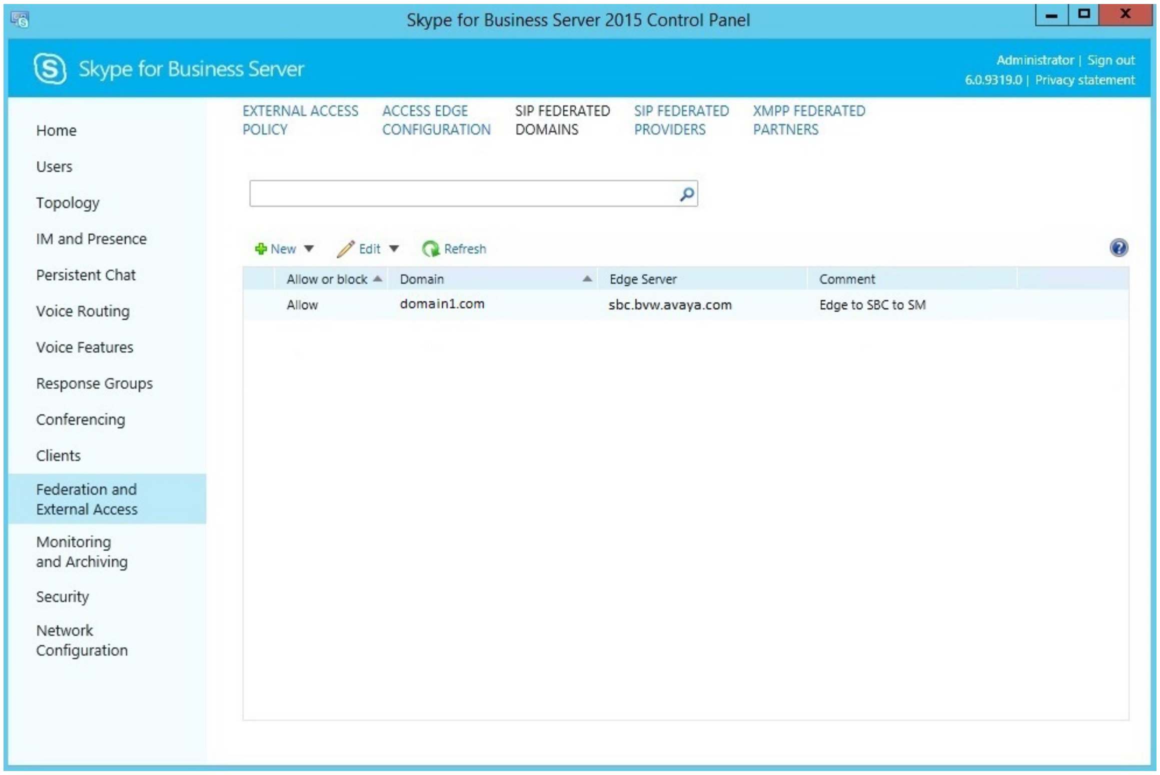
   This administrator user must be part of the CSAdministrator group.

2. Start the Microsoft Lync Server Control Panel or the Skype for Business Server Control Panel application.
3. In the **Federation and External Access** section, select the **SIP Federated Domains** tab.
4. Select **Allowed domain** to add a new domain.
5. In the **Domain name** field, add the Presence or the IM handle domain used by the federated Avaya Aura® users.

For example, if a Microsoft user “ms-user@domain2.com” is federating with an Avaya Aura® user with a presence handle: “aura-user@domain1.com”, then the domain field should contain: “domain1.com”.

6. In the **Access Edge service (FQDN)** field, enter the FQDN of the Avaya Session Border Controller for Enterprise.
7. In the **Comment** field, add an appropriate comment.
8. Click **Commit**.
9. After the commit, ensure that the domain is set to Allow.

Example



Allow or block	Domain	Edge Server	Comment
Allow	domain1.com	sbc.bvw.avaya.com	Edge to SBC to SM

Configuring routing between Session Manager and Avaya Session Border Controller for Enterprise

A federated domain must be configured on the System Manager to allow the Session Manager to route signaling messages from Presence Services to the Microsoft Edge server through the Avaya Session Border Controller for Enterprise.

The following items must be configured on System Manager:

- Certificates
- Entity and Entity Link for the Avaya Session Border Controller for Enterprise with monitoring disabled.
- Session Manager Regular Expression.

- Session Manager Routing Policy.

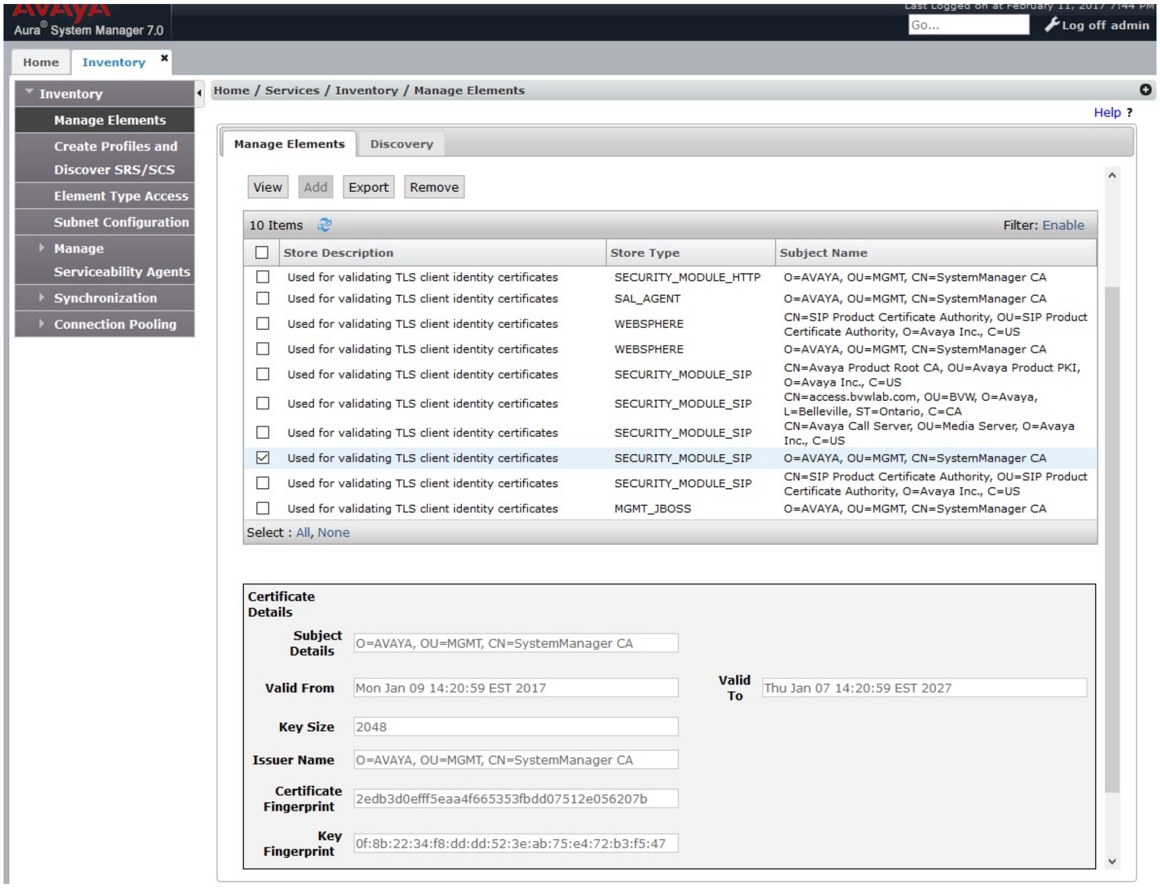
Setting up required certificates for Session Manager

Procedure

1. Log in to the System Manager as the administrator.
2. Select Inventory from the **Services group**, and select **Manage Elements**.
3. Find and select the Session Manager in the list of elements.
4. In the **More Actions** field, select **Configure Trusted Certificates**.
5. The CA certificate that was used to sign the Avaya Session Border Controller for Enterprise identity certificate must be loaded into the SECURITY_MODULE_SIP trust store so that the Session Manager can validate the Avaya Session Border Controller for Enterprise identity certificate.

Example

The System Manager Default CA was used, and is selected in the following example:



10 Items   Filter: Enable

□	Store Description	Store Type	Subject Name
□	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=SystemManager CA
□	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=SystemManager CA
□	Used for validating TLS client identity certificates	WEBSPHERE	CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	WEBSPHERE	O=AVAYA, OU=MGMT, CN=SystemManager CA
□	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=access.bvwlab.com, OU=BVW, O=Avaya, L=Belleville, ST=Ontario, C=CA
□	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
☑	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=SystemManager CA
□	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=SystemManager CA

Select : All, None

Certificate Details

Subject Details: O=AVAYA, OU=MGMT, CN=SystemManager CA

Valid From: Mon Jan 09 14:20:59 EST 2017   Valid To: Thu Jan 07 14:20:59 EST 2027

Key Size: 2048

Issuer Name: O=AVAYA, OU=MGMT, CN=SystemManager CA

Certificate Fingerprint: 2edb3d0efff5eaa4f665353fbdd07512e056207b

Key Fingerprint: 0f:8b:22:34:f8:dd:dd:52:3e:ab:75:e4:72:b3:f5:47

Setting up the Avaya Session Border Controller for Enterprise entity and entity link

Procedure

1. Log in to the System Manager as the administrator.

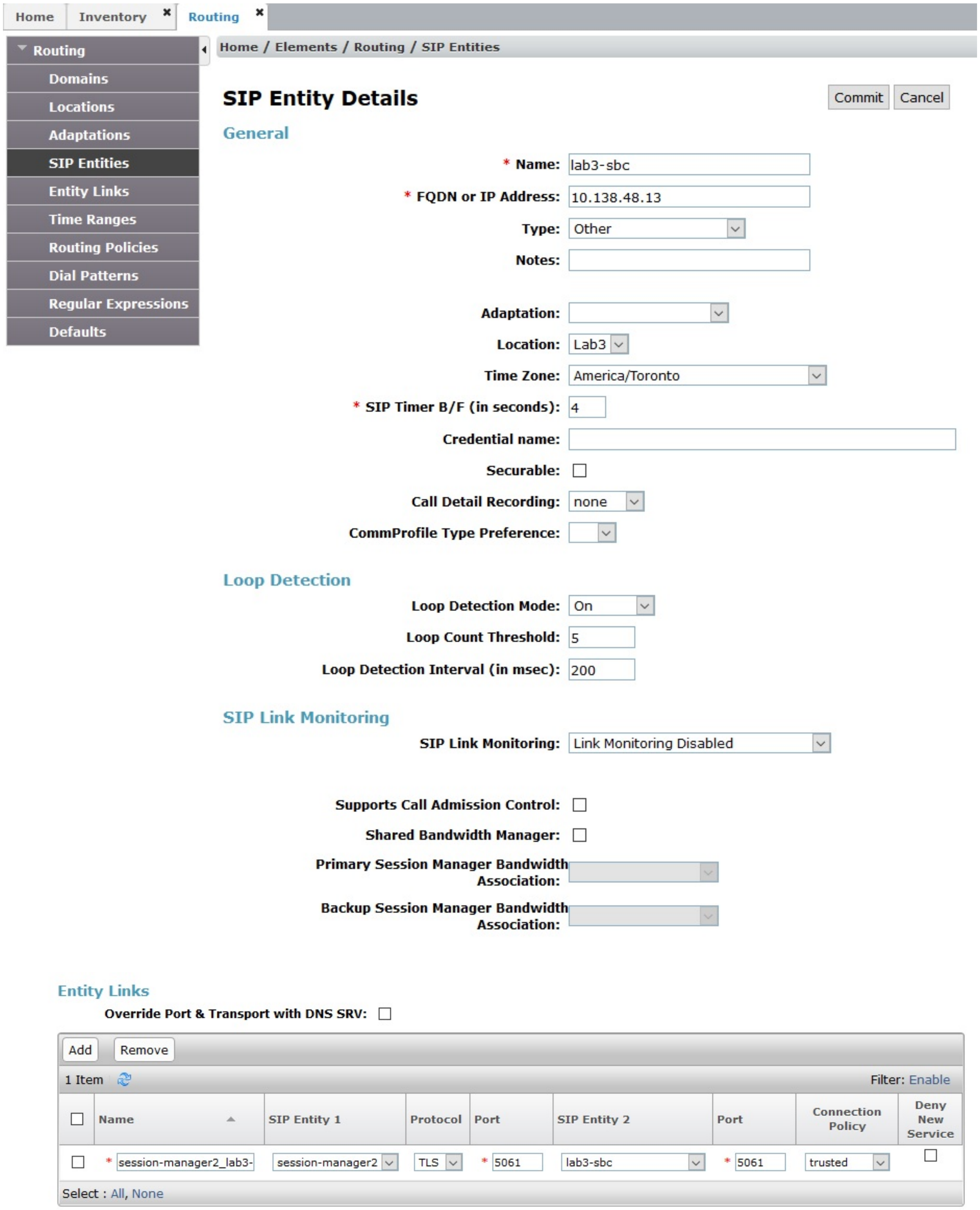
2. Select **Routing** from the **Elements** group, and select SIP Entities.
3. Click **New**, and enter the required data:
    a. The name of the Avaya Session Border Controller for Enterprise server.
    b. The IP address or Fully qualified domain name (FQDN) of the Avaya Session Border Controller for Enterprise internal interface, that is on the internal domain or network. If a FQDN is used, it must be resolvable by the Session Manager.
    c. Set the **Type** to Other.
    d. Set the **Location** and **Time zone**.
    e. **Loop detection** can be left enabled.
    f. **SIP link monitor** must be disabled.

        Note:

        If the Avaya Session Border Controller for Enterprise is configured to respond to the OPTIONS SIP message properly, the **link monitor** can be enabled. But by default the Avaya Session Border Controller for Enterprise will pass the OPTIONS message through to the Microsoft Edge, which will not respond.

    g. All other fields can be left as default.
    h. Create an entity link to the Session Manager using TLS, 5061, and policy trusted for the newly created entity.
4. Click **Commit** to create the entity and the entity link.

Example



Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: lab3-sbc

* FQDN or IP Address: 10.138.48.13

Type: Other

Notes:

Adaptation:

Location: Lab3

Time Zone: America/Toronto

* SIP Timer B/F (in seconds): 4

Credential name:

Securable: □

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

Supports Call Admission Control: □

Shared Bandwidth Manager: □

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: □

1 Item Filter: Enable

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* session-manager2_lab3-	session-manager2	TLS	* 5061	lab3-sbc	* 5061	trusted	□

Select : All, None

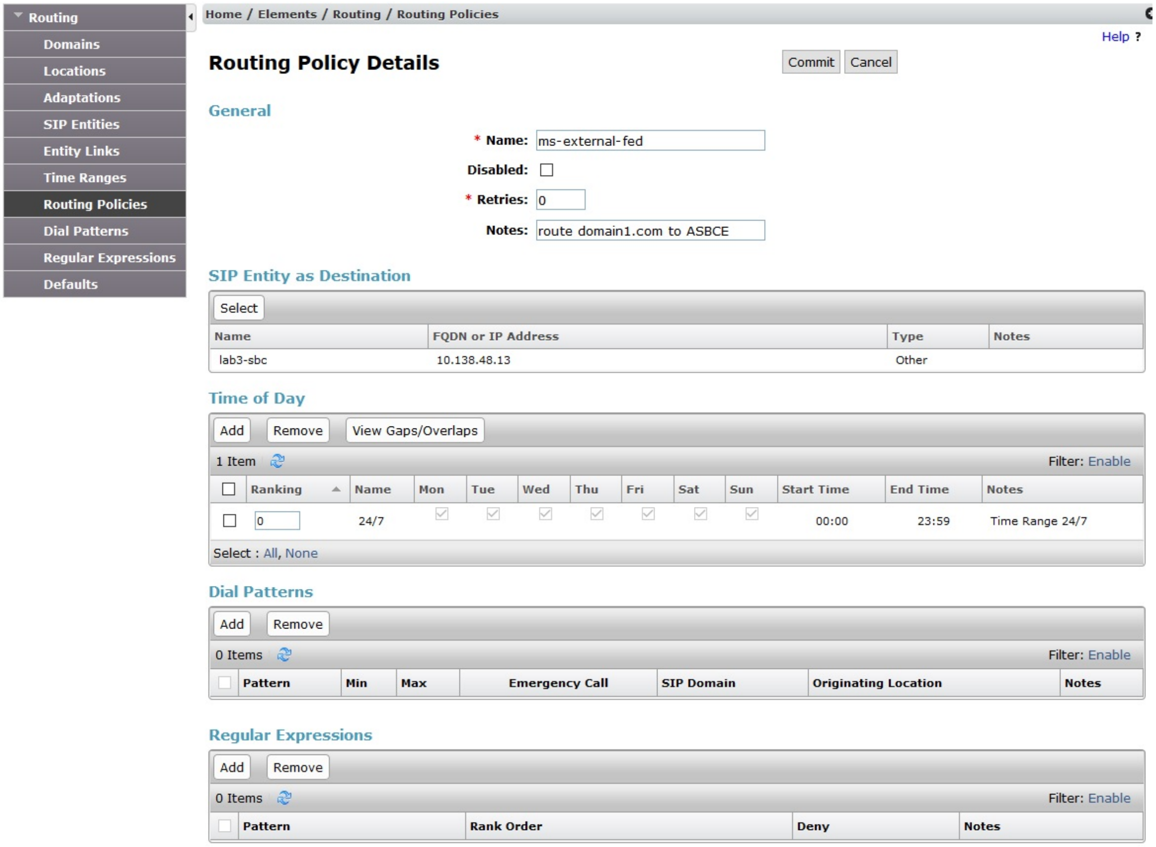
Setting up the Session Manager routing policy

Procedure

1. Log in to the System Manager as the administrator.

2. Select Routing from the **Elements** group, and select Routing Policies.
3. Click **New**, and enter the required data.
    a. Enter a name, for example “ms-external-federation”.
    b. Clear the disabled box.
    c. Set retries to `0`.
    d. Enter relevant notes.
    e. Select the destination SIP entity created earlier.
    f. Time of Day, Dial Patterns and Regular Expressions can be left in their default states.
4. Click **Commit** to create the routing policy.

Example



Routing Policy Details

General

* Name: ms-external-fed

Disabled: ☐

* Retries: 0

Notes: route domain1.com to ASBCE

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
lab3-sbc	10.138.48.13	Other	

Time of Day

Add | Remove | View Gaps/Overlaps

1 Item — Filter: Enable

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add | Remove

0 Items — Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Regular Expressions

Add | Remove

0 Items — Filter: Enable

☐	Pattern	Rank Order	Deny	Notes

Setting up the Session Manager regular expression

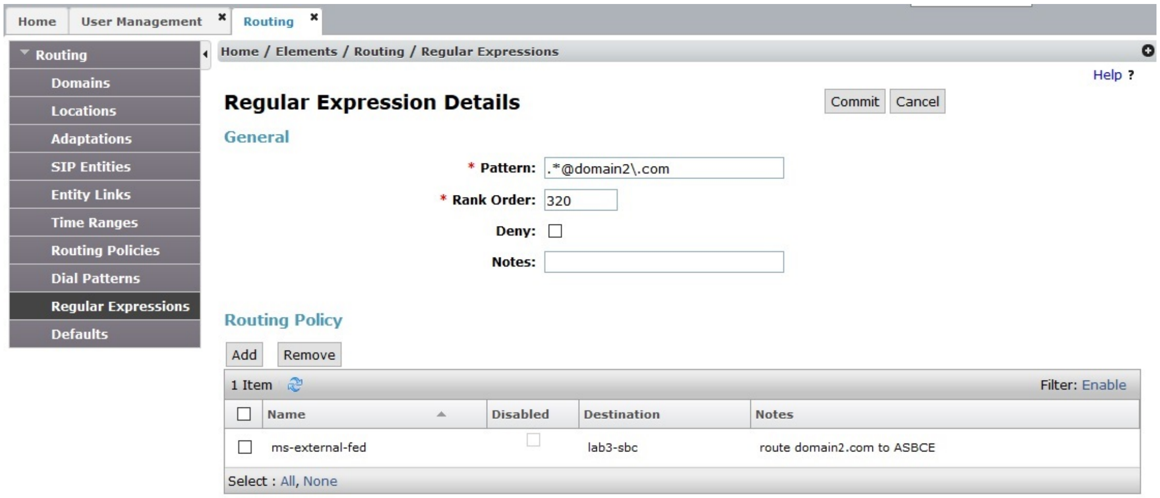
Procedure

1. Log in to the System Manager as the administrator.
2. Select Routing from the **Elements** group, and select Regular Expressions.

3. Click **New**, and enter the required data.
    a. The pattern is specified to match any user in the Microsoft domain that the Avaya Aura® users will federate with.

       For example, if a Microsoft user "ms-user@domain2.com" is federating with an Avaya Aura® user with a presence handle "aura-user@domain1.com", then the pattern should be: ".*@domain2\.com" .
    b. The **rank order** can be `0` or some other appropriate number.
    c. **Deny** should be cleared.
    d. In **Routing Policy**, click **Add** and select the policy created in the earlier procedure.
4. Click **Commit** to create the regular expression.

Example



Regular Expression Details

General

* Pattern: .*@domain2\.com

* Rank Order: 320

Deny: □

Notes:

Routing Policy

1 Item

□	Name	Disabled	Destination	Notes
□	ms-external-fed	□	lab3-sbc	route domain2.com to ASBCE

Presence Services Microsoft federation attributes configuration

The Microsoft external federated domain must be configured in the Presence Services cluster attributes on the System Manager to allow the System Manager to route signaling messages to the Microsoft Edge server through the Session Manager and Avaya Session Border Controller for Enterprise.

Setting up cluster attributes for external domain Microsoft federation

Procedure

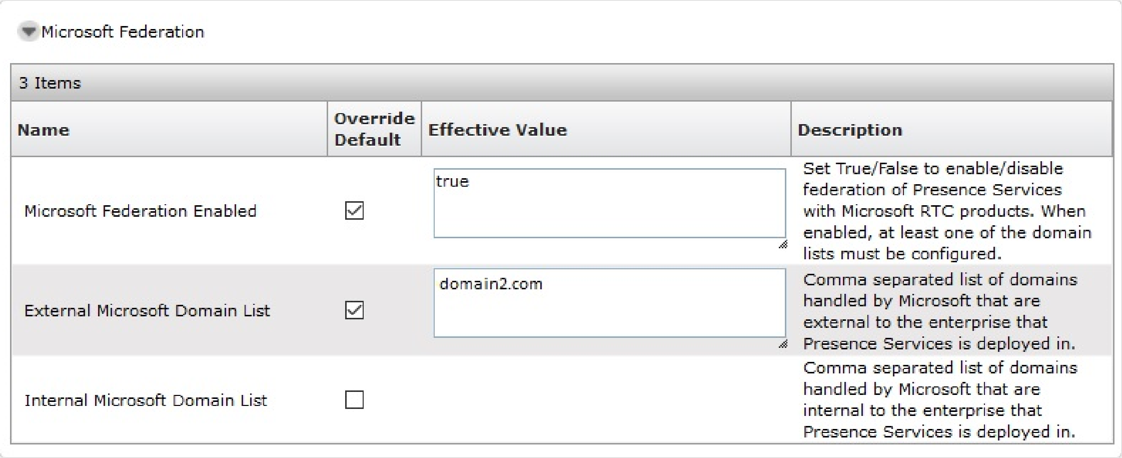
1. Log in to the System Manager as the administrator.
2. Select Avaya Breeze™ from the **Elements** group.
3. Click **Configuration**.
4. Click **Attributes**, and select the Service Clusters tab.
5. Select the System Manager cluster and installed Presence Services snap-in.

6. Scroll down to the **Microsoft Federation** section, and set the following:
    a. Check the **Override Default for the Microsoft Federation Enabled** field and set the effective value to True.
    b. Check the **Override Default for the External Microsoft Domain List** and enter the Microsoft user domain.

       For example, “domain2.com” as used in the earlier examples.
7. Click **Commit** to save the configuration changes.

   Note:

   For the External Domain Federation to work properly the Microsoft domain configured in this procedure must be different than any of the Presence or IM domains in use by Presence Services users.



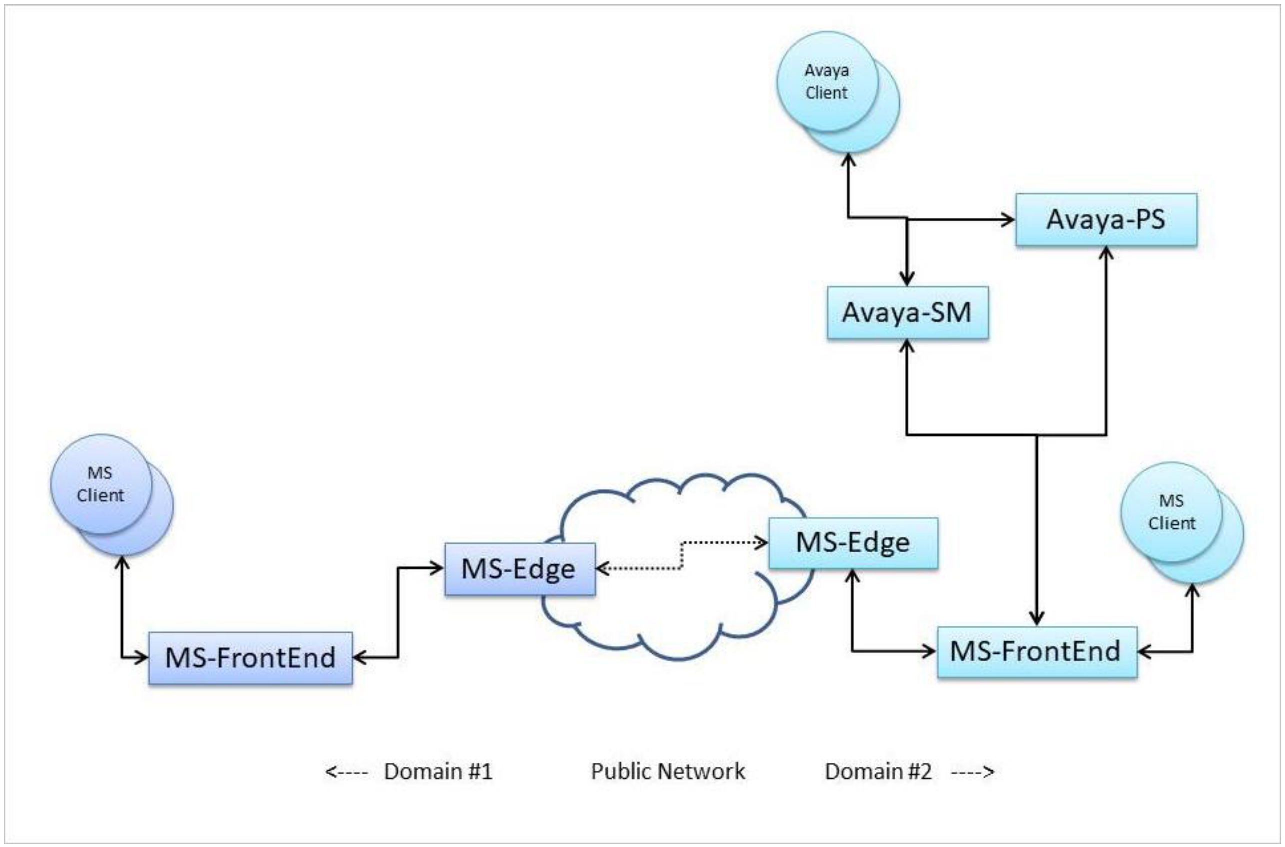
Microsoft Federation

3 Items

Name	Override Default	Effective Value	Description
Microsoft Federation Enabled	☑	true	Set True/False to enable/disable federation of Presence Services with Microsoft RTC products. When enabled, at least one of the domain lists must be configured.
External Microsoft Domain List	☑	domain2.com	Comma separated list of domains handled by Microsoft that are external to the enterprise that Presence Services is deployed in.
Internal Microsoft Domain List	☐		Comma separated list of domains handled by Microsoft that are internal to the enterprise that Presence Services is deployed in.

Microsoft federation with internal Avaya Aura domain and external Microsoft domain

The following diagram illustrates the message flow and server connections of the different components. In this deployment, it is possible for Microsoft clients in domain #1 to federate with both Microsoft and Avaya Aura clients in domain #2. Similarly, it is possible for both Microsoft and Avaya Aura clients in domain #2 to federate with Microsoft clients in domain #1. If Avaya Aura clients are federated with Microsoft clients in domain #1, the messages tandem through the Microsoft system in domain #2.



Checklist for configuring Microsoft federation with internal Avaya Aura domain and external Microsoft domain

No.	Task	Reference	✔
1	Configure Microsoft external domain federation between the Microsoft systems in domain #1 and domain #2. As a result of this setup, Microsoft clients in domain #1 must be able to federate with Microsoft clients in domain #2, and Microsoft clients in domain #2 must be able to federate with Microsoft clients in domain #1.	See Microsoft documentation as this is a standard Microsoft configuration.	
2	Configure Microsoft Real Time Communication (RTC) Federation between the Microsoft system in domain #2 and the Avaya Aura Presence Services system in domain #2. As a result of this configuration, Microsoft clients in domain #2 must be able to federate with Avaya Aura clients in domain #2, and Avaya Aura clients in domain #2 must be able to federate with Microsoft clients in domain #2.	Microsoft Real Time Communication (RTC) Federation on page 83	

Table continues…

No.	Task	Reference	✔
3	Configure Avaya Presence Services attributes to enable the tandem domain support. As a result of this configuration, Microsoft clients in domain #1 will be able to federate with Avaya Aura clients in domain #2, and Avaya Aura clients in domain #2 will be able to federate with Microsoft clients in domain #1.	Configure Avaya Aura Presence Services attributes to enable tandem domain support on page 140	

Configuring Presence Services attributes to enable tandem domain support

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze**.
2. In the navigation pane, click **Configuration > Attributes**.
3. Click the **Service Clusters** tab or **Service Globals** tab.
    - If Microsoft federation only applies to one Breeze Cluster, you should use the **Service Clusters** tab for the Attribute setting.
    - If the configuration is for all the Breeze Clusters, select the **Service Globals** tab option.
4. In the **Service** field, select the PresenceServices snap-in service.

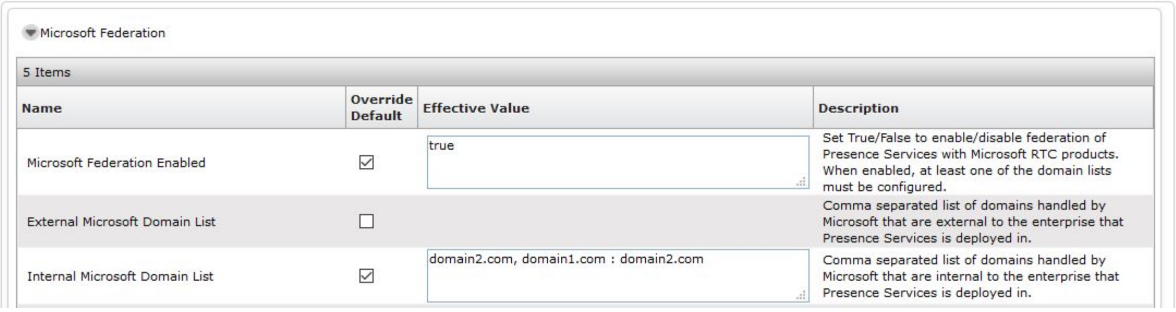
    The table displays the attributes that you can configure for the service, including a description of each attribute.
5. In the **Microsoft Federation** section, do the following:
    a. Microsoft Federation Enabled: Select the **Override Default** check box, and enter `True` in the **Effective Value** field.

    b. Internal Microsoft Domain List: Select the **Override Default** check box, and enter the list of Microsoft domain names, comma separated if there are multiple Microsoft domains.

    The syntax for configuring a tandem domain is: **`“target-domain-name : tandem-domain-name”`**.
6. Click **Commit**.

    The following diagram shows the “Internal Microsoft Domain List” to be domain2.com, and domain1.com:domain2.com. This is the correct configuration for the diagram shown in the *Microsoft federation with internal Avaya Aura domain and external Microsoft domain* section.

    The first entry “domain2.com” is used to federate in domain #2 between Microsoft and Avaya Aura users. The second entry “domain1.com : domain2.com” is used to federate between Microsoft users in domain #1 and the Avaya Aura users in domain #2. This configuration instructs Presence Services to use domain2.com as a tandem to reach Microsoft users in domain1.com.



▾ Microsoft Federation

5 Items

Name	Override Default	Effective Value	Description
Microsoft Federation Enabled	☑	true	Set True/False to enable/disable federation of Presence Services with Microsoft RTC products. When enabled, at least one of the domain lists must be configured.
External Microsoft Domain List	☐		Comma separated list of domains handled by Microsoft that are external to the enterprise that Presence Services is deployed in.
Internal Microsoft Domain List	☑	domain2.com, domain1.com : domain2.com	Comma separated list of domains handled by Microsoft that are internal to the enterprise that Presence Services is deployed in.

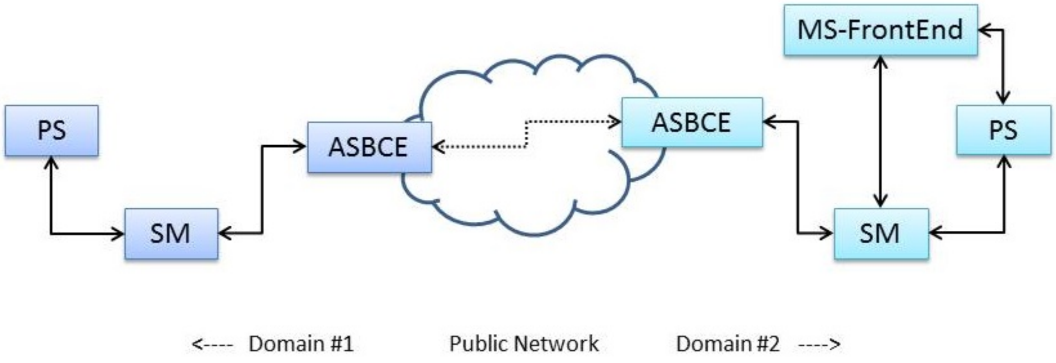
Microsoft federation with internal and external domains using inter-PS federation

The following diagram illustrates the message flow and server connections of the different components required to deploy Internal domain federation combined with Inter-PS federation.

Avaya Aura® users in domain 1 can watch Microsoft users in domain 2 using the Presence Services in domain 2 as a tandem server. Avaya Aura® users in domain 1 can also watch Avaya Aura® users in domain 2 using Inter-PS federation.

Similarly Microsoft users in domain 2 can watch Avaya Aura® users in the external domain 1 via the tandem Presence Services in domain 2. They can also watch Avaya Aura® users in domain 2 using Microsoft Internal Domain federation.

Using the concepts and configuration details described below, the Microsoft Front End server could be deployed in either domain, or one in each domain. For simplicity, the steps will cover a Front End server deployed only in domain 2.



Checklist for configuring Microsoft federation with internal and external domains using Inter-PS federation

No.	Task	Link	✔
Domain 1 configuration			
1	Configure Inter-PS Federation to domain 2.	Configuring inter-PS federation to domain 2 on page 143	
2	Configure Session Manager routing policies and regular expression to Avaya SBCE for domain 1.	Configuring Session Manager routing policies and regular expression to Avaya SBCE for domain 1 on page 143	
Domain 2 configuration			
1	Configure Microsoft Internal domain federation.	Configuring Microsoft internal domain federation on page 144	
2	Configure Microsoft trusted application.	Configuring Microsoft trusted application on page 144	
3	Configure Microsoft trusted application pool.	Configuring Microsoft trusted application pool on page 144	
4	Configure Microsoft front end static routing.	Configuring Microsoft front end static routing on page 144	
5	Configure Inter-PS federation to domain 1.	Configuring inter-PS federation to domain 1 on page 145	
6	Configure Session Manager routing policies and regular expressions to Avaya SBCE for domain 2.	Configuring Session Manager routing policies and regular expressions to Avaya SBCEfor domain 2 on page 145	

Domain 1 configuration

TheAvaya Aura® system in domain 1 is configured to use Inter-PS federation to allow its users to watch Avaya Aura® and Microsoft users in domain 2. Signaling for Avaya Aura® users watching Microsoft users in domain 2 is tandemed through the Presence Services in domain 2. All signaling is routed through Avaya Session Border Controller for Enterprise at the edges of each domain. Use of Avaya Session Border Controller for Enterprise is optional, since no message manipulation is required, but recommended to protect each domain from the public network.

Since both Avaya Aura® and Microsoft users are in the same external domain that is, domain 2, a single set of configuration rules routing to that domain are required. Refer to the section describing

“Configuring federation between two Presence Services clusters on different System Manager” for more detail.

Configuring inter-PS federation to domain 2

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** .
2. Click **Configuration** > **Attributes**.
3. Select the appropriate cluster and Presence Services snap-in.
4. In the **Inter-PS Federation** group, enable the feature, and add Domain 2 to the Inter-PS Domain name list.

Configuring Session Manager routing policies and regular expression to Avaya SBCE for domain 1

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing**.
2. Create a new regular expression and routing policy to route the Inter-PS messages to either the local Avaya Aura® Session Border Controller in domain 1 or the remote Session Manager in domain 2. The routing policy must have either the local Avaya SBCE or the remote Session Manager as its destination SIP Entity.
3. Ensure that the regular expression contains a generic user and domain regular expression that identifies the users in domain 2. For example, “.*@domain2\.com”.

Domain 2 configuration

The Avaya Aura® system in domain 2 is configured to use Inter-PS federation to enable users and the Microsoft users to watch Avaya Aura® users in domain 1. Signaling for Microsoft users watching Avaya Aura® users in domain 1 is tandemed through the Presence Services in domain 2. All signaling is routing through Avaya Aura® Session Border Controller at the edges of each domain. Use of Avaya Aura® Session Border Controller is optional, since no message manipulation is required, but recommended to protect each domain from the public network

Following are the sets of routing configuration required:

1. Inter-PS federation between the domain 1 and domain 2. For more information, see “Configuring federation between two Presence Services clusters on different System Manager”.
2. Microsoft internal domain federation within domain 2 between the Avaya Aura® and Microsoft systems. For more information, see “Microsoft RTC Federation”.
3. Additional Session Manager routing configuration required to force Microsoft internal federation signaling into Presence Services in domain 2. For more information, see “Configuring Microsoft Internal Domain Federation”.

Configuring Microsoft internal domain federation

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** .
2. Click **Configuration** > **Attributes**.
3. Select the appropriate cluster and Presence Services snap-in.
4. In the Microsoft Federation group, enable the feature, and add the Microsoft domain to the Internal Microsoft Domain List.

Configuring Microsoft trusted application pool

Procedure

1. On the Microsoft front end server, use the `New-CsTrustedApplicationPool` cmdlet to create the application pool.
2. Select one of the Presence Services cluster nodes as the ComputerFqdn.
3. Add all additional Presence Services cluster nodes into the pool using the `New-CsTrustedApplicationComputer` cmdlet specifying each Presence Services node and pool created earlier. For more information, see ,"Configure Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route".

Configuring Microsoft trusted application

Procedure

On the Microsoft Front End server, use the `New-CsTrustedApplication` cmdlet to create the trusted application specifying an application identity and the trusted pool created earlier. For more information, see "Configure Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route".

Configuring Microsoft front end static routing

Procedure

1. On the Microsoft Front End server, use the `New-CsStaticRoute` and `Set-CsStaticRoutingConfiguration` cmdlets to create a static route. The static route will route signaling from the Microsoft Front End to the Domain 2 Presence Services federation relay component by specifying the trust application pool identifier, the internal domain (Domain 2) and port `5063`.
2. Create a second static route that will route signaling from the Microsoft Front End to the Domain 2 Presence Services federation relay component by specifying the same trusted application pool identifier, the external domain (Domain 1) and port `5063`. The Domain 2 Presence Services will forward the signaling to the Domain 1 Presence Services through Inter-PS federation. For more information, see "Configure Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route".

Configuring inter-PS federation to domain 1

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** .
2. Click **Configuration** > **Attributes**.
3. Select the appropriate cluster and Presence Services snap-in.
4. In the **Inter-PS Federation** group, enable the feature, and add Domain 1 to the Inter-PS Domain name list.

Configuring Session Manager routing policies and regular expressions to Avaya SBCEfor domain 2

Procedure

1. On the System Manager web console, navigate to **Elements** > **Routing.** Create a new regular expression and routing policy to route the Inter-PS messages to either the local Avaya Aura® Session Border Controller in domain 2 or the remote Session Manager in domain 1..

   Ensure that the routing policy has either the local Avaya Session Border Controller for Enterprise or the remote Session Manager as its destination SIP Entity.

   Ensure that the regular expression contains a generic user and domain regular expression that identifies the users in domain 1 with an additional special parameter. For example, “.*@domain1\.com.*av-ps-ps-fed.*”.

2. Create a second routing policy with three Regular Expressions.

   One to route the tandem Inter-PS signaling from Domain 1 into the Domain 2 Presence Services to be forwarded to the Microsoft Front End. The second and third Regular Expressions to route the tandem presence and IM signaling from the Microsoft Front End into the local Presence Services cluster in Domain 2.

   a. Ensure that the routing policy has the local Presence Services cluster as its destination SIP Entity.

      This SIP Entity is of type Presence Services that represents the Presence Services cluster.

   b. Ensure that the first Regular Expression contains a generic user and domain Regular Expression that identifies the users in domain 2, either Avaya Aura or Microsoft users, with an additional special parameter.

      This will route Inter-PS signaling from domain 1 into the Presence Services in domain 2. For example: `.*@domain2\.com.*av-ps-ps-fed.*`

   c. Ensure that the second and third Regular Expressions contains a generic user and domain Regular Expression that identifies the Aura users in domain 1 with additional special parameters.

      One regular expression to route Microsoft federation presence signaling into the Domain 2 Presence Services to be forwarded through Inter-PS federation to Domain

1. For example: `.*@domain1\.com.*av-msfe-ps-fed.*`. The second Regular Expression to route Microsoft federation IM signaling into the domain 2 Presence Services to be forwarded through Inter-PS federation to domain 1. For example: `.*@domain1\.com.*av-msfe-imgw-fed.*`. The separation of presence and IM signaling is to allow for deployments with AMM.

3. For Presence Services and Microsoft federation deployments that include AMM, a third routing policy is required to route tandem IM signaling from the Microsoft Front End into the local AMM server in Domain 2 instead of Presence Services.

   a. Create a third routing policy with one Regular Expression to route the tandem IM signaling from the Microsoft Front End into the local AMM server in Domain 2.

   b. Ensure that the routing policy has the local AMM server as its destination SIP Entity.

   c. Ensure the Regular Expression contains a generic user and domain that identifies the Aura users in domain 1 with an additional special parameter.

      For example: `.*@domain1\.com.*av-msfe-imgw-fed.*`

   The AMM Lync Adaptation Module functionality has been included in the Presence Services Federation Relay component. When AMM is deployed with Presence Services and the Federation Relay is used for Microsoft RTC internal domain federation, the AMM Lync Adapter is not longer required, and need not be installed into the Session Manager.

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 8: 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 148	
2	Configure the Session Manager routing for both the System Managers.	Configuring the Session Manager routing on page 149	
3	Assign communication profile to users.	Assigning Avaya Presence/IM communication address to user on System Manager on page 147	
4	Downloading certificate from the first System Manager instance.	Downloading certificate from System Manager on page 149	
5	Adding certificate to Session Manager on the second System Manager instance.	Adding certificate to Session Manager on page 150	
6	Downloading certificate from the second System Manager instance.	Downloading certificate from System Manager on page 149	
7	Adding certificate to Session Manager on the first System Manager instance.	Adding certificate to Session Manager on page 150	

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

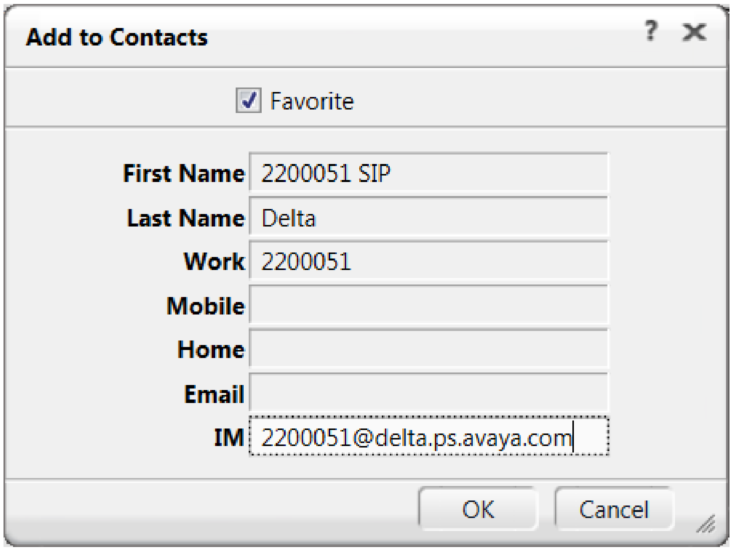
1. Navigate to **Services** > **Inventory** > **Manage Elements**.
2. Select the Session Manager instance and click **More Actions** > **Configure Trusted Certificates**.
3. Click **Add**.
4. Select **Import from file** and import the PEM file downloaded in “Downloading certificate from System Manager”.
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.

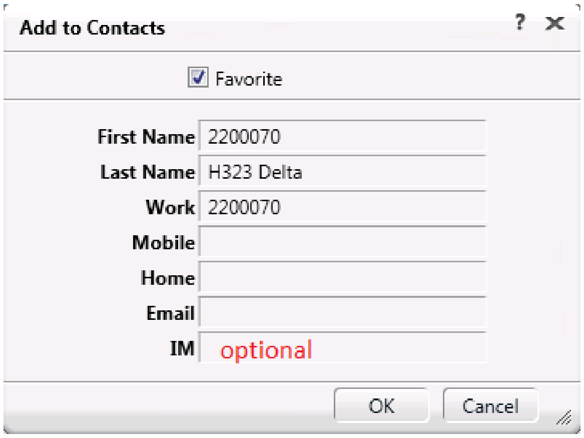
H323 watcher of a federated presentity:



☑ Favorite

First Name	2200051 SIP
Last Name	Delta
Work	2200051
Mobile	
Home	
Email	
IM	2200051@delta.ps.avaya.com

SIP watcher of a federated presentity:



Add to Contacts

☑ Favorite

First Name 2200070

Last Name H323 Delta

Work 2200070

Mobile

Home

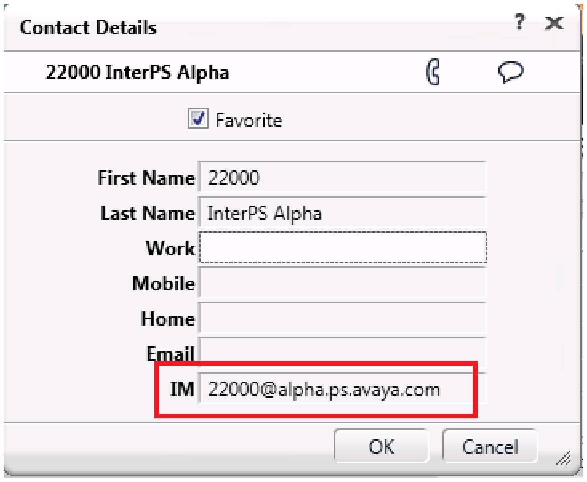
Email

IM optional

Presence Services clusters on different System Managers

A federated contact is added like an external contact.

H323 or SIP watcher of a federated presentity:



Contact Details

22000 InterPS Alpha

☑ Favorite

First Name 22000

Last Name InterPS Alpha

Work

Mobile

Home

Email

IM 22000@alpha.ps.avaya.com

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 uses XMPP to federate with the following types of remote deployments:

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

- Any standard XMPP server

Ignite Realtime Openfire, Cisco Jabber, and UC Federation-NextPlane 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 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 9: Single-server Cluster Federated with Ignite Openfire example values”. The **Sample value** column is based on the following example:

- Presence Services 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 9: 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 10: 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 160	
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 162	
3	Administer XMPP federation in unsecure mode (TCP).	Administering XMPP federation in unsecure mode (TCP) on page 158	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 155	
5	Administer Security Settings (TCP) in Openfire.	Administering Security Settings (TCP) on Openfire on page 155	
6	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 163	

Table 11: 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 160	
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 162	
3	Administer XMPP federation in secure mode (TLS).	Administering XMPP federation in secure mode (TLS) on page 159	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 155	
5	Administer Security Settings TLS on Openfire.	Administering Security Settings TLS on Openfire on page 156	

Table continues…

No.	Task	Reference	✔
6	Administer Disable Certificate Verification in Openfire.	Administering Disable Certificate Verification on Openfire on page 157	
7	Export Openfire Certificate on Linux.	Exporting Openfire Certificate (Linux) on page 236	
8	Export Openfire Certificate on Windows.	Exporting Openfire Certificate (Windows) on page 237	
9	Import Certificate into Cluster Truststore.	Importing certificate into Cluster Truststore on page 237	
10	Import System Manager root CA certificate into Openfire Truststore on Windows.	Importing System Manager root CA certificate into Openfire Truststore (Windows) on page 238	
11	Import System Manager root CA certificate into Openfire Truststore on Linux.	Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store on page 239	
12	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 163	

Table 12: 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 160	
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 162	
3	Administer XMPP federation in secure mode (TLS).	Administering XMPP federation in secure mode (TLS) on page 159	
4	Administer Server to Server Settings in Openfire.	Administering Server to Server Settings on Openfire on page 155	
5	Administering Security Settings TLS on Openfire.	Administering Security Settings TLS on Openfire on page 156	
6	Administer Disable Certificate Verification in Openfire.	Administering Disable Certificate Verification on Openfire on page 157	
7	Create Entity Profile on System Manager.	Creating Entity Profile on System Manager on page 239	

Table continues…

No.	Task	Reference	✔
8	Generate a Certificate Signing Request (CSR) on Openfire.	Generating a certificate signing request on the Openfire server on page 240	
9	Sign the Openfire CSR on System Manager.	Signing the Openfire certificate signing request (CSR) on System Manager on page 241	
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 241	
11	Verify DNS resolution and server reachability.	Verifying DNS resolution and server reachability on page 163	

Administering Server to Server Settings on Openfire

About this task

This procedure uses the samples values in the “Table 9: 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

About this task

Use this procedure to modify the Openfire server settings for TCP connections. The procedures are different depending on the version of Openfire installed. For more details, refer to Openfire documentation.

Procedure

1. For Openfire 3.x:

   a. Navigate to **Server** > **Server Settings** > **Security Settings**.

   b. In **Server Connection Security**, configure the Openfire server to use TCP:

   a. 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.

   c. Click **Save Settings**.

2. For Openfire 4.x:

   a. Navigate to **Server** > **Server Settings** > **Server to Server Settings**.

   b. In the **Plain-text (with STARTTLS) connections** section, click **Advanced Configuration**.

   c. In **TCP Settings**, select **Enabled** and enter Port 5269.

   d. In **STARTTLS policy**, select **Disabled**.

   e. Click **Save Settings**.

Administering Security Settings TLS on Openfire

About this task

Use this procedure to modify the Openfire server settings for TLS connections. The procedures are different depending on the version of Openfire installed. For more details, refer to Openfire documentation.

Procedure

1. For Openfire 3.x:

   a. On the Openfire server, navigate to **Server** > **Server Settings** > **Security Settings**.

   b. 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.

   c. Click **Save Settings**.

2. For Openfire 4.x:

   a. Navigate to **Server** > **Server Settings** > **Server to Server Settings**.

   b. In the **Plain-text (with STARTTLS) connections** section, click **Advanced Configuration**.

c. In **TCP Settings**, select **Enabled** and enter Port 5269.

d. In **STARTTLS policy**, select **Required**.

e. In **Mutual Authentication**, select **Needed** if the Presence Services certificate contains a subject alternative name (SAN) of the OtherName type with an XMPPaddr identifier. Otherwise, select **Disabled**.

f. In **Certificate chain checking**, select **Allow peer certificates to be self-signed** and **Verify that the certificate is currently valid**.

g. In **Encryption Protocols**, clear **TLSv1.1** (not supported by Avaya Aura®). Ensure that the minimum supported TLS version configured on System Manager matches the TLS versions chosen on Openfire. For example, if the minimum supported version on System Manager is TLSv1.2, then TLSv1.2 must be selected on Openfire as well.

h. 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.

Note:

This procedure is not supported for Openfire 4.1.1. Openfire versions greater than 4.1.1 support this procedure.

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 9: 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.
      - `nextplane` to federate with UC federation- NextPlane.
      - `generic` to federate with other XMPP servers.

      `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 9: 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.
        - `nextplane` to federate with UC federation- NextPlane.
        - `generic` to federate with other XMPP servers.

        `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

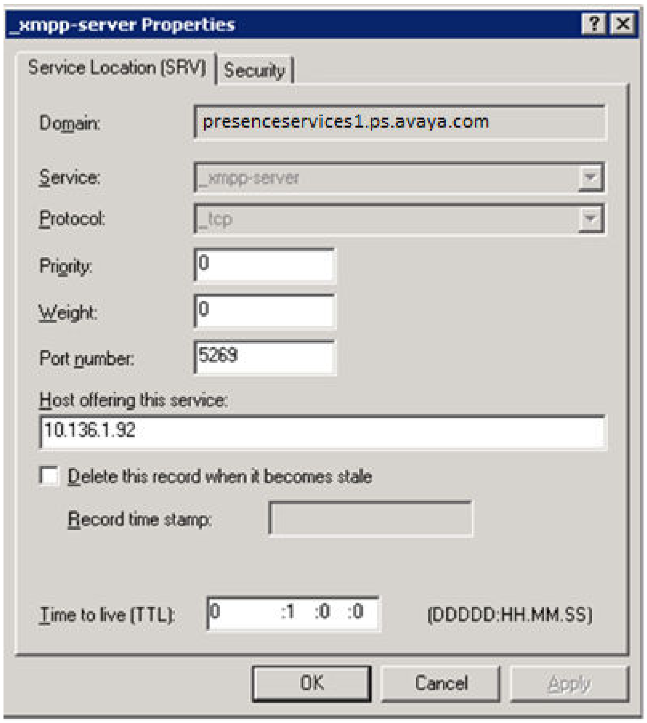
About this task

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 9: 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`



Domain: presenceservices1.ps.avaya.com

Service: _xmpp-server

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5269

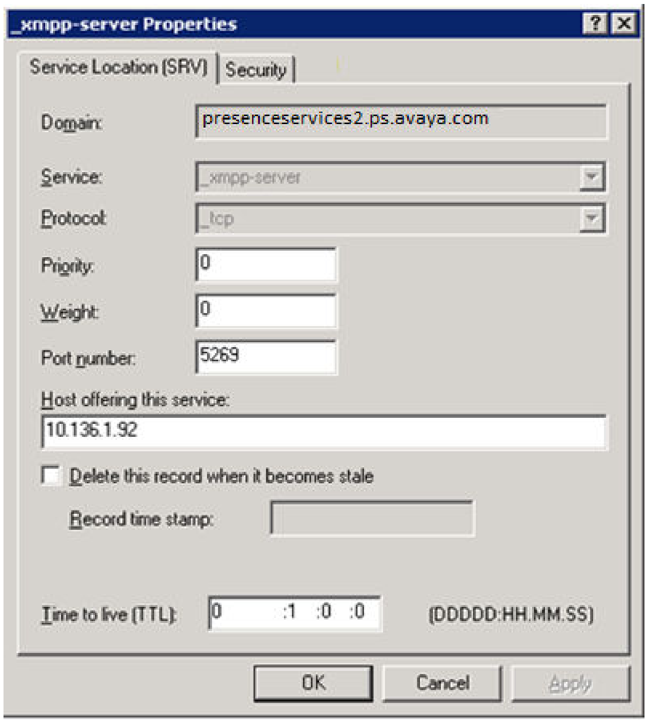
Host offering this service:
10.136.1.92

□ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

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`



Domain: presenceservices2.ps.avaya.com

Service: _xmpp-server

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5269

Host offering this service: 10.136.1.92

□ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Administering DNS SRV records for remote domains

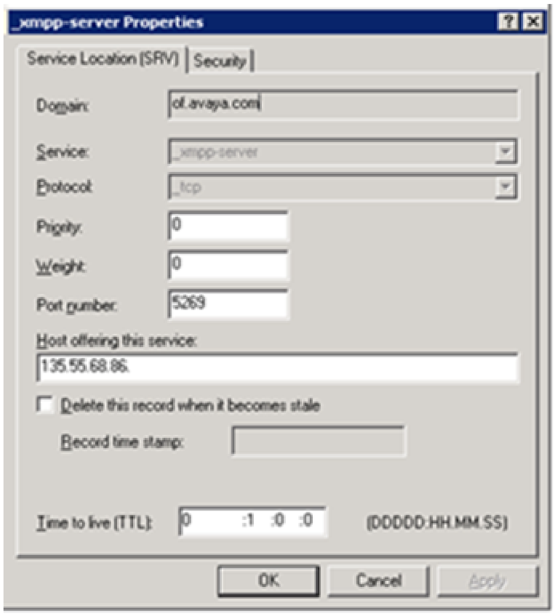
About this task

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 9: 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`



Domain: of.avaya.com

Service: _xmpp-server

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5269

Host offering this service: 135.55.68.86.

□ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

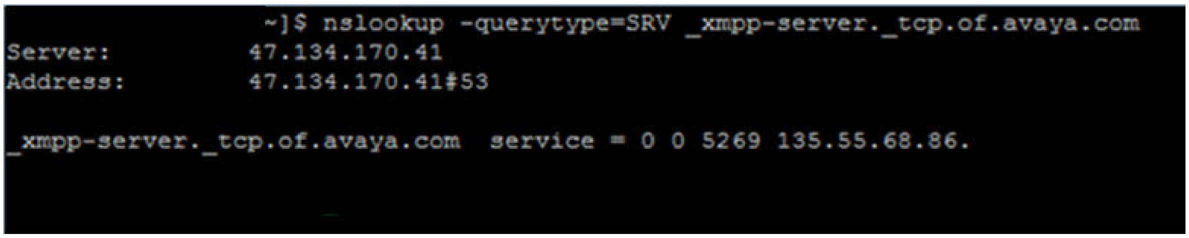
Verifying DNS resolution and server reachability

About this task

This procedure uses the sample values in the “Table 9: Single-server Cluster Federated with Ignite Openfire example values” section.

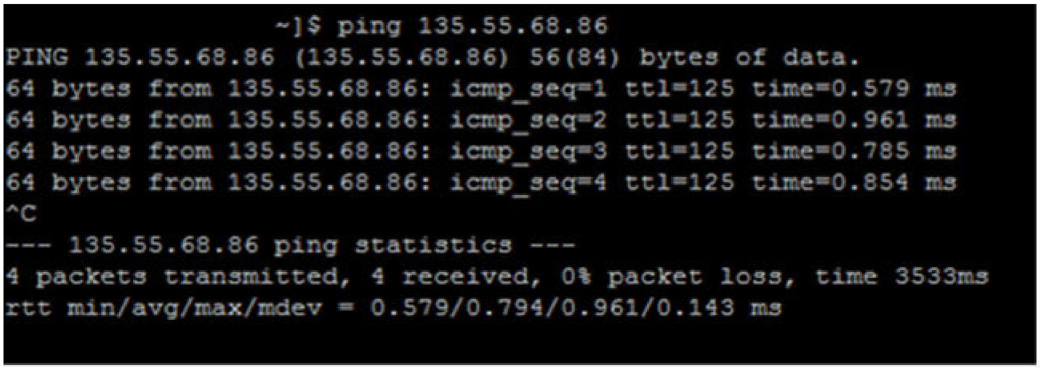
Procedure

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.



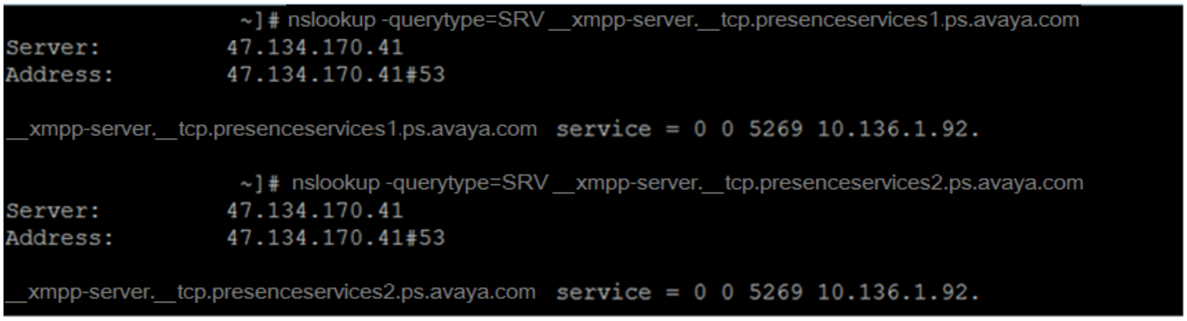
```
                  ~]$ nslookup -querytype=SRV _xmpp-server._tcp.of.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_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.



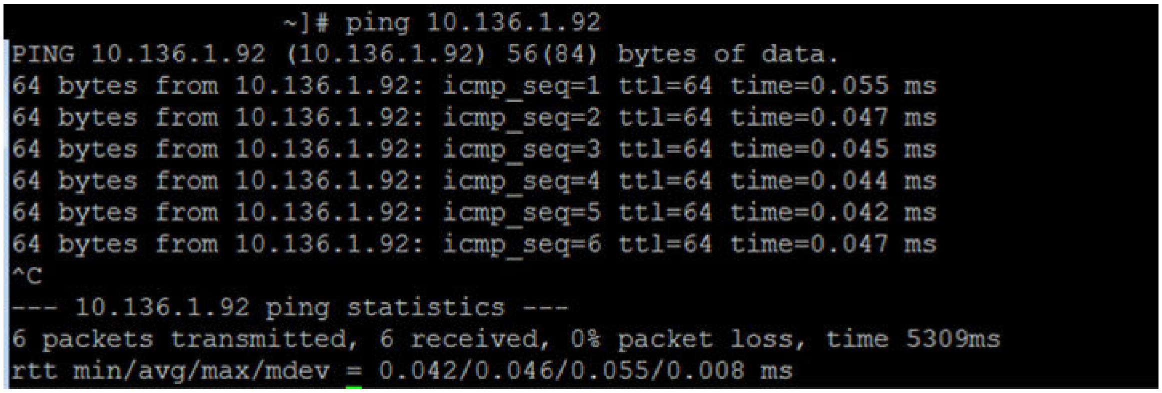
```
                  ~]$ ping 135.55.68.86
PING 135.55.68.86 (135.55.68.86) 56(84) bytes of data.
64 bytes from 135.55.68.86: icmp_seq=1 ttl=125 time=0.579 ms
64 bytes from 135.55.68.86: icmp_seq=2 ttl=125 time=0.961 ms
64 bytes from 135.55.68.86: icmp_seq=3 ttl=125 time=0.785 ms
64 bytes from 135.55.68.86: 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 13: 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 236	
2	Enable Certificate Verification on the Openfire server.	Administering Enable Certificate Verification on Openfire on page 157	

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 152	
2	Administer XMPP federation on DC-2.	Checklist for configuring XMPP federation on page 152	
3	Administer DNS on external XMPP server.	Administration of DNS on external XMPP server for a Geographic Redundant deployment on page 166	

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 166	
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 166	

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 14: 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 15: 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 NextPlane

For administering XMPP federation with NextPlane on Avaya Breeze™ server, refer to the “XMPP federation” section.

The similar administration of federation setting and import of the certificates should be done on NextPlane server in order for Presence/IM exchange between Presence and Nextplane. Contact NextPlane Support for administration help.

Related links

XMPP federation on page 151

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 16: Checklist for configuring XMPP federation with Cisco Jabber

No.	Task	Reference	✔
1	Configure DNS SRV records.	Setting up DNS on page 169	

Table continues…

No.	Task	Reference	✔
2	Configure Presence Services to enable federation. Presence Services support dynamic configuration change except port number.	Configuring Presence Services on page 170	
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 170	
4	If using TLS. import Cisco certificate to presence server and import System Manager certificate to Cisco Jabber.	Cisco Jabber certificates on page 172	

Setting up DNS

Before you begin

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

Procedure

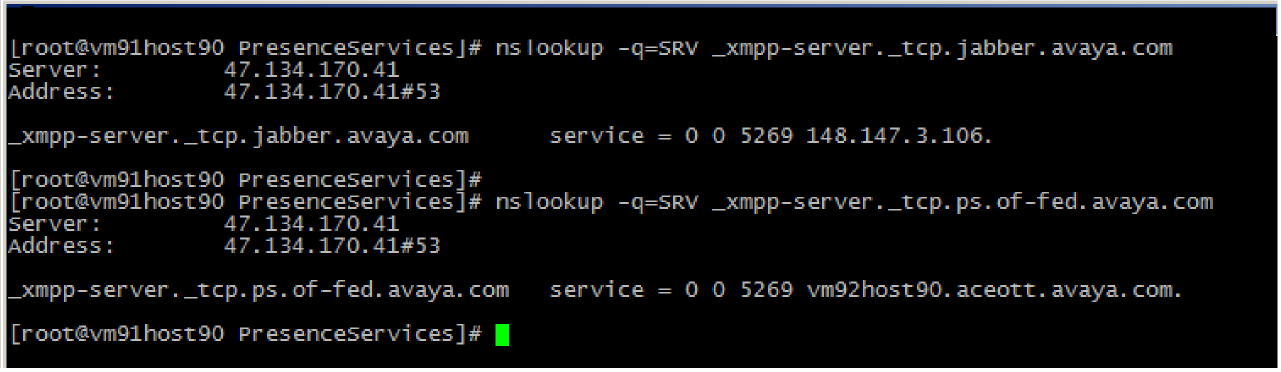
To verify SRV records run following commands.

- `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`.

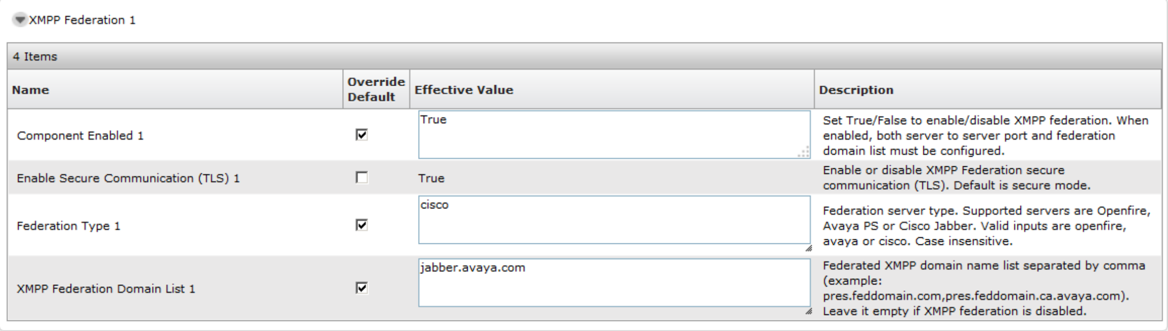


```
[root@vm91host90 PresenceServices]# nslookup -q=SRV _xmpp-server._tcp.jabber.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_xmpp-server._tcp.jabber.avaya.com      service = 0 0 5269 148.147.3.106.

[root@vm91host90 PresenceServices]#
[root@vm91host90 PresenceServices]# nslookup -q=SRV _xmpp-server._tcp.ps.of-fed.avaya.com
Server:         47.134.170.41
Address:        47.134.170.41#53

_xmpp-server._tcp.ps.of-fed.avaya.com   service = 0 0 5269 vm92host90.aceott.avaya.com.

[root@vm91host90 PresenceServices]#
```

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.



XMPP Federation 1

4 Items

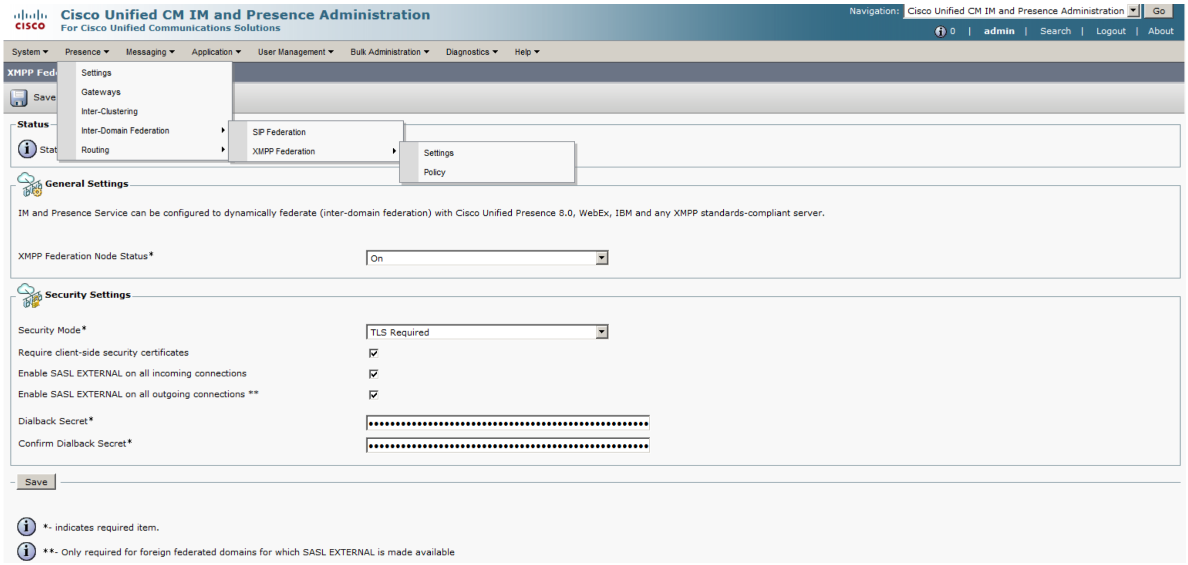
Name	Override Default	Effective Value	Description
Component Enabled 1	☑	True	Set True/False to enable/disable XMPP federation. When enabled, both server to server port and federation domain list must be configured.
Enable Secure Communication (TLS) 1	□	True	Enable or disable XMPP Federation secure communication (TLS). Default is secure mode.
Federation Type 1	☑	cisco	Federation server type. Supported servers are Openfire, Avaya PS or Cisco Jabber. Valid inputs are openfire, avaya or cisco. Case insensitive.
XMPP Federation Domain List 1	☑	jabber.avaya.com	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.

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`



General Settings

IM and Presence Service can be configured to dynamically federate (inter-domain federation) with Cisco Unified Presence 8.0, WebEx, IBM and any XMPP standards-compliant server.

XMPP Federation Node Status* On

Security Settings

Security Mode* TLS Required

Require client-side security certificates ☑

Enable SASL EXTERNAL on all incoming connections ☑

Enable SASL EXTERNAL on all outgoing connections ** ☑

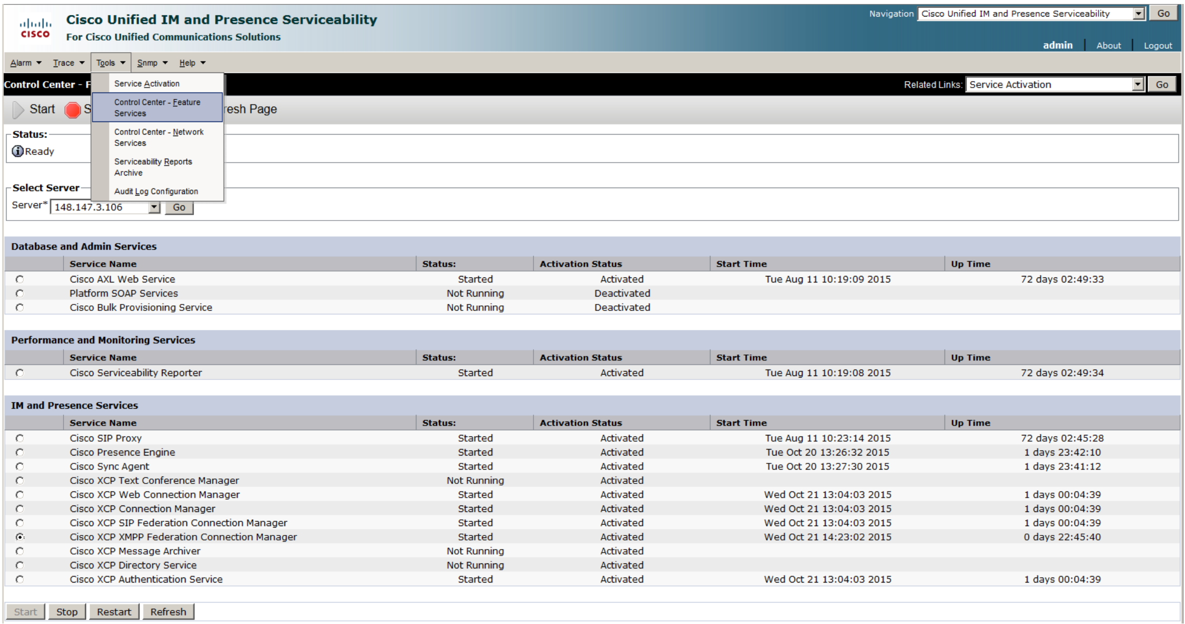
Dialback Secret* ••

Confirm Dialback Secret* ••

*- indicates required item.

**- Only required for foreign federated domains for which SASL EXTERNAL is made available

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


Cisco Unified IM and Presence Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified IM and Presence Serviceability Go
admin | About | Logout
Alarm Trace Tools Snmp Help
Service Activation
Control Center - Feature Services
Control Center - Network Services
Serviceability Reports Archive
Audit Log Configuration
Control Center - F
Related Links: Service Activation Go
Start S resh Page
Status:
Ready
Select Server
Server* 148.147.3.106 Go

Database and Admin Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco AXL Web Service	Started	Activated	Tue Aug 11 10:19:09 2015	72 days 02:49:33
○	Platform SOAP Services	Not Running	Deactivated		
○	Cisco Bulk Provisioning Service	Not Running	Deactivated		

Performance and Monitoring Services

	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco Serviceability Reporter	Started	Activated	Tue Aug 11 10:19:08 2015	72 days 02:49:34

IM and Presence Services

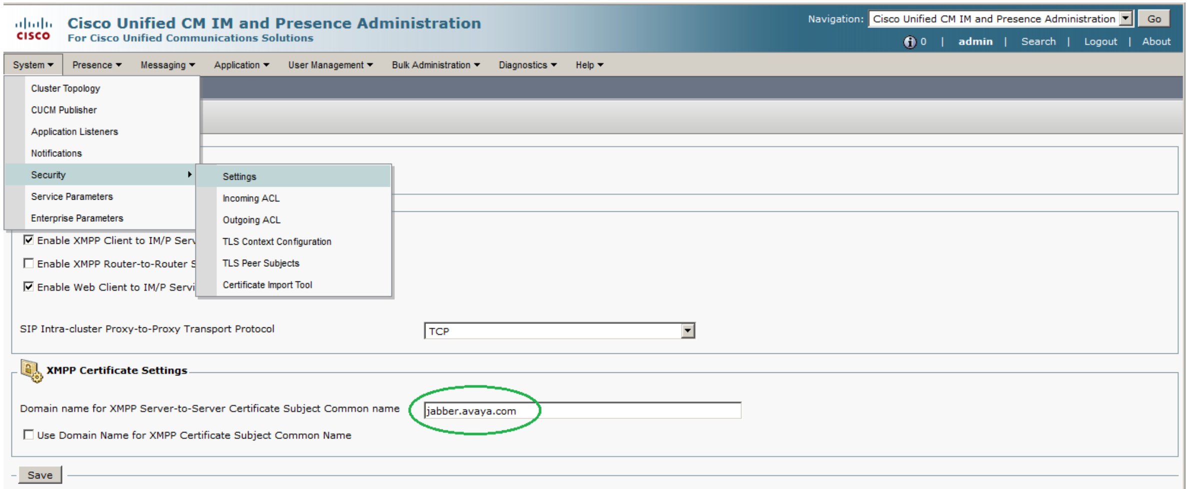
	Service Name	Status:	Activation Status	Start Time	Up Time
○	Cisco SIP Proxy	Started	Activated	Tue Aug 11 10:23:14 2015	72 days 02:45:28
○	Cisco Presence Engine	Started	Activated	Tue Oct 20 13:26:32 2015	1 days 23:42:10
○	Cisco Sync Agent	Started	Activated	Tue Oct 20 13:27:30 2015	1 days 23:41:12
○	Cisco XCP Text Conference Manager	Not Running	Activated		
○	Cisco XCP Web Connection Manager	Started	Activated	Wed Oct 21 13:04:03 2015	1 days 00:04:39
○	Cisco XCP Connection Manager	Started	Activated	Wed Oct 21 13:04:03 2015	1 days 00:04:39
○	Cisco XCP SIP Federation Connection Manager	Started	Activated	Wed Oct 21 13:04:03 2015	1 days 00:04:39
●	Cisco XCP XMPP Federation Connection Manager	Started	Activated	Wed Oct 21 14:23:02 2015	0 days 22:45:40
○	Cisco XCP Message Archiver	Not Running	Activated		
○	Cisco XCP Directory Service	Not Running	Activated		
○	Cisco XCP Authentication Service	Started	Activated	Wed Oct 21 13:04:03 2015	1 days 00:04:39

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**.


Cisco Unified CM IM and Presence Administration
For Cisco Unified Communications Solutions
Navigation: Cisco Unified CM IM and Presence Administration Go
0 | admin | Search | Logout | About
System Presence Messaging Application User Management Bulk Administration Diagnostics Help
Cluster Topology
CUCM Publisher
Application Listeners
Notifications
Security
Service Parameters
Enterprise Parameters
Settings
Incoming ACL
Outgoing ACL
TLS Context Configuration
TLS Peer Subjects
Certificate Import Tool
Save

☑ Enable XMPP Client to IM/P Serv

☐ Enable XMPP Router-to-Router S

☑ Enable Web Client to IM/P Servi

SIP Intra-cluster Proxy-to-Proxy Transport Protocol: TCP

XMPP Certificate Settings

Domain name for XMPP Server-to-Server Certificate Subject Common name: jabber.avaya.com

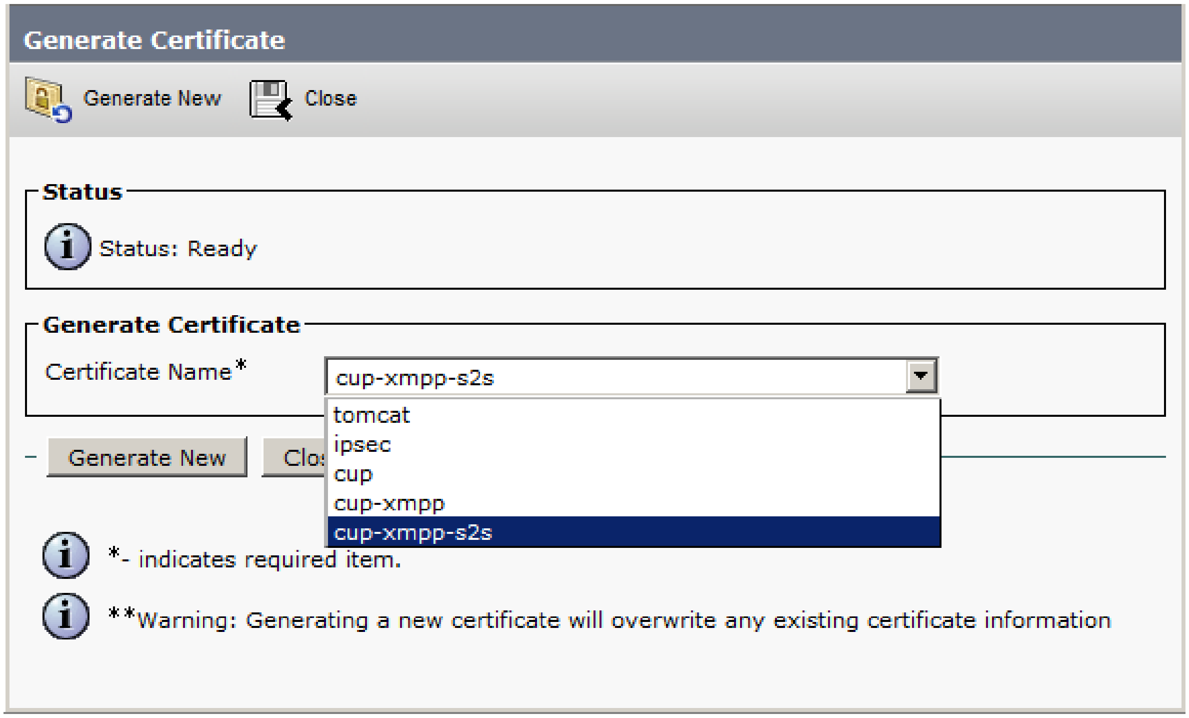
☐ Use Domain Name for XMPP Certificate Subject Common Name

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**.



Generate Certificate

Status

Status: Ready

Generate Certificate

Certificate Name* cup-xmpp-s2s

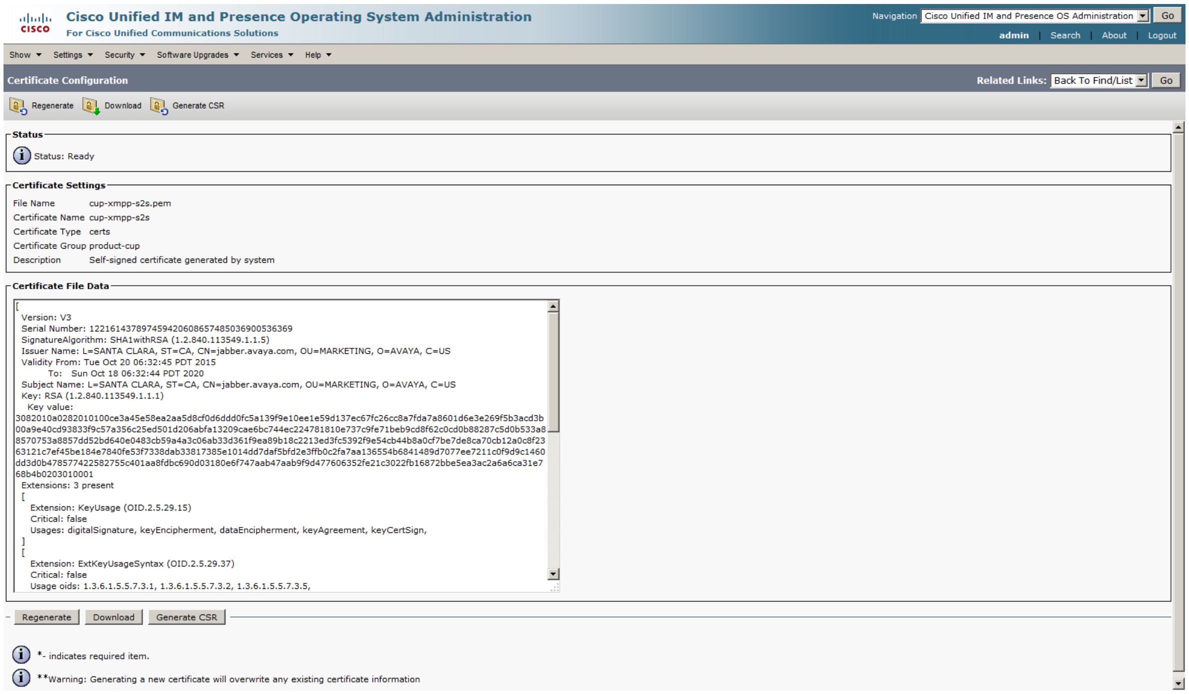
*- indicates required item.

**Warning: Generating a new certificate will overwrite any existing certificate information

   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.


Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified IM and Presence OS Administration Go
admin | Search | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate Configuration
Related Links: Back To Find/List Go
Regenerate Download Generate CSR

Status

Status: Ready

Certificate Settings

File Name	cup-xmpp-s2s.pem
Certificate Name	cup-xmpp-s2s
Certificate Type	certs
Certificate Group	product-cup
Description	Self-signed certificate generated by system

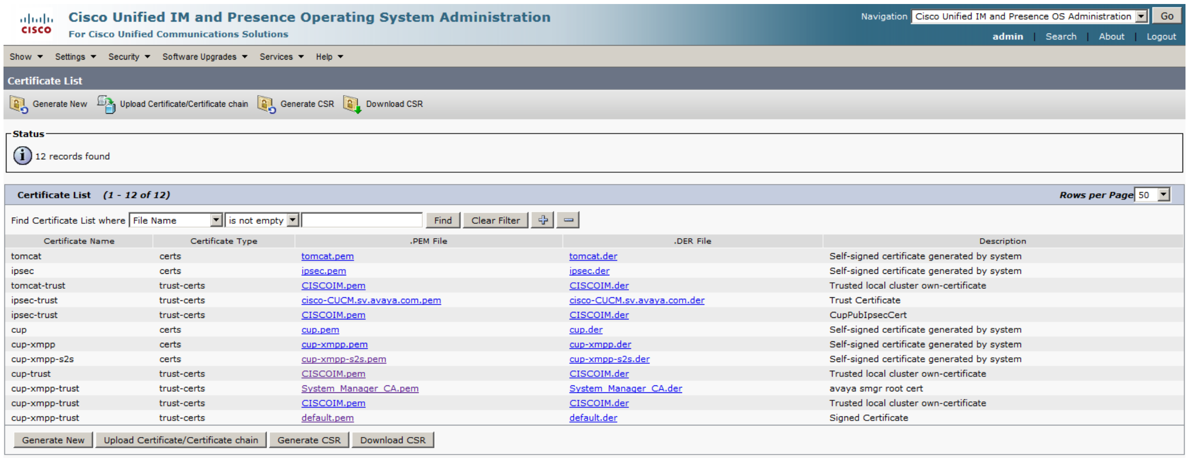
Certificate File Data

```
[
  Version: V3
  Serial Number: 122161437897459420608657485036900536369
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=SANTA CLARA, ST=CA, CN=jabber.avaya.com, OU=MARKETING, O=AVAYA, C=US
  Validity From: Tue Oct 20 06:32:45 PDT 2015
         To:   Sun Oct 18 06:32:44 PDT 2020
  Subject Name: L=SANTA CLARA, ST=CA, CN=jabber.avaya.com, OU=MARKETING, O=AVAYA, C=US
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100ce3a45e58ea2aa5d8cf0d6ddd0fc5a139f9e10ee1e59d137ec67fc26cc8a7fda7a8601d6e3e269f5b3acd3b
00a9e40cd93833f9c57a356c25ed501d206abfa13209cae6bc744ec224781810e737c9fe71beb9cd8f62c0cd0b88287c5d0b533a8
8570753a8857dd52bd640e0483cb59a4a3c06ab33d361f9ea89b18c2213ed3fc5392f9e54cb44b8a0cf7be7de8ca70cb12a0c8f23
63121c7ef45be184e7840fe53f7338dab33817385e1014dd7daf5bfd2e3ffb0c2fa7aa136554b6841489d7077ee7211c0f9d9c1460
dd3d0b478577422582755c401aa8fdbc690d03180e6f747aab47aab9f9d477606352fe21c3022fb16872bbe5ea3ac2a6a6ca31e7
68b4b0203010001
  Extensions: 3 present
  [
    Extension: KeyUsage (OID.2.5.29.15)
    Critical: false
    Usages: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign,
  ]
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
```

*- indicates required item.

**Warning: Generating a new certificate will overwrite any existing certificate information

12. Click **Download**.


Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified IM and Presence OS Administration Go
admin | Search | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate New Upload Certificate/Certificate chain Generate CSR Download CSR

Status

12 records found

Certificate List (1 - 12 of 12) Rows per Page 50

Find Certificate List where File Name is not empty

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

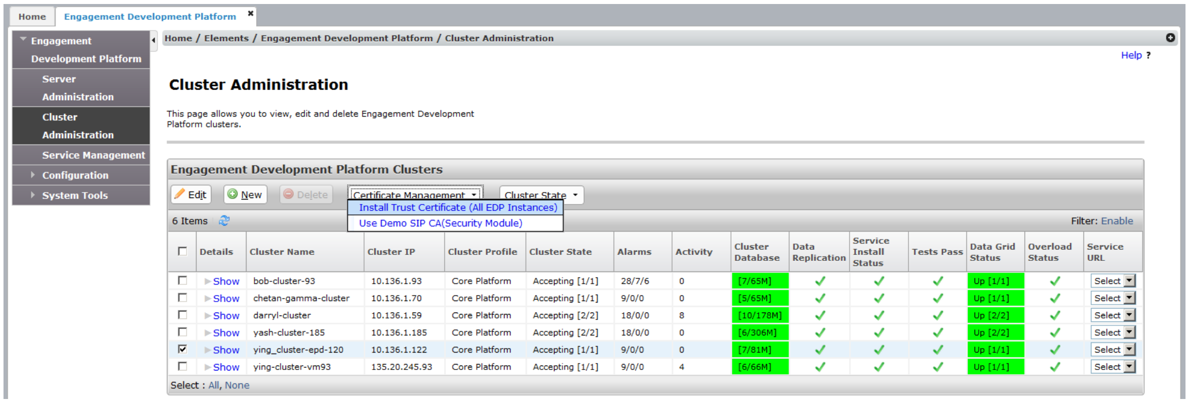
Generate New Upload Certificate/Certificate chain Generate CSR Download CSR

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)**.


Home
Engagement Development Platform
Engagement Development Platform
Server Administration
Cluster Administration
Service Management
Configuration
System Tools
Home / Elements / Engagement Development Platform / Cluster Administration
Help ?
Edit
New
Delete
Certificate Management
Install Trust Certificate (All EDP Instances)
Use Demo SIP CA(Security Module)
Cluster State
6 Items
Filter: Enable
Select : All, None

Cluster Administration

This page allows you to view, edit and delete Engagement Development Platform clusters.

Engagement Development Platform Clusters

□	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status	Service URL
□	Show	bob-cluster-93	10.136.1.93	Core Platform	Accepting [1/1]	28/7/6	0	[7/65M]	✓	✓	✓	Up [1/1]	✓	Select
□	Show	chetan-gamma-cluster	10.136.1.70	Core Platform	Accepting [1/1]	9/0/0	0	[5/65M]	✓	✓	✓	Up [1/1]	✓	Select
□	Show	darryl-cluster	10.136.1.59	Core Platform	Accepting [2/2]	18/0/0	8	[10/178M]	✓	✓	✓	Up [2/2]	✓	Select
□	Show	yash-cluster-185	10.136.1.185	Core Platform	Accepting [2/2]	18/0/0	0	[6/306M]	✓	✓	✓	Up [2/2]	✓	Select
☑	Show	ying_cluster-epd-120	10.136.1.122	Core Platform	Accepting [1/1]	9/0/0	0	[7/81M]	✓	✓	✓	Up [1/1]	✓	Select
□	Show	ying-cluster-vm93	135.20.245.93	Core Platform	Accepting [1/1]	9/0/0	4	[6/66M]	✓	✓	✓	Up [1/1]	✓	Select

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:7
5:4D: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
```

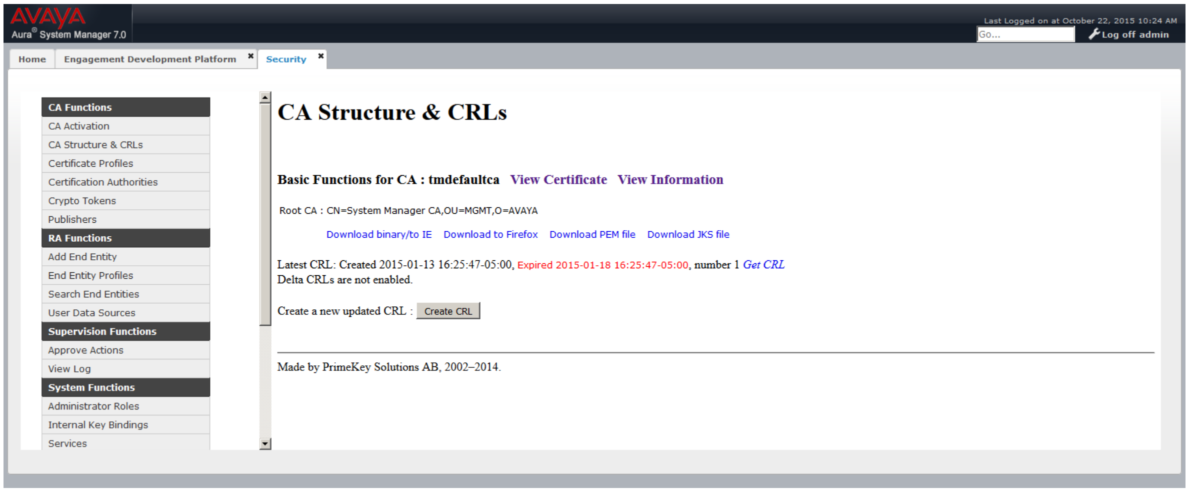
```
Data_Encipherment
Key_Agreement
Key_CertSign
]

#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.



CA Structure & CRLs

Basic Functions for CA : tmdefaultca

Root CA : CN=System Manager CA,OU=MGMT,O=AVAYA

Latest CRL: Created 2015-01-13 16:25:47-05:00, Expired 2015-01-18 16:25:47-05:00, number 1

Delta CRLs are not enabled.

Create a new updated CRL :

Made by PrimeKey Solutions AB, 2002–2014.

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

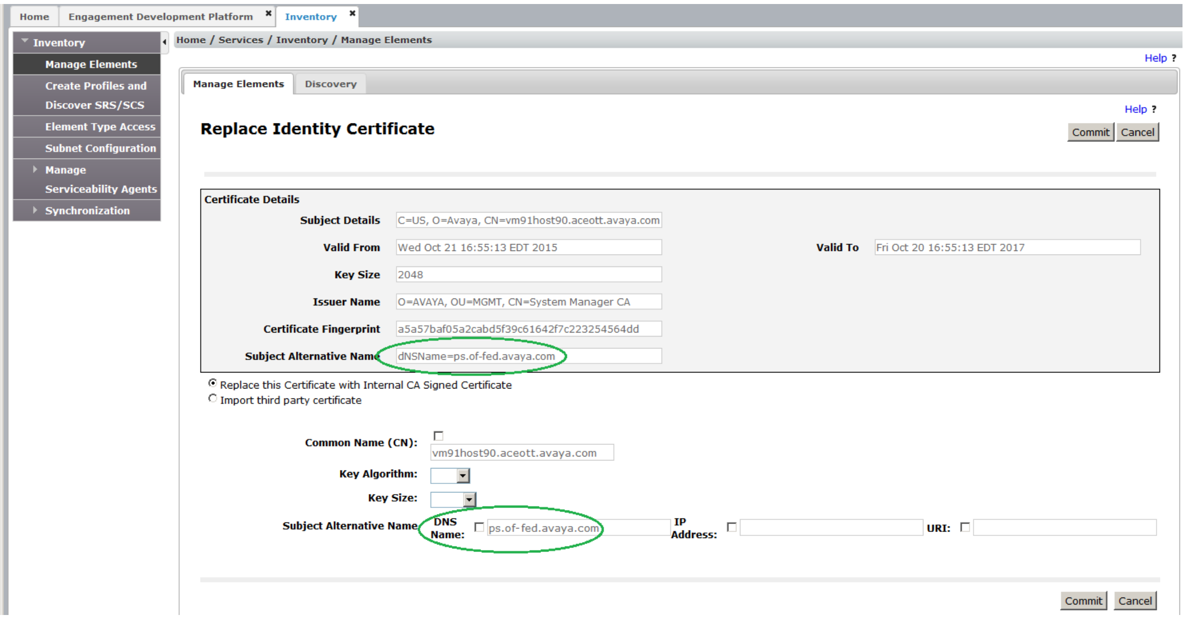
About this task

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.



Replace Identity Certificate

Certificate Details

Subject Details: C=US, O=Avaya, CN=vm91host90.aceott.avaya.com

Valid From: Wed Oct 21 16:55:13 EDT 2015

Valid To: Fri Oct 20 16:55:13 EDT 2017

Key Size: 2048

Issuer Name: O=AVAYA, OU=MGMT, CN=System Manager CA

Certificate Fingerprint: a5a57baf05a2cabd5f39c61642f7c223254564dd

Subject Alternative Name: dNSName=ps.of-fed.avaya.com

● Replace this Certificate with Internal CA Signed Certificate
○ Import third party certificate

Common Name (CN): □ vm91host90.aceott.avaya.com

Key Algorithm:

Key Size:

Subject Alternative Name: DNS Name: □ ps.of-fed.avaya.com IP Address: □ URI: □

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
]
]
```

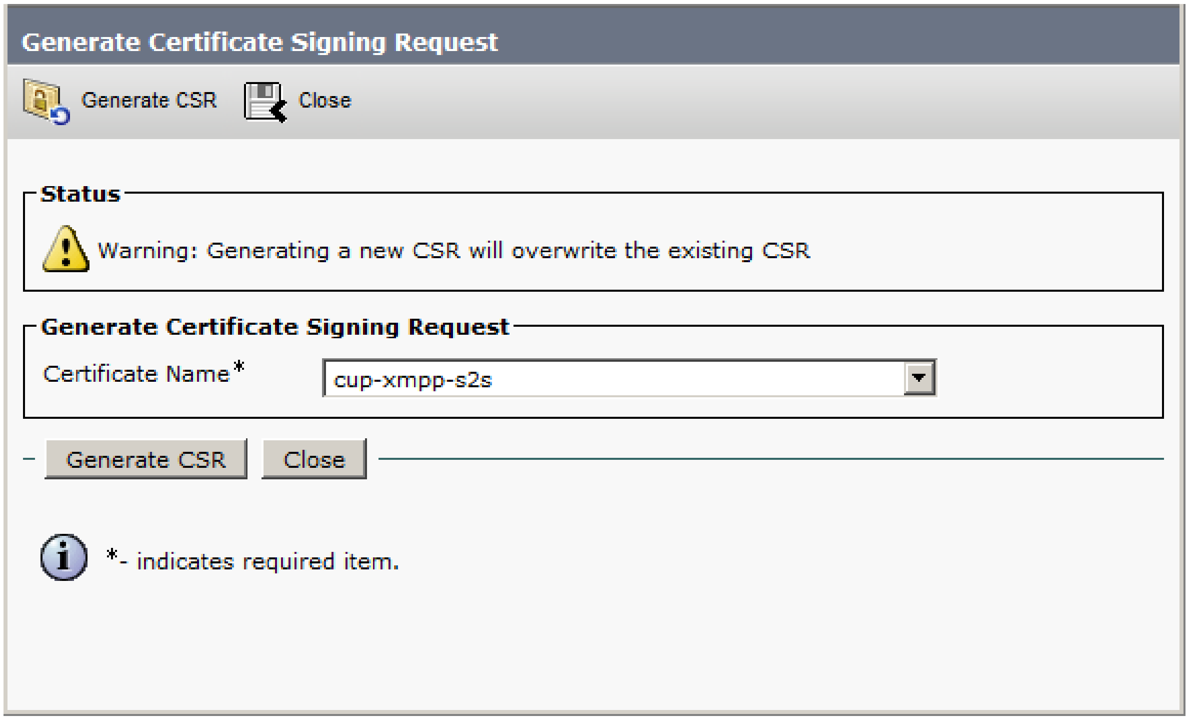
Generating the Certificate Signing Request file

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.



Generate Certificate Signing Request

Status

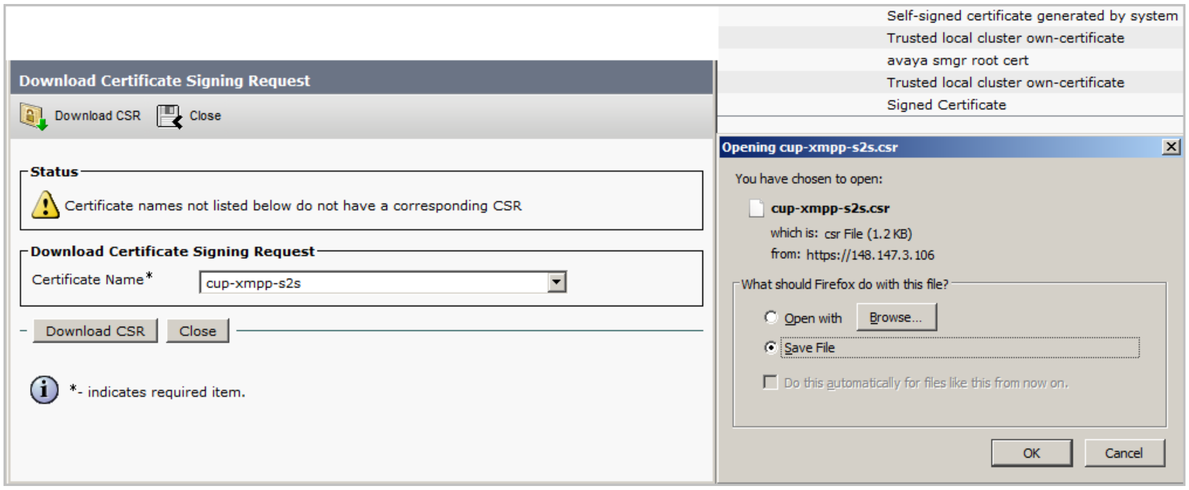
Warning: Generating a new CSR will overwrite the existing CSR

Generate Certificate Signing Request

Certificate Name* cup-xmpp-s2s

*- indicates required item.

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



Self-signed certificate generated by system
Trusted local cluster own-certificate
avaya smgr root cert
Trusted local cluster own-certificate
Signed Certificate

Download Certificate Signing Request

Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Name* cup-xmpp-s2s

*- indicates required item.

Opening cup-xmpp-s2s.csr

You have chosen to open:

cup-xmpp-s2s.csr

which is: csr File (1.2 KB)

from: https://148.147.3.106

What should Firefox do with this file?

○ Open with

● Save File

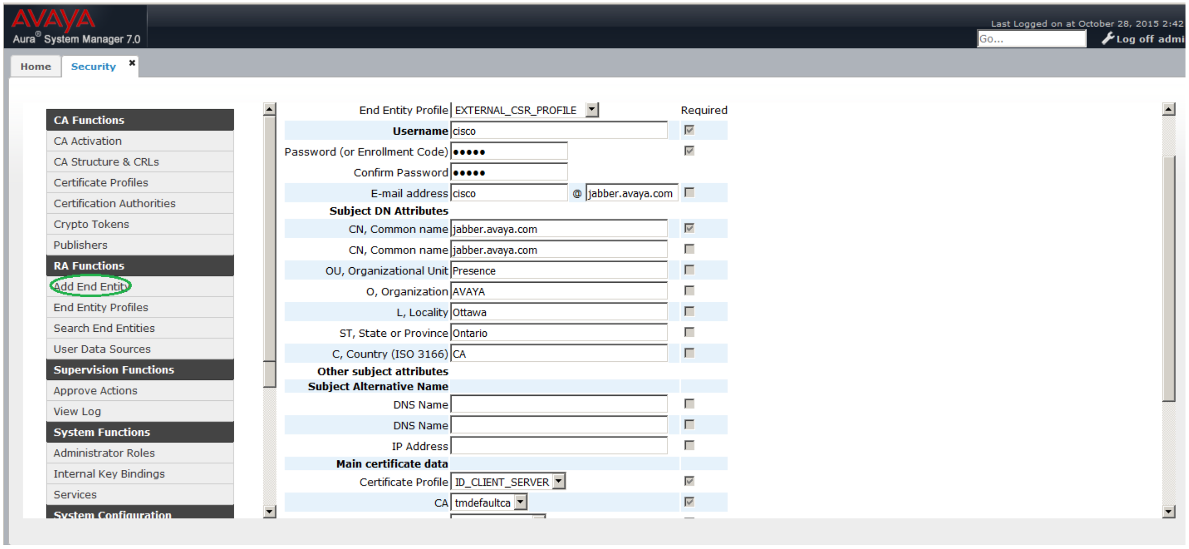
□ Do this automatically for files like this from now on.

Generating profile on System Manager

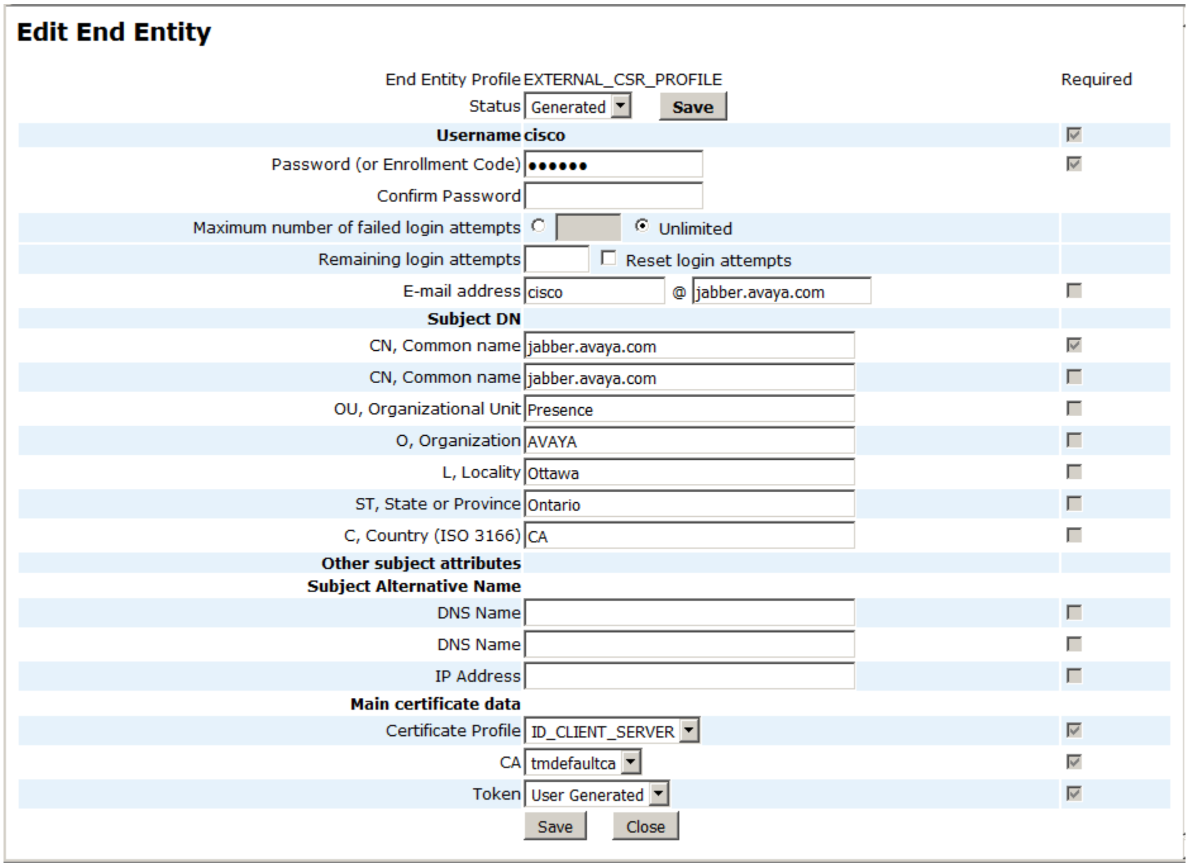
Procedure

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`



		Required
End Entity Profile	EXTERNAL_CSR_PROFILE	
Username	cisco	☑
Password (or Enrollment Code)	●●●●●	☑
Confirm Password	●●●●●	
E-mail address	cisco @ jabber.avaya.com	□
Subject DN Attributes		
CN, Common name	jabber.avaya.com	☑
CN, Common name	jabber.avaya.com	□
OU, Organizational Unit	Presence	□
O, Organization	AVAYA	□
L, Locality	Ottawa	□
ST, State or Province	Ontario	□
C, Country (ISO 3166)	CA	□
Other subject attributes		
Subject Alternative Name		
DNS Name		□
DNS Name		□
IP Address		□
Main certificate data		
Certificate Profile	ID_CLIENT_SERVER	☑
CA	tmdefaultca	☑



Edit End Entity

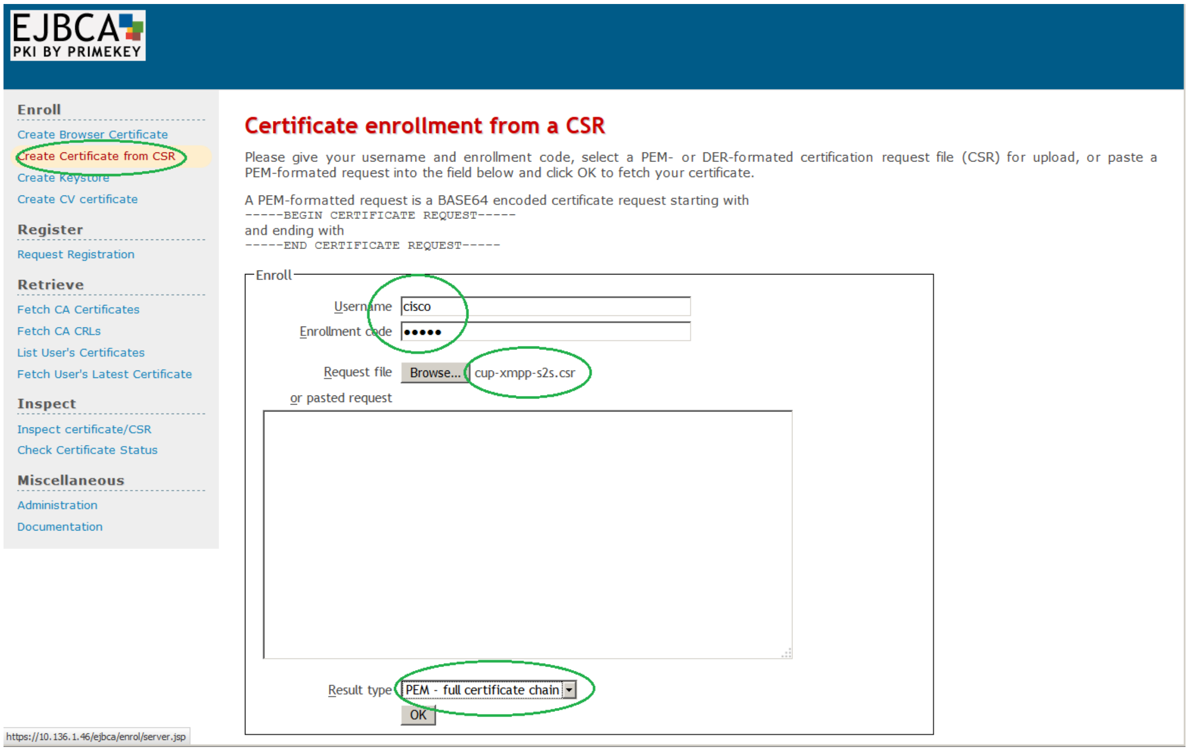
End Entity Profile	EXTERNAL_CSR_PROFILE	Required
Status	Generated ▾ **Save**	
Username	**cisco**	☑
Password (or Enrollment Code)	••••••	☑
Confirm Password		
Maximum number of failed login attempts	○ ● Unlimited	
Remaining login attempts	□ Reset login attempts	
E-mail address	cisco @ jabber.avaya.com	□
Subject DN		
CN, Common name	jabber.avaya.com	☑
CN, Common name	jabber.avaya.com	□
OU, Organizational Unit	Presence	□
O, Organization	AVAYA	□
L, Locality	Ottawa	□
ST, State or Province	Ontario	□
C, Country (ISO 3166)	CA	□
Other subject attributes		
Subject Alternative Name		
DNS Name		□
DNS Name		□
IP Address		□
Main certificate data		
Certificate Profile	ID_CLIENT_SERVER ▾	☑
CA	tmdefaultca ▾	☑
Token	User Generated ▾	☑
	Save Close	

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**



Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formated certification request file (CSR) for upload, or paste a PEM-formated request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with

```
-----BEGIN CERTIFICATE REQUEST-----
```

and ending with

```
-----END CERTIFICATE REQUEST-----
```

Enroll

Username: cisco

Enrollment code: •••••

Request file: cup-xmpp-s2s.csr

or pasted request

Result type: PEM - full certificate chain

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

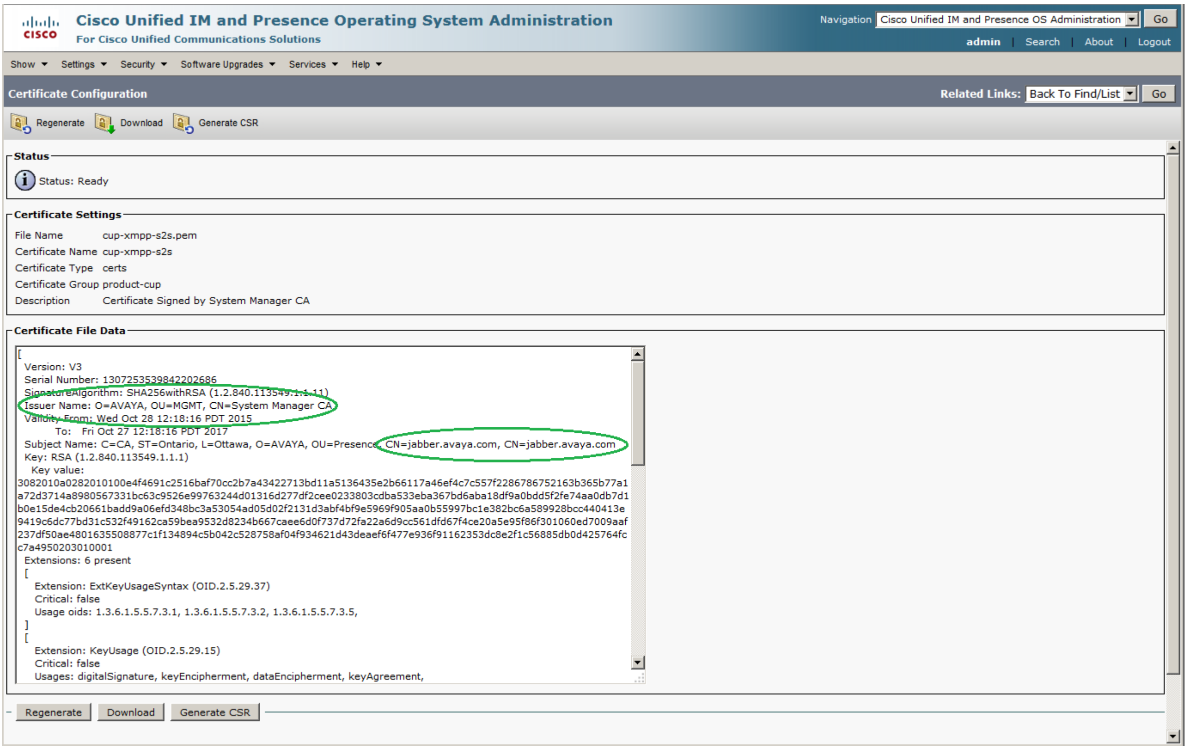
Installing System Manager signed Cisco certificate on Cisco Jabber

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**.


Cisco Unified IM and Presence Operating System Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified IM and Presence OS Administration
Go
admin | Search | About | Logout
Show
Settings
Security
Software Upgrades
Services
Help
Certificate Configuration
Related Links:
Back To Find/List
Go
Regenerate
Download
Generate CSR

Status

Status: Ready

Certificate Settings

File Name cup-xmpp-s2s.pem
Certificate Name cup-xmpp-s2s
Certificate Type certs
Certificate Group product-cup
Description Certificate Signed by System Manager CA

Certificate File Data

```
[
  Version: V3
  Serial Number: 1307253539842202686
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: O=AVAYA, OU=MGMT, CN=System Manager CA
  Validity From: Wed Oct 28 12:18:16 PDT 2015
        To:   Fri Oct 27 12:18:16 PDT 2017
  Subject Name: C=CA, ST=Ontario, L=Ottawa, O=AVAYA, OU=Presence, CN=jabber.avaya.com, CN=jabber.avaya.com
  Key: RSA (1.2.840.113549.1.1.1)
   Key value:
3082010a0282010100e4f4691c2516baf70cc2b7a43422713bd11a5136435e2b66117a46ef4c7c557f2286786752163b365b77a1
a72d3714a8980567331bc63c9526e99763244d01316d277df2cee0233803cdba533eba367bd6aba18df9a0bdd5f2fe74aa0db7d1
b0e15de4cb20661badd9a06efd348bc3a53054ad05d02f2131d3abf4bf9e5969f905aa0b55997bc1e382bc6a589928bcc440413e
9419c6dc77bd31c532f49162ca59bea9532d8234b667caee6d0f737d72fa22a6d9cc561dfd67f4ce20a5e95f86f301060ed7009aaf
237df50ae4801635508877c1f134894c5b042c528758af04f934621d43deaef6f477e936f91162353dc8e2f1c56885db0d425764fc
c7a4950203010001
  Extensions: 6 present
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
  ]
  [
    Extension: KeyUsage (OID.2.5.29.15)
    Critical: false
    Usages: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement,
```

Zang Federation

Presence Services supports federation with Zang Cloud Services to enable users to exchange instant messages as SMS with mobile users.

Zang federation enables users to:

- Send IMs to a mobile user added as a private contact of an Aura user.
- Receive the SMS sent by a mobile user as an IM.
- Send and receive IM or SMS as described earlier using the Presence Services REST APIs.

Prerequisites

Procedure

1. The organization must have a Zang account and subscription for Zang Cloud Services.

   The Account SID and the Auth Token are required to configure the federation.

   To access Zang home page, go to https://zang.io/. To access the Zang Clound Services, go to https://cloud.zang.io/.

2. The organization needs access to Zang phone numbers.

   Zang phone numbers can be bought from Zang using the administrator dashboard. These numbers are assigned to Aura users to enable them to use Zang services.

3. The organization must select the communication options with Zang Cloud Services:
    - Using Zang events: If Zang federation is configured in this mode, Zang Cloud Services will send any incoming SMS as HTTP events to Presence Services.

      This mode requires that the Avaya Breeze™ cluster running Presence Services to be reachable from Zang Cloud Services. The organization needs to ensure that HTTPS port 443 is not blocked by any firewall.
    - Using Presence Services SMS polling service: If Zang federation is configured in this mode, Presence Services polls Zang Cloud Services periodically to fetch any incoming SMS. Hence, it is not required that Zang Cloud Services send SMS events as they arrive. Use this mode of operation if the Avaya Breeze™ cluster is not reachable from outside the enterprise.

   This setting is required for receiving any incoming SMS from external users to the enterprise.

Importing CA certificate to the Avaya Breeze™ cluster

About this task

To communicate with Zang Cloud Services securely, the CA which signs Zang certificate needs to be imported on the Avaya Breeze™ cluster. The certificate is provided in the Presence Services bundle ZIP file. Use the following procedure to import this certificate.

Procedure

1. Locate the `Baltimore CyberTrust Root.pem` file in the `PresenceServices-Bundle-x.x.x.x.zip`.
2. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Cluster Administration**.
3. Select the Avaya Breeze™ cluster, and click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze Instances)**.
4. Select **Store Type** as **WEBSPHERE**.
5. Choose file as the PEM from the Presence Services bundle ZIP.
6. Click **Retrieve Certificate**.
7. Click **Commit**.

Enabling Zang Federation on 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 Avaya Breeze™ cluster and select the **Service** as **PresenceServices**.

5. Within the **Zang Federation** group, configure the attributes as follows:
    - Set the **Enable Zang Federation** field to `True`.
    - In the **Zang Account SID** field, enter the Zang account service identifier.

      This information may be retrieved from Zang administrator dashboard.
    - In the **Zang Auth Token** field, enter the Zang account authentication token.

      This information may be retrieved from Zang administrator dashboard.
    - Leave the **Zang SMS Request URL** field blank if you intend to use Zang events delivered to Presence Services, otherwise configure the Zang PubSub SMS Request URL as per SMS settings of the Zang application to use SMS polling.

Configuration of Zang federation

Zang Cloud Services must be configured so that Zang can deliver incoming SMS to Presence Services.

Configuring Zang federation using Zang events

About this task

Use the following procedure to configure SMS Request URL on Zang as Avaya Breeze™ URL.

Procedure

1. Log in to your Zang Cloud Services account.
2. Navigate to **Numbers** > **Manage Applications**.
3. Click **Add Application**.
4. In the General tab, enter a name.

   For example, `PresenceServices`
5. In the SMS tab, enter the SMS Request URL as `http(s)://<breeze-cluster-fqdn>/services/PresenceServices/rest/zang/sms`.
6. Leave the **Zang SMS Request URL** attribute empty.

   It is recommended to use https instead of http URL for secure transmission of data. If http URL is configured, the Avaya Breeze™ cluster must allow non-secure communication.

Configuring Zang federation using Presence Services SMS polling service

About this task

Use the following procedure to configure SMS Request URL on Zang as PubSub URL.

Procedure

1. Log in to your Zang Cloud Services account.
2. Navigate to **Numbers** > **Manage Applications**.
3. Click **Add Application**.

4. In the General tab, enter a name.

   For example, `PresenceServices`

5. In the SMS tab, enter the SMS Request URL as `https://pubsub.zang.io/<account-sid>/<container-name>`.

   <account-sid> is the is the Zang Account SID and *<container-name>* is any unique string within this account SID.

6. Configure Presence Services Zang SMS Request URL to the URL created in previous step.

Configuring users for Zang federation

About this task

Users must be assigned Zang phone numbers to be able to send and receive SMS to external mobile users. Use the following procedure to enable users for Zang federation.

Procedure

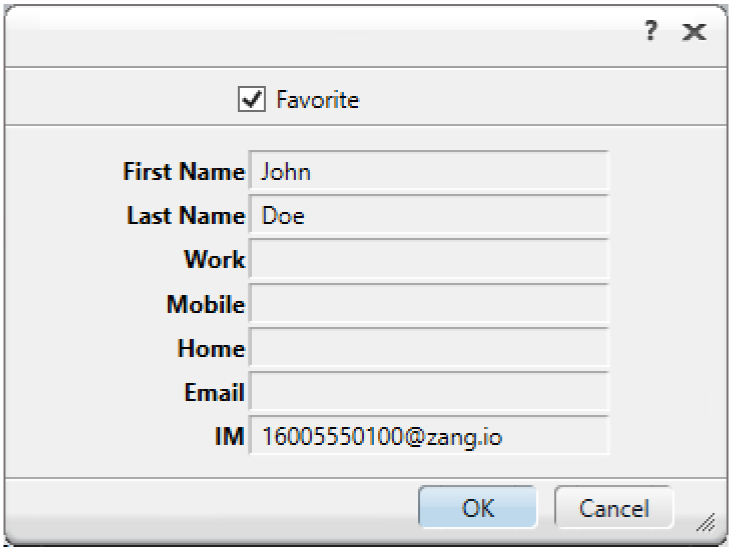
1. On the System Manager web console, navigate to **Users** > **User Management** > **Manage Users**.
2. Select the user and click **Edit**.
3. Click the Communication Profile tab.
4. In the **Communication Address** field, click **New**.
5. Select **Type** as **Other SIP**.
6. Enter the Fully Qualified Address as `<Zang Phone Number>@zang.io`.
7. Click **Add**.
8. Click **Commit**.
9. Repeat Step 1 to Step 8 for all the users you want to be Zang enabled.

Sending SMS to mobile users as private contacts

Procedure

1. Add external mobile users as private contacts of a Zang-enabled Aura user to facilitate sending SMS to them through an IM.

   This can be done using an Avaya One-X Communicator client as shown in the following figure. The IM address is configured as `<mobile number>@zang.io`. You must suffix the mobile number with zang.io domain.

   ☑ Favorite

First Name	John
Last Name	Doe
Work	
Mobile	
Home	
Email	
IM	16005550100@zang.io

2. Once the private contact is added, the user can initiate an IM to this contact which will be delivered as a SMS to the mobile user.

   a. Ensure that the Zang federation is enabled and configured.

   b. Ensure that the user has a Zang phone number assigned in his communication profile.

      The mobile user who receives this SMS will see the Zang phone number of the sender.

      If the mobile user sends an SMS or replies to an SMS, the SME is delivered to the Aura user as an IM.

3.

Sending SMS to mobile users through REST APIs

About this task

A Zang-enabled user can send SMS through Presence Services REST APIs.

Procedure

The user or application can use Zang address space to specify the recipient mobile number.

There is no need to suffix the number with zang.io domain.

If the mobile user sends an SMS or replies to an SMS, the SMS is delivered to the Aura user as an IM through the EventDelivery Service on Avaya Breeze™.

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

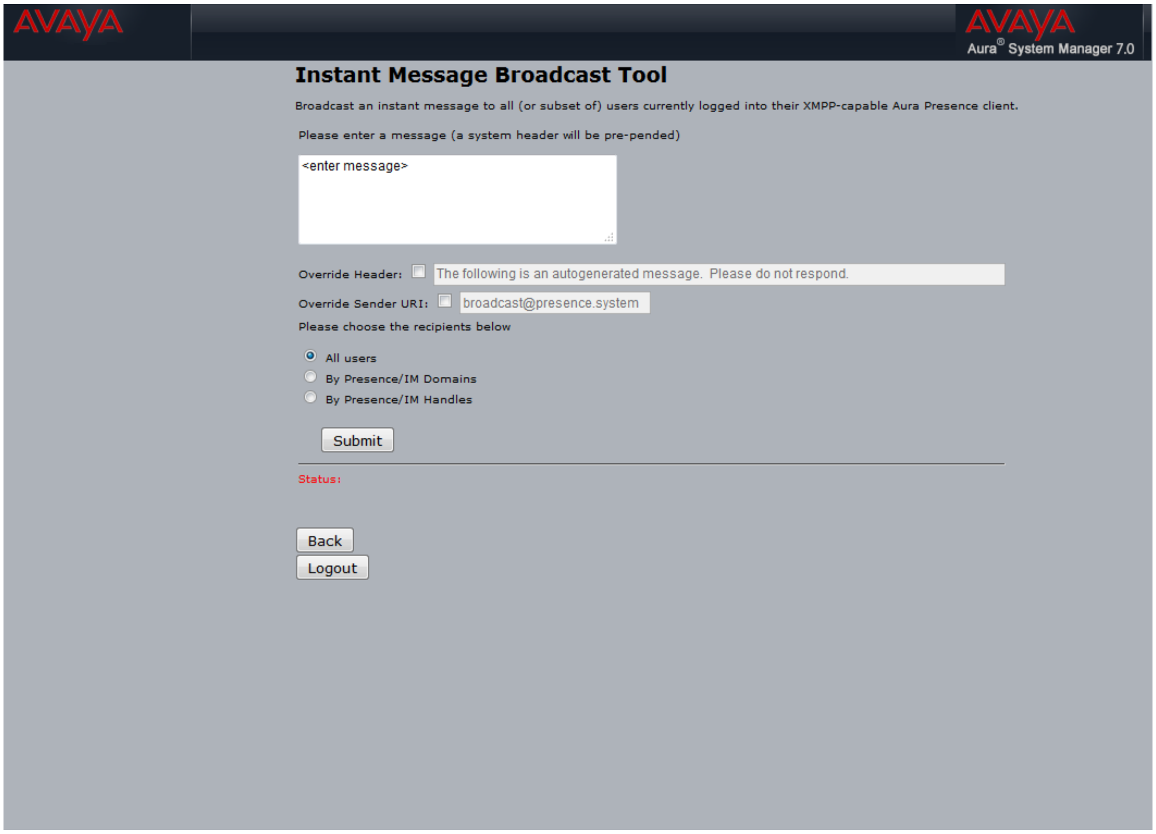
1. On the Presence Services Software Inventory web service page, log in using the System Manager administrative credentials.
2. Click **Instant Message Broadcast Tool**.

   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.



Instant Message Broadcast Tool

Broadcast an instant message to all (or subset of) users currently logged into their XMPP-capable Aura Presence client.

Please enter a message (a system header will be pre-pended)

<enter message>

Override Header: □ The following is an autogenerated message. Please do not respond.

Override Sender URI: □ broadcast@presence.system

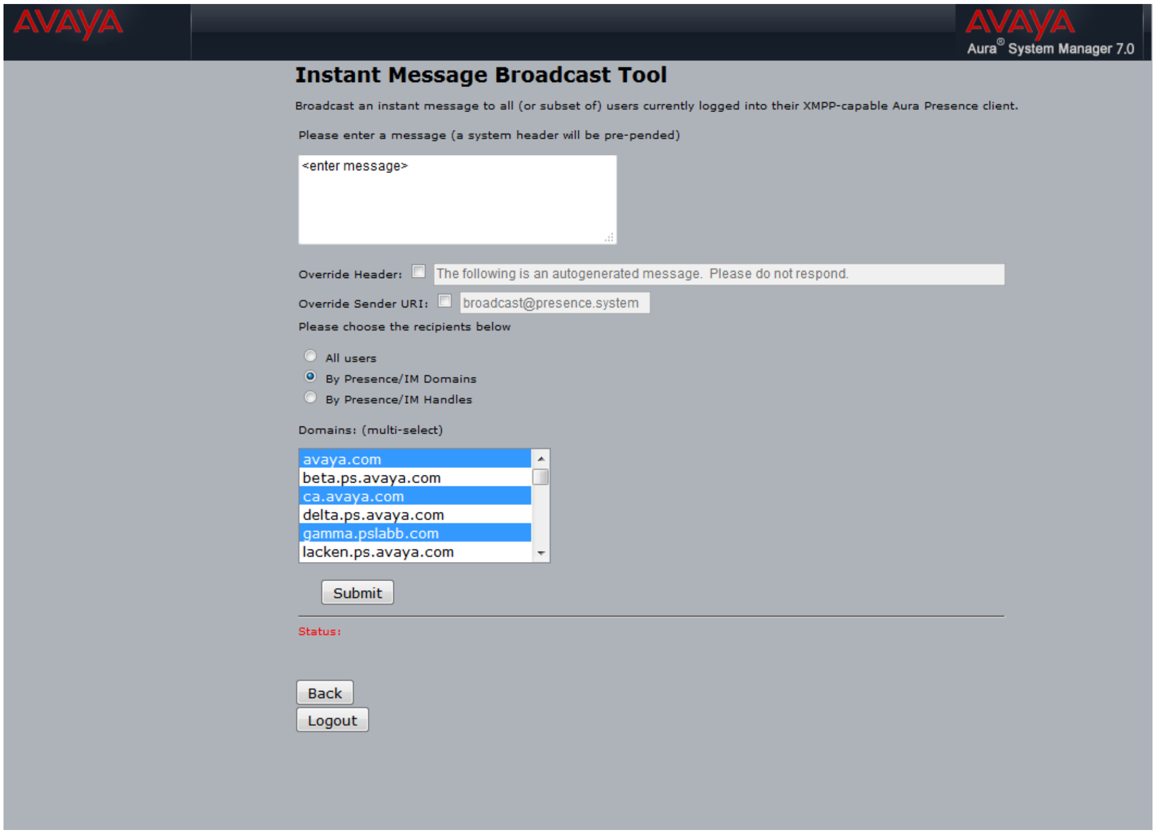
Please choose the recipients below

● All users
○ By Presence/IM Domains
○ By Presence/IM Handles

Status:

- 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.



Instant Message Broadcast Tool

Broadcast an instant message to all (or subset of) users currently logged into their XMPP-capable Aura Presence client.

Please enter a message (a system header will be pre-pended)

<enter message>

Override Header: □ The following is an autogenerated message. Please do not respond.

Override Sender URI: □ broadcast@presence.system

Please choose the recipients below

○ All users
● By Presence/IM Domains
○ By Presence/IM Handles

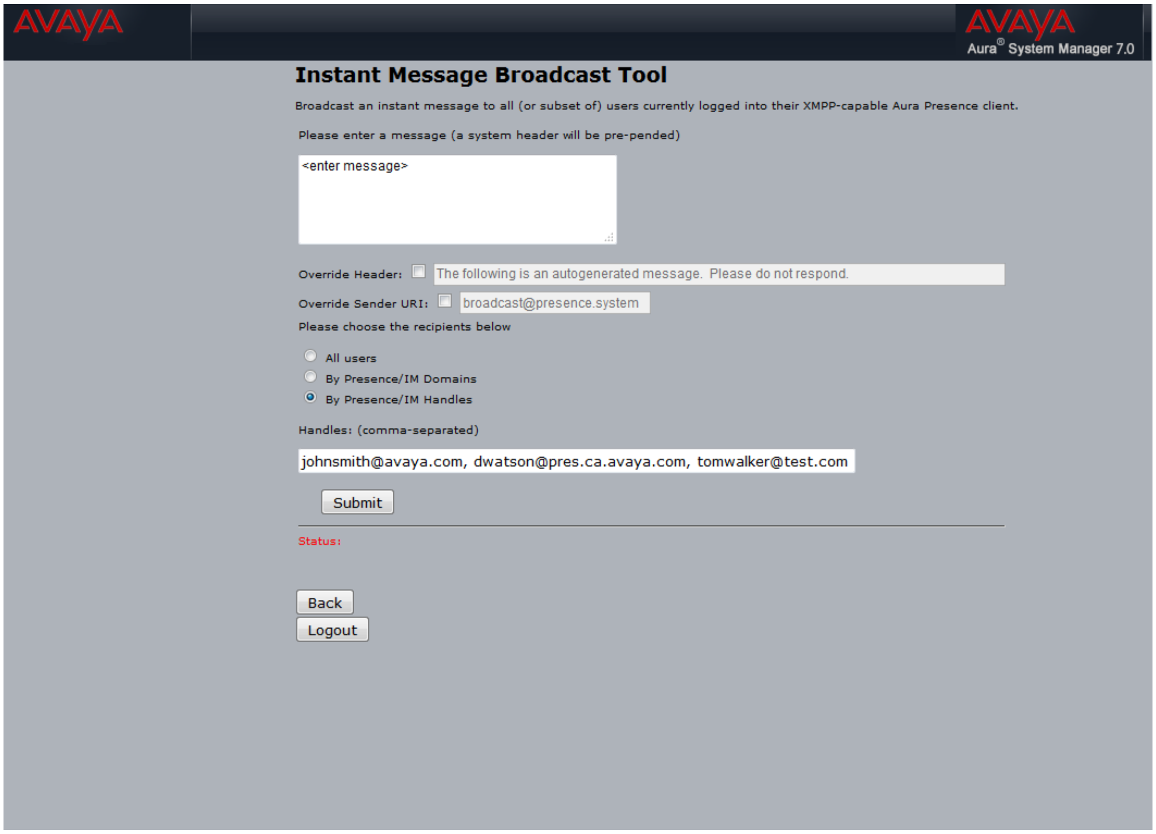
Domains: (multi-select)

[✓ avaya.com]
beta.ps.avaya.com
[✓ ca.avaya.com]
delta.ps.avaya.com
[✓ gamma.pslabb.com]
lacken.ps.avaya.com

Status:

- 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.



Instant Message Broadcast Tool

Broadcast an instant message to all (or subset of) users currently logged into their XMPP-capable Aura Presence client.

Please enter a message (a system header will be pre-pended)

<enter message>

Override Header: □ The following is an autogenerated message. Please do not respond.

Override Sender URI: □ broadcast@presence.system

Please choose the recipients below

○ All users
○ By Presence/IM Domains
● By Presence/IM Handles

Handles: (comma-separated)

johnsmith@avaya.com, dwatson@pres.ca.avaya.com, tomwalker@test.com

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:

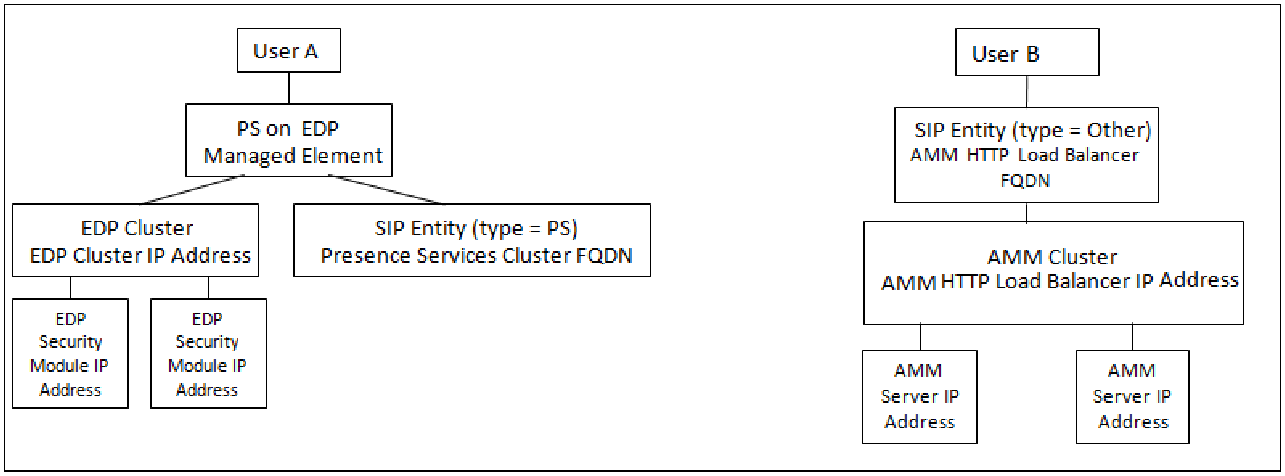
- If the user has an Instant Messaging device, then:
    - For Presence, administer the home Presence Services cluster of the user at **Users** > **User Management** > **Manage Users** > **Communication Profile** > **Presence Profile** > **System**.
    - For Messaging, administer the home Presence Services 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, 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.


User A
PS on EDP Managed Element
EDP Cluster EDP Cluster IP Address
SIP Entity (type = PS) Presence Services Cluster FQDN
EDP Security Module IP Address
EDP Security Module IP Address
User B
SIP Entity (type = Other) AMM HTTP Load Balancer FQDN
AMM Cluster AMM HTTP Load Balancer IP Address
AMM Server IP Address
AMM Server IP Address

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 17: 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 18: Checklist for administering Avaya Multimedia Messaging

No.	Task	Reference	✔
1	Administer DNS A record to resolve Avaya Breeze™ HTTP Load Balancer FQDN to Avaya Breeze™ Cluster IP Address.	—	
2	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 197	
3	Administer DNS A record to resolve Avaya Multimedia Messaging HTTP Load Balancer FQDN to Avaya Multimedia Messaging HTTP Load Balancer IP Address.	—	
4	Administer Avaya Multimedia Messaging SIP Entity.	Administering Avaya Multimedia Messaging SIP Entity on page 197	
5	Administer *x* users' home Avaya Multimedia Messaging Cluster.	Administering home Avaya Multimedia Messaging Cluster of the user on page 198	
6	Administer Avaya Breeze™ Cluster for Avaya Multimedia Messaging interoperability.	Administering Avaya Breeze Cluster for Avaya Multimedia Messaging interoperability on page 198	
7	Administer Avaya Multimedia Messaging Service Attributes.	Administering Avaya Multimedia Messaging Service Attributes on page 199	
8	Modify *y* Presence Services Security Module HTTPS identity certificates.	Modifying Presence Services Security Module HTTPS identity certificate on page 200	
9	Modify *y* Presence Services WebSphere identity certificates.	Modifying Presence Services WebSphere identity certificate on page 202	
10	Restart Presence Services.	Restarting Presence Services on page 233	

Table continues…

No.	Task	Reference	✔
11	Refer AMM reference documentation to setup federation with Presence Services.	—	

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 secure web communications** field.
8. Select the checkbox to the right of the Is **Load balancer enabled** field.

   You can select this field only when deploying two or more Presence Services nodes.
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**.

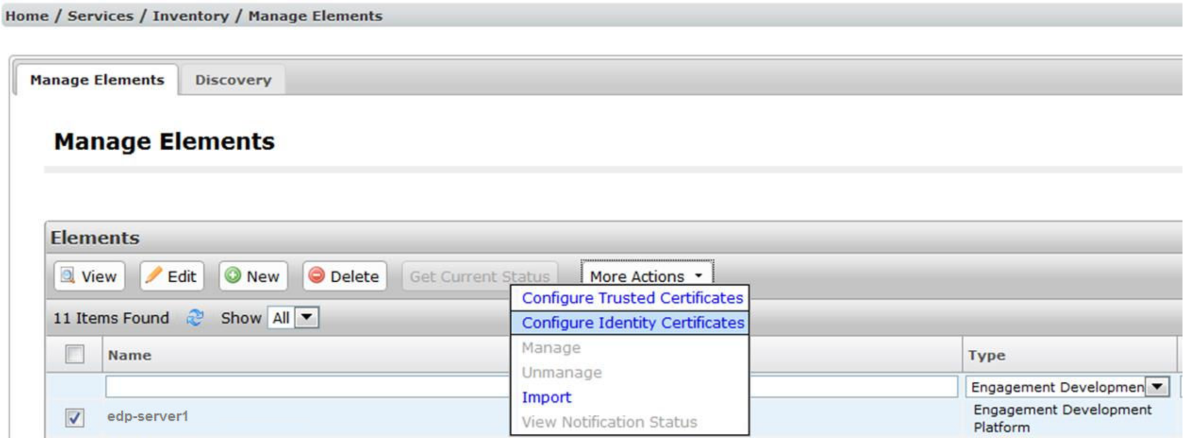
Modifying Presence Services Security Module HTTPS identity certificate

About this task

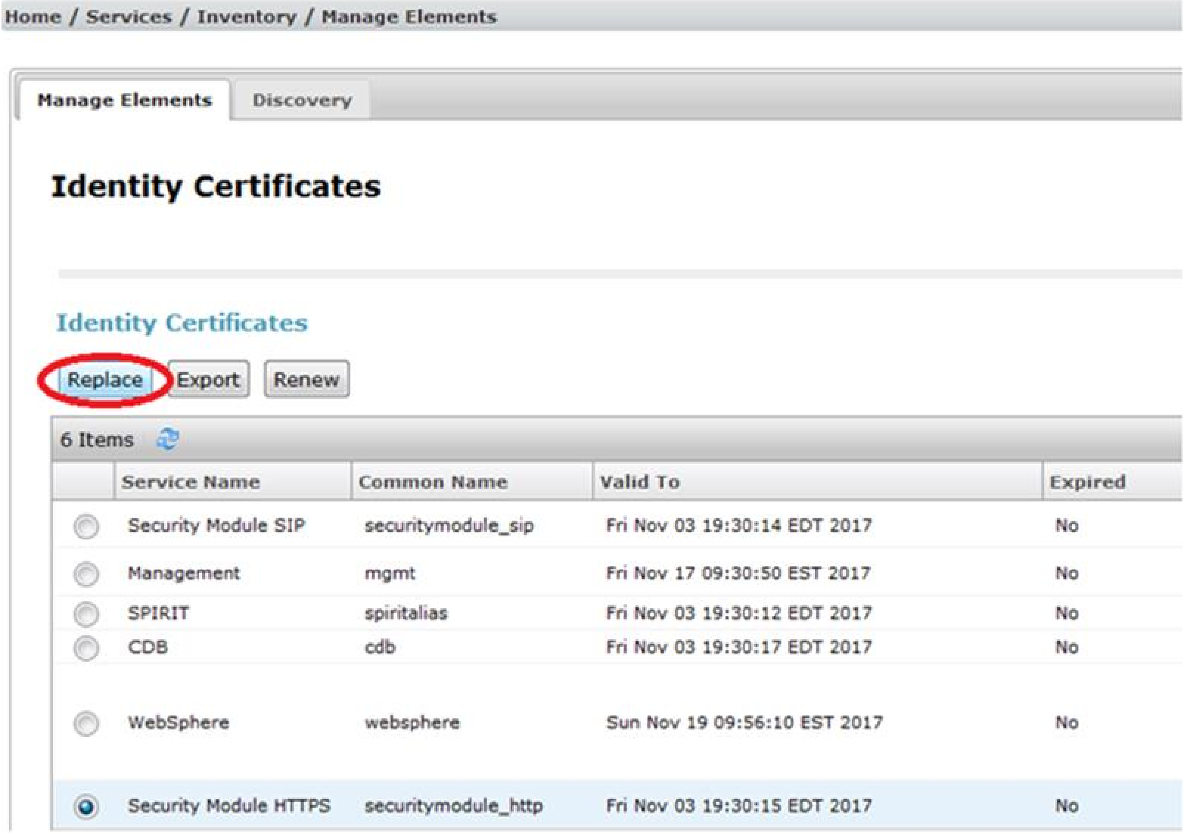
Perform the following procedure for each server in the Presence Services cluster.

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**.



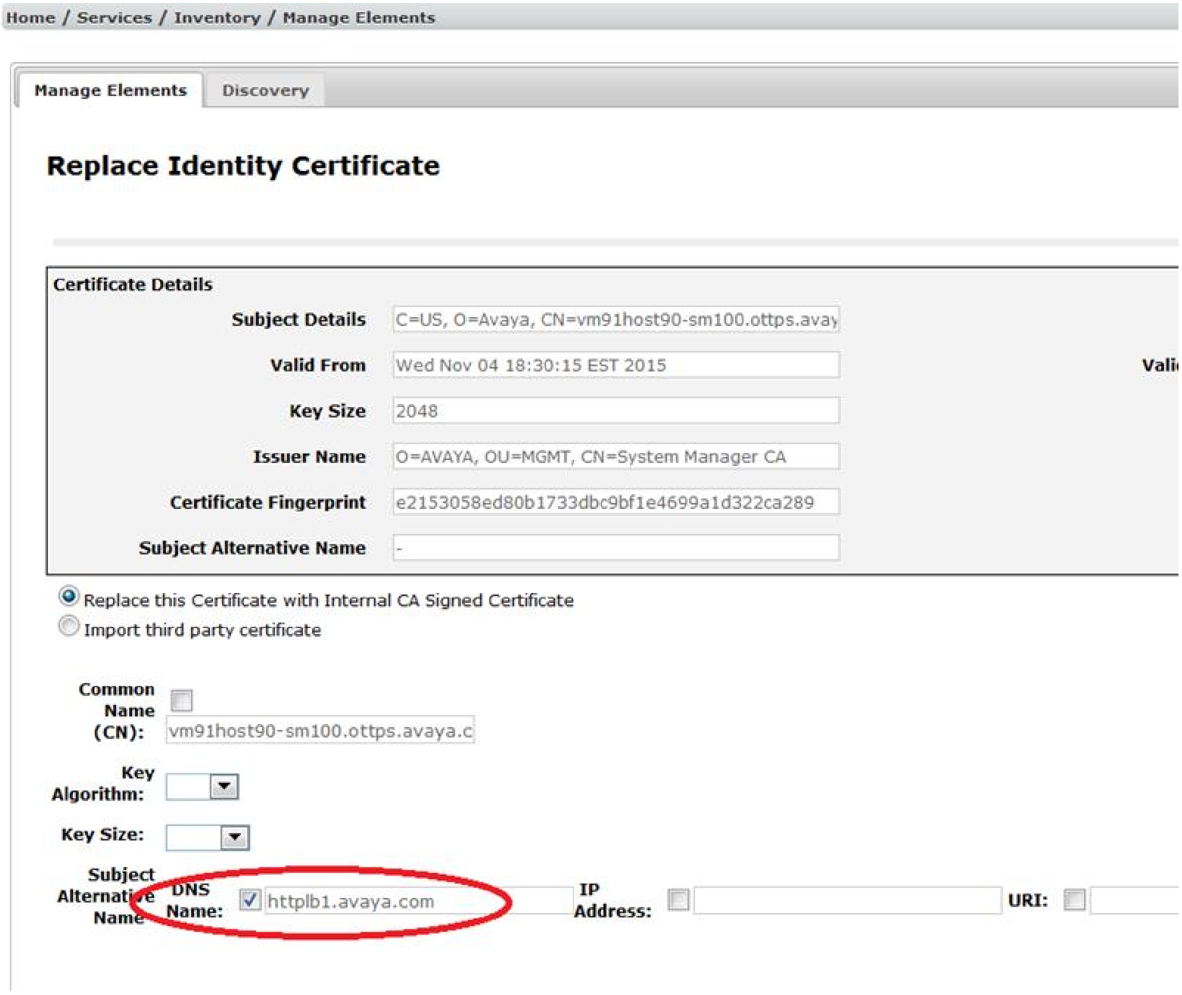
4. Select **Security Module HTTPS**, and click **Replace**.



	Service Name	Common Name	Valid To	Expired
○	Security Module SIP	securitymodule_sip	Fri Nov 03 19:30:14 EDT 2017	No
○	Management	mgmt	Fri Nov 17 09:30:50 EST 2017	No
○	SPIRIT	spiritalias	Fri Nov 03 19:30:12 EDT 2017	No
○	CDB	cdb	Fri Nov 03 19:30:17 EDT 2017	No
○	WebSphere	websphere	Sun Nov 19 09:56:10 EST 2017	No
●	Security Module HTTPS	securitymodule_http	Fri Nov 03 19:30:15 EDT 2017	No

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.



Home / Services / Inventory / Manage Elements

Manage Elements | Discovery

Replace Identity Certificate

Certificate Details

Subject Details	C=US, O=Avaya, CN=vm91host90-sm100.ottps.avay
Valid From	Wed Nov 04 18:30:15 EST 2015
Key Size	2048
Issuer Name	O=AVAYA, OU=MGMT, CN=System Manager CA
Certificate Fingerprint	e2153058ed80b1733dbc9bf1e4699a1d322ca289
Subject Alternative Name	-

● Replace this Certificate with Internal CA Signed Certificate

○ Import third party certificate

Common Name (CN): □ vm91host90-sm100.ottps.avaya.c

Key Algorithm:

Key Size:

Subject Alternative Name: DNS Name: ☑ httplb1.avaya.com IP Address: □ URI: □

6. Click **Commit**.
7. Restart Presence Services.

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

Modifying Presence Services WebSphere identity certificate

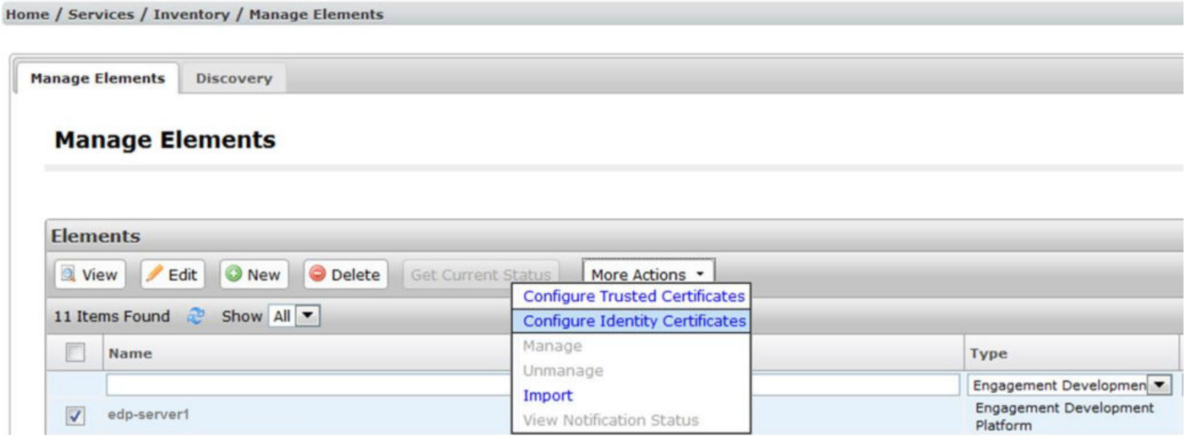
About this task

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

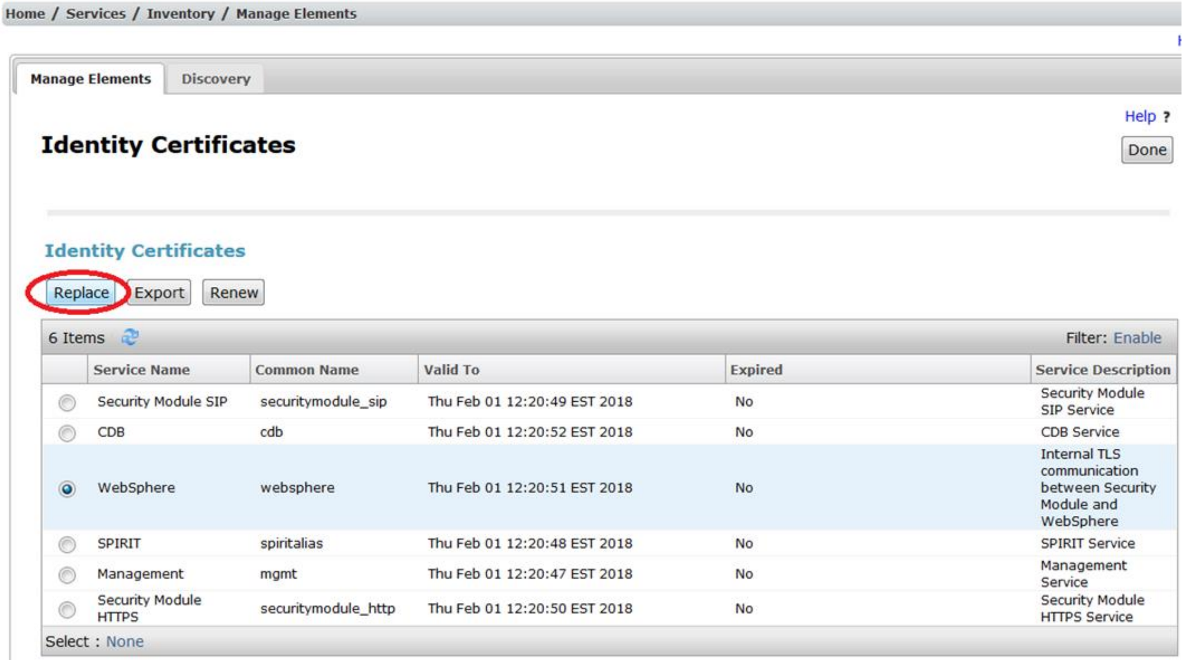
Procedure

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**.

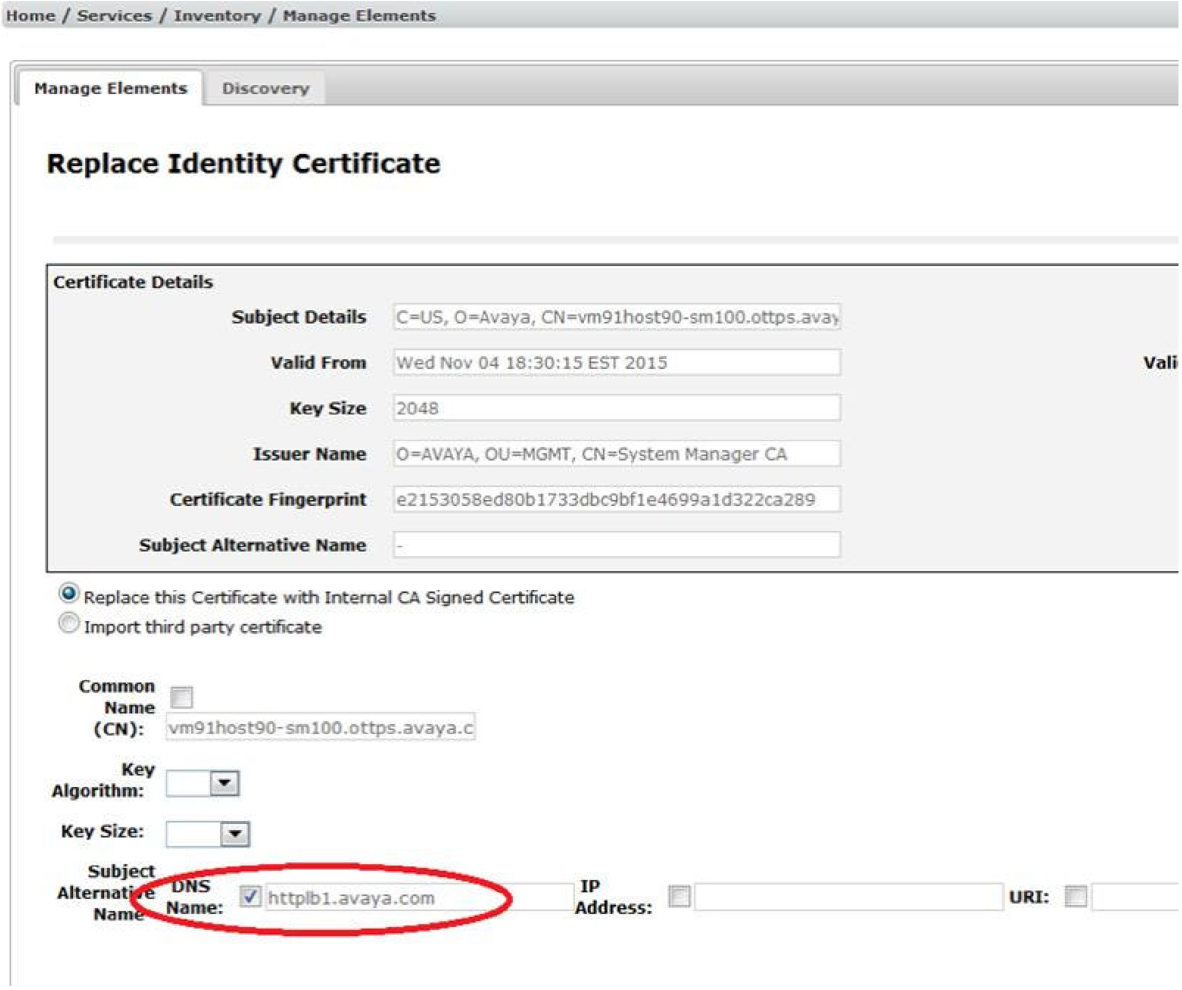


	Service Name	Common Name	Valid To	Expired	Service Description
○	Security Module SIP	securitymodule_sip	Thu Feb 01 12:20:49 EST 2018	No	Security Module SIP Service
○	CDB	cdb	Thu Feb 01 12:20:52 EST 2018	No	CDB Service
●	WebSphere	websphere	Thu Feb 01 12:20:51 EST 2018	No	Internal TLS communication between Security Module and WebSphere
○	SPIRIT	spiritalias	Thu Feb 01 12:20:48 EST 2018	No	SPIRIT Service
○	Management	mgmt	Thu Feb 01 12:20:47 EST 2018	No	Management Service
○	Security Module HTTPS	securitymodule_http	Thu Feb 01 12:20:50 EST 2018	No	Security Module HTTPS Service

Select : None

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.



Replace Identity Certificate

Certificate Details

Subject Details	C=US, O=Avaya, CN=vm91host90-sm100.ottps.avay
Valid From	Wed Nov 04 18:30:15 EST 2015
Key Size	2048
Issuer Name	O=AVAYA, OU=MGMT, CN=System Manager CA
Certificate Fingerprint	e2153058ed80b1733dbc9bf1e4699a1d322ca289
Subject Alternative Name	-

● Replace this Certificate with Internal CA Signed Certificate
○ Import third party certificate

Common Name (CN): □ vm91host90-sm100.ottps.avaya.c

Key Algorithm:

Key Size:

Subject Alternative Name: DNS Name: ☑ httplb1.avaya.com IP Address: □ URI: □

6. Click **Commit**.
7. Restart Presence Services.

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

Multi-User Chat

Presence Services can interoperate with Avaya Multimedia Messaging (AMM) and an external XMPP federation system, such as Openfire, to support XEP-0045 style Multi-User Chat between AMM-enabled users and external XMPP federation users. In this scenario, Presence Services acts as a gateway to exchange messaging between AMM and the external XMPP federated system.

For each FQDN of the conference service or multi-user chat URI hosted on the external XMPP federation system, add that FQDN to the appropriate XMPP Domain List Service Attribute. For more information, see “XMPP Federation” section.

For this feature to work, you must configure federation and AMM, and determine the following:

- For Multi-User Chat sessions hosted by AMM, determine the FQDNs of the conference services or Multi-User Chat URIs configured on AMM. For example, `muc.amm.avaya.com`.
- For Multi-User Chat sessions hosted by external XMPP federation system, determine the FQDNs of the conference services or Multi-User Chat URIs configured on the external system. For example, `conference.openfire.com`.

  Ensure that the Multi-User Chat URI is also added to the XMPP Federation domain list. For more information, see “Presence Services Service Attributes” table.
- Configure AMM according to their reference documentation.

Related links

Interoperability with Avaya Multimedia Messaging on page 193
Federation on page 83

Administering DNS SRV records to resolve Avaya Multimedia Messaging conference services

Procedure

1. On the DNS server used by the external XMPP federation system, create a DNS SRV record with the following values:
   - **Domain**: Enter the AMM conference service FQDN.
   - **Service**: Enter `_xmpp-server`.
   - **Protocol**: Enter `_tcp`.
   - **Priority**: Assign any value.
   - **Weight**: Assign any value.
   - **Port Number**: Enter `5269`.
   - **Host offering this service**: Enter the Presence Services Cluster FQDN. See “Table 1: Key customer configuration information”.
2. On the DNS server used by Presence Services, create a DNS SRV record with the following values:
   - **Domain**: Enter the AMM conference service FQDN.
   - **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 AMM HTTP Load Balancer FQDN. See “Table 1: Key customer configuration information”.

3. Repeat Step 1 and 2 for each AMM conference services or Multi-User Chat URI configured on AMM.

Administering DNS SRV records to resolve external XMPP federation system conference services

Procedure

1. On the DNS server used by Presence Services, create a DNS SRV record with the following values:
   - **Domain**: Enter the external XMPP system's conference service URI.
   - **Service**: Enter `_xmpp-server`.
   - **Protocol**: Enter `_tcp`.
   - **Priority**: Assign any value.
   - **Weight**: Assign any value.
   - **Port Number**: Enter `5269`.
   - **Host offering this service**: External XMPP federation server IP or FQDN. See "Table 1: Key customer configuration information".
2. Repeat Step 1 for each AMM conference services or Multi-User Chat URI configured on AMM.

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.

Inter-Tenant Presence and IM

By default, Presence Services prevents presence and IM from being shared between tenants. You can allow presence and IM between tenants by enabling the System attribute **Enable Inter-Tenant Presence and IM**. Changing this attribute does not require a restart of Presence Services.

Related links

Configuring Inter-Tenant Presence and IM on page 207

Configuring Inter-Tenant Presence and IM

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-Tenant Presence and IM** field:
   - To enable Inter-Tenant Presence and IM, select **Override Default**, and select the check box in the **Effective Value** field.

- To disable Inter-Tenant Presence and IM, select **Override Default**, and clear the check box in the **Effective Value** field.

7. Click **Commit**.

Related links

Inter-Tenant Presence and IM on page 207

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. **(Optional)** In the **Message Archiving Remote Path** field within the Instant Messaging group, enter the sub-directory name on the remote SFTP server where Presence Services must transfer the IMs.

   Note:

   The value entered is relative to the home folder of the user and is not an absolute path. The sub-directory will be only one level under user's home. If left blank, 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*.

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 Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route

About this task

The administrator needs to configure the Presence Services cluster as a trusted application pool that can be referred to in a Front End static route and a trusted application definition.

Procedure

1. On Lync Front End server, run **Lync Server Management Shell** and on Skype for Business Front End server, run **Skype for Business Server Management Shell**.
2. Create a trusted application pool.

3. Use the new `New-CsTrustedApplicationPool cmdlet` to create a trusted application pool `sc-8209-cl-03.avaya.com` to host the trusted application.

   ```
   New-CsTrustedApplicationPool -Identity sc-8209-cl-03.avaya.com  -Registrar
   Registrar:lync2013-fe.bvwlab.com  -Site 1  -ComputerFqdn sc-8205-sm100.avaya.com -
   ThrottleAsServer $true -TreatAsAuthenticated $true -RequiresReplication $false
   ```

   For more information see help of the **`New-CsTrustedApplicationPool cmdlet`**

   -*Identity* is the FQDN of the new pool and it is the Avaya Breeze™ cluster FQDN

   -*Registrar* is the FQDN of the Front End pool to which this trusted application pool belongs.

   You can find the Register parameter with **`cmdlet Get-CsPool | Where-Object {$_.Services -match "Registrar:"}`**

   -*Site* is the Site ID to which this trusted application pool belongs; use Get-CsSite cmdlet to retrieve the SiteId.

   -*ComputerFqdn* defines the FQDN of the first Breeze server Security Module FQDN in the trusted application pool.

4. Add other Avaya Breeze node to the trusted application pool for multi-nodes cluster setup:
5. Use the **`New-CsTrustedApplicationComputer cmdlet`** to add other other Breeze server(s) to the trusted application pool.

   ```
   New-CsTrustedApplicationComputer -Identity sc-8215-sm100.avaya.com -Pool sc-8209-
   cl-03.avaya.com
   ```

   -*Identity* is Breeze server Security Module FQDNof the 2nd node. (For single node cluster, skip this step).

   -*Pool* is the trusted application pool defined in step 2.

   By adding all Avaya Breeze nodes to the trusted application pool, it provides load-balanced setup for the Presence/IM services from all the hosts.

6. Repeat this step for each node in a multi-node cluster.

   Note:

   When creating a trusted application pool (and trusted application computer) in this way, Lync/Skype for Business will issue a warning:

   Warning:

   Machine xxx from the topology you are publishing was not found in Active Directory and will result in errors during Enable-CsTopology as it tries to prepare Active Directory entries for the topology machines.

   This warning can be safely ignored as the Breeze nodes are not domain joined in Microsoft Active Directory, and you should answer “Yes” to this warning.

7. Create a trusted application representing Presence Services:

8. Use the **`New-CsTrustedApplication cmdlet`** to create a trusted application represents the Presence Services.

   ```
   New-CsTrustedApplication -ApplicationID edps -TrustedApplicationPoolFqdn sc-8209-
   cl-03.avaya.com -Port 5063
   ```

   -ApplicationID is friendly identifier for the trusted application

   -TrustedApplicationPoolFqdn is the trusted application pool created in step 2.

9. Create a static route for Aura Presence/IM domain routing and associate this route with trusted application pool:

10. Use the **`New-CsStaticRoute & Set-CsStaticRoutingConfiguration cmdlets`** to create Static Route associated with global routing table.

    ```
    $newstaticroute = New-CsStaticRoute -TLSRoute -Destination sc-8209-
    cl-03.avaya.com -Port 5063 -MatchUri bvwlab.com -UseDefaultCertificate $true
    Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$newstaticroute}
    ```

    -TLSRoute defines that the static route we are creating will use SIP TLS transport.

    -Destination is the Destination is the FQDN of the next hop server for routing Presence/IM messages.

    In this example, the routing destination is the Avaya Breeze cluster FQDN.

    -Port is the Presence Service port for federation, default is 5063.

    -MatchUri is the domain suffix used to determine if the Presence/IM message is being sent to an Aura user handled by this route. In this example, Lync or Skype client watching Aura client aura-user@bvwlab.com will use the defined static route, sending to destination at FQDN `sc-8209-cl-03.avaya.com`.

    Note:

    Microsoft Federation supports a shared domain setup, in which the Microsoft domain can be the same as Aura Presence/IM domain. In this shared domain configuration, Lync or Skype for Business will only send Presence/IM requests to Aura client which is not defined as Lync or Skype client. And Microsoft Federation also supports different domains between MS domain and Aura Presence/IM domain. If static routes for additional domains are required, re-run the two cmdlets above, substituting the -MatchUri parameter with desired Aura Presence/IM domain name.

11. Enable the new Topology.

12. Use the **`-Enable-CsTopology cmdlet`** to enable the newly create topology. The **`cmdlet`** has no passed parameter.

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 233

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**.

Network Management System configuration

This section describes how to setup a third-party Network Management System (NMS) to receive alarms from a Avaya Breeze™ platform running Presence Services. In this document, OpenNMS is used. OpenNMS is an enterprise grade network management platform developed in the open source model. For more information, refer to https://www.opennms.org/en.

The following sections describe how to:

- Configure System Manager.
- Install and configure OpenNMS.
- Test the setup by generating test alarms on a Avaya Breeze™ server and receiving them as events on OpenNMS.

Related links

Configuring System Manager on page 218
Exporting the MIB file on page 221
Installing OpenNMS on page 223
Starting OpenNMS on page 225
Configuring Linux firewall on page 226
Accessing the OpenNMS web console on page 226
Importing MIB files into OpenNMS on page 226
Modifying OpenNMS event definitions on page 228
Creating OpenNMS node elements on page 229
Testing the OpenNMS installation on page 230
Viewing the Alarm events in OpenNMS on page 231

Configuring System Manager

About this task

System Manager is used to configure the SNMP Agent on Avaya Breeze™. The following procedure shows how to configure the Serviceability Agent on System Manager to enable Avaya Breeze™ to send SNMP alarms (traps) to OpenNMS.

Procedure

1. Configure an SNMP target v2 profile.

   Note:

   A user profile is not required for a v2 target profile.

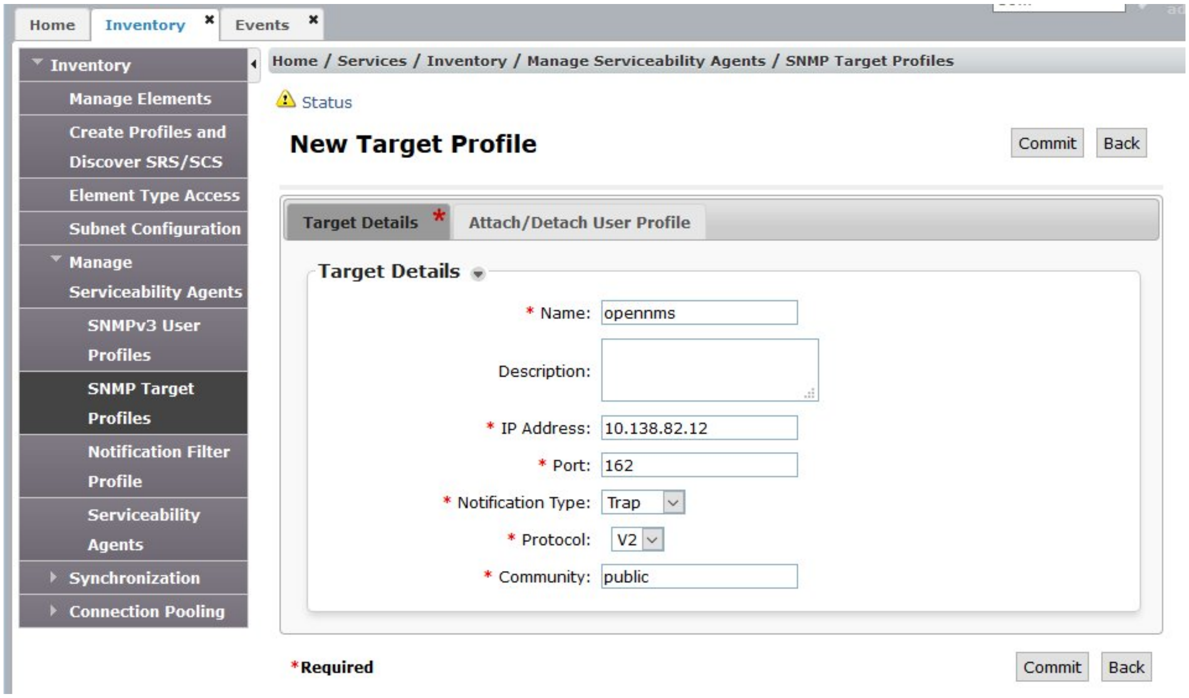
   a. On System Manager, navigate to **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.

   b. Click **New**.

c. Fill in the following details:

  - **Name**: Enter a name.
  - **Description**: Enter a short description.
  - **IP Address**: Enter the IP address of the openNMS server.
  - **Port**: Enter a port number.
  - **Notification Type**: Select **trap**.
  - **Protocol**: Select **v2**.
  - **Community**: Select **public**.

d. Click **Commit**.



Home / Services / Inventory / Manage Serviceability Agents / SNMP Target Profiles

New Target Profile

Target Details

* Name: opennms

Description:

* IP Address: 10.138.82.12

* Port: 162

* Notification Type: Trap

* Protocol: V2

* Community: public

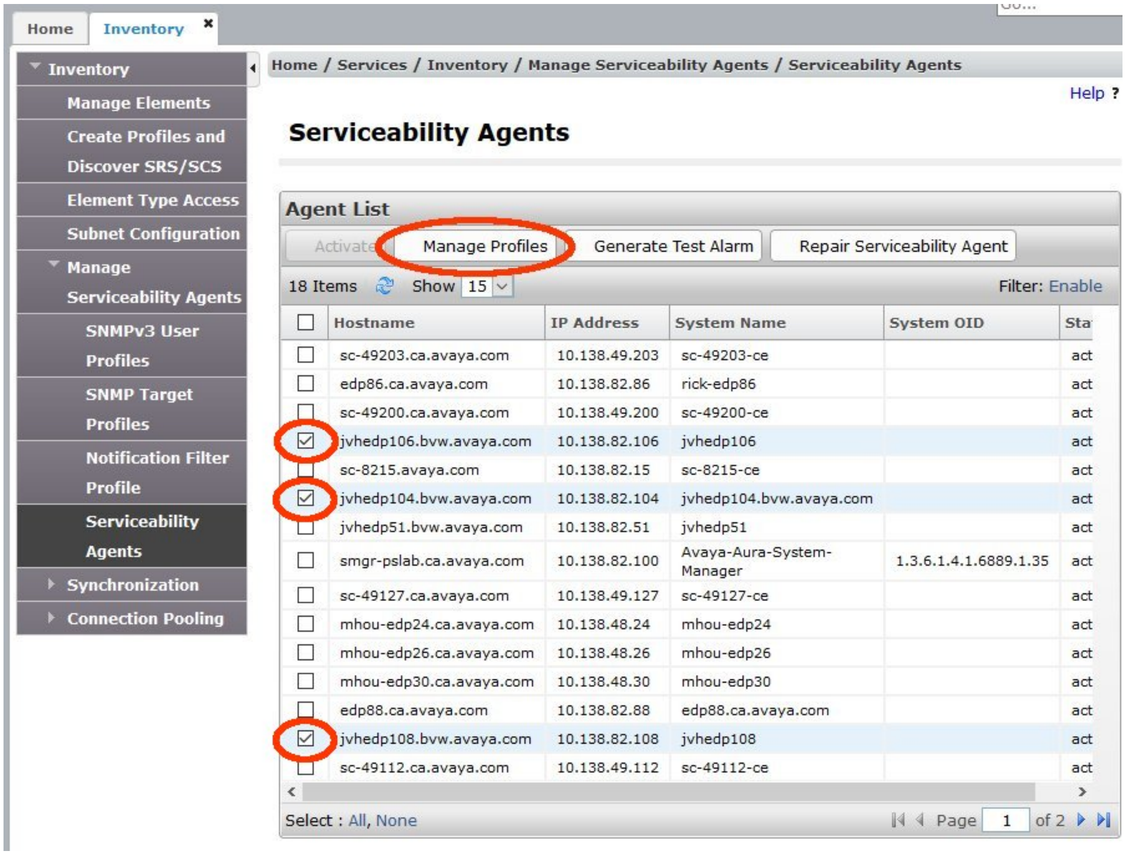
*Required

2. Configure the Serviceability Agent.

   a. On System Manager, navigate to **Inventory** > **Manage Serviceability Agents**.

   b. Select the Avaya Breeze™ hostname or multiple hosts that form a Avaya Breeze™ cluster from the list of serviceability agents.

c. Once all the servers are selected, click the **Mange Profiles** button.



□	Hostname	IP Address	System Name	System OID	Sta
□	sc-49203.ca.avaya.com	10.138.49.203	sc-49203-ce		act
□	edp86.ca.avaya.com	10.138.82.86	rick-edp86		act
□	sc-49200.ca.avaya.com	10.138.49.200	sc-49200-ce		act
☑	jvhedp106.bvw.avaya.com	10.138.82.106	jvhedp106		act
□	sc-8215.avaya.com	10.138.82.15	sc-8215-ce		act
☑	jvhedp104.bvw.avaya.com	10.138.82.104	jvhedp104.bvw.avaya.com		act
□	jvhedp51.bvw.avaya.com	10.138.82.51	jvhedp51		act
□	smgr-pslab.ca.avaya.com	10.138.82.100	Avaya-Aura-System-Manager	1.3.6.1.4.1.6889.1.35	act
□	sc-49127.ca.avaya.com	10.138.49.127	sc-49127-ce		act
□	mhou-edp24.ca.avaya.com	10.138.48.24	mhou-edp24		act
□	mhou-edp26.ca.avaya.com	10.138.48.26	mhou-edp26		act
□	mhou-edp30.ca.avaya.com	10.138.48.30	mhou-edp30		act
□	edp88.ca.avaya.com	10.138.82.88	edp88.ca.avaya.com		act
☑	jvhedp108.bvw.avaya.com	10.138.82.108	jvhedp108		act
□	sc-49112.ca.avaya.com	10.138.49.112	sc-49112-ce		act

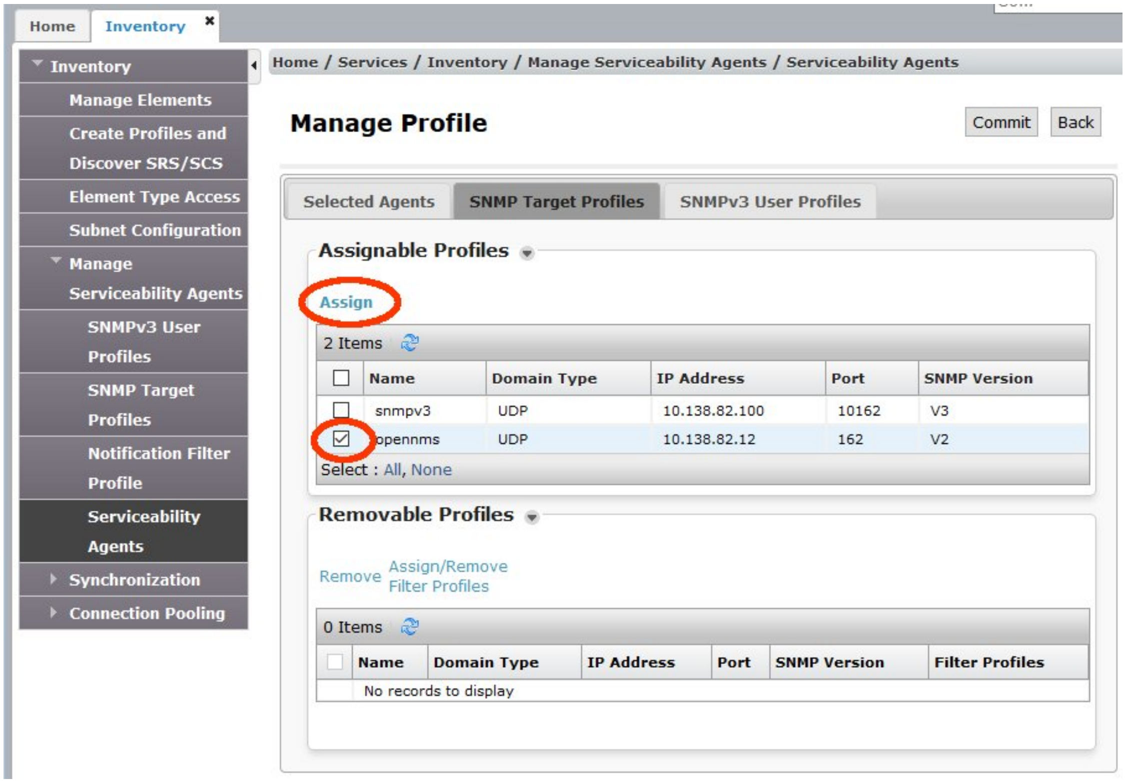
d. Select the **SNMP Target Profiles** tab.

e. Select the target profile configured earlier from the **Assignable Profiles**.

f. Click on the blue **Assign** button to make the profile to agent assignment.

The system moves the profile from the Assignable list to the Removable list.

g. Click **Commit**.



	Name	Domain Type	IP Address	Port	SNMP Version
☐	snmpv3	UDP	10.138.82.100	10162	V3
☑	opennms	UDP	10.138.82.12	162	V2

	Name	Domain Type	IP Address	Port	SNMP Version	Filter Profiles
	No records to display					

Related links

Network Management System configuration on page 218

Exporting the MIB file

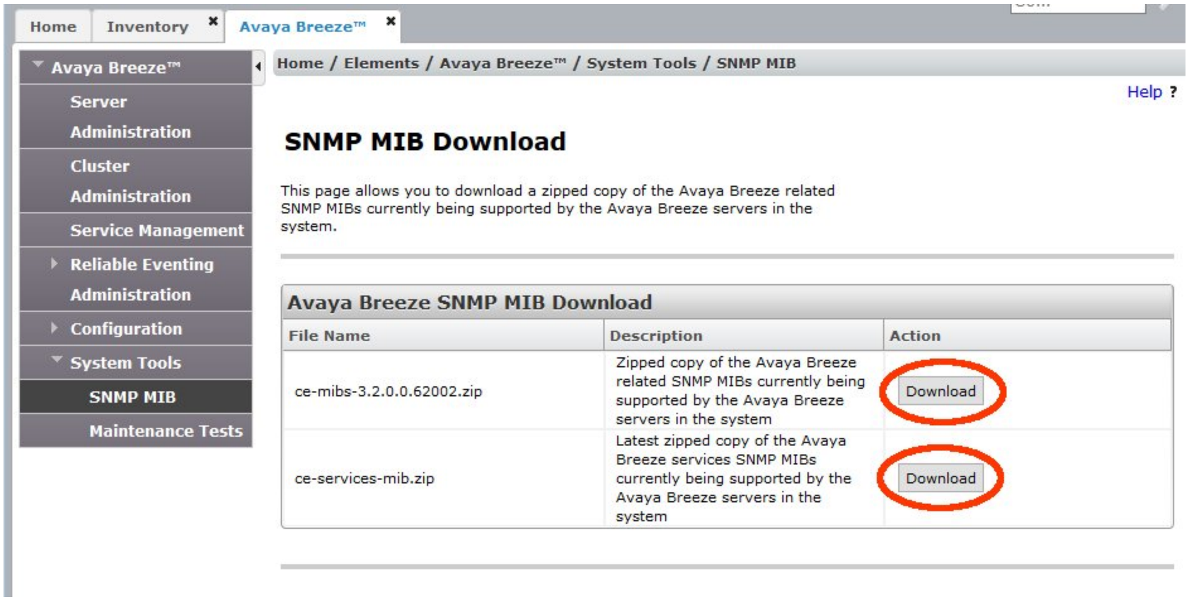
About this task

Management Information Base (MIB) files are used to describe the contents of the alarms or traps. These files define the Object Identifiers (OIDs) and data types used to build SNMP alarm messages. Some NMS systems require a complete specification of all the OIDs used for all alarm messages that a target system could generate. However, OpenNMS does not have this restriction. The following procedure describes how to retrieve all the MIBs to define every OID that could be sent from a Avaya Breeze™ platform running Presence Services.

Procedure

1. On the System Manager web interface, navigate to **Elements** > **Avaya Breeze™**.
2. Click **System Tools** > **SNMP MIB**.

3. Click **Download** next to the `ce-mibs-xxx.zip` and the `ce-services-mib.zip` files.



SNMP MIB Download

This page allows you to download a zipped copy of the Avaya Breeze related SNMP MIBs currently being supported by the Avaya Breeze servers in the system.

Avaya Breeze SNMP MIB Download

File Name	Description	Action
ce-mibs-3.2.0.0.62002.zip	Zipped copy of the Avaya Breeze related SNMP MIBs currently being supported by the Avaya Breeze servers in the system	Download
ce-services-mib.zip	Latest zipped copy of the Avaya Breeze services SNMP MIBs currently being supported by the Avaya Breeze servers in the system	Download

You need to extract the following two files:

- `opt/Avaya/AUS/snapin-alarms/avaya-products-PresenceServices.my`
- `SNAPIN-VARBIND/EDP-Snapin-var-bind-mib.my`

```
$ unzip -l ce-services-mib.zip
Archive:  ce-services-mib.zip
  Length      Date    Time    Name
 --------    ----    ----    ----
     8175  06-03-16 11:18   opt/Avaya/AUS/snapin-alarms/Avaya-products-
EngagementDesigner.my
     8194  07-13-16 17:24   opt/Avaya/AUS/snapin-alarms/CEServices-CommonAlarmDef-
Data.my
     8221  09-22-16 15:11   opt/Avaya/AUS/snapin-alarms/avaya-products-
PresenceServices.my
 --------                   -------
    32777                   4 files
$ unzip -l ce-mibs-3.2.0.0.62002.zip
Archive:  ce-mibs-3.2.0.0.62002.zip
  Length      Date    Time    Name
 --------    ----    ----    ----
        0  06-29-16 12:07   CE/
    10709  06-29-16 12:07   CE/CE-CommonAlarmDef-Data.my
     4486  06-29-16 12:07   CE/SmSecMod-CommonAlarmDef-Data.my
     3910  06-29-16 12:07   CE/CeThirdPrty-CommonAlarmDef-Data.my
        0  06-29-16 12:07   CEELEM/
     3863  06-29-16 12:07   CEELEM/CEELEM-CommonAlarmDef-Data.my
        0  06-29-16 12:07   STANDARD/
    54084  06-29-16 12:02   STANDARD/HOST-RESOURCES-MIB.my
    29349  06-29-16 12:02   STANDARD/Tcp-mib.my
    30159  06-29-16 12:02   STANDARD/SNMPv2-MIB.my
    73505  06-29-16 12:02   STANDARD/If-mib.my
    21431  06-29-16 12:02   STANDARD/Udp-mib.my
     5577  06-29-16 12:02   STANDARD/INADS-MIB.my
    46150  06-29-16 12:02   STANDARD/UCD-SNMP-MIB.my
        0  06-29-16 12:07   SNAPIN-VARBIND/
     5498  06-29-16 12:02   SNAPIN-VARBIND/EDP-Snapin-var-bind-mib.my
 ---------                    --------
   288721                     16 files
```

4. You must download the third MIB file `Avaya_Aura_ServicabilityAgent_Mib.my` from the Avaya support site:
    a. Navigate to https://support.avaya.com/.
    b. Search with the string `snmp white paper`.

       The system displays several versions of the *System Manager SNMP White Paper* document.
    c. Download the appropriate version and find the Serviceability Agent MIB file attached in the appendix of the document.

    These three MIB files provide a complete description of all the OIDs used by the alarms that are generated by Presence Services running on the Avaya Breeze™ platform. OpenNMS only requires the `avaya-products-PresenceServices.my` MIB file to be imported.

Related links

Network Management System configuration on page 218

Installing OpenNMS

About this task

OpenNMS can be installed on Windows or Linux platform types. Refer to the installation documentation on the OpenNMS website for more details: https://docs.opennms.org/opennms/releases/latest/guide-install/guide-install.html.

Before you begin

The following are the prerequisites for installing OpenNMS:

- Oracle Java SE Development Kit 8. OpenJDK is not recommended for production.
- PostgrresSQL 9.1 or later.
- Configured yum package manager.

Installing OpenNMS with the yum package manager will ensure that all the pre-requisites are installed.

Procedure

1. Download the OpenNMS repository file and install the packages as follows:

   You must run the installation as the root user.

```
# rpm -Uvh http://yum.opennms.org/repofiles/opennms-repo-stable-rhel6.noarch.rpm
# yum install opennms
. . .
. . .
Installed:
  opennms.noarch
0:18.0.2-1
```

```
Dependency Installed:
  jdk1.8.0_60.x86_64 2000:1.8.0_60-fcs
  jicmp.x86_64 0:1.4.5-2
  jicmp6.x86_64 0:1.2.4-1
  opennms-core.noarch 0:18.0.2-1
  opennms-webapp-jetty.noarch 0:18.0.2-1

Complete!
```

Note:

In this example, the Postgres database is already installed.

2. Use the following commands to prepare the database.

```
# service postgresql-9.1 initdb            # initialize the DB
# chkconfig postgresql-9.1 on              # enable DB server on system startup
# service postgresql-9.1 start             # start the DB server
```

3. Enter the following postgres command to create a database user for OpenNMS to use.

```
# su - postgres
-bash-4.1$ createuser -P opennms
Enter password for new role:  opennms
Enter it again: opennms
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create databases? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
-bash-4.1$ createdb -O opennms opennms
-bash-4.1$ exit
```

4. Modify the password for the Postgres super user account.

```
# su - postgres
-bash-4.1$ psql -c "ALTER USER postgres WITH PASSWORD 'opennms18';"
ALTER ROLE
-bash-4.1$ exit
```

5. Modify the postgres configuration for OpenNMS access over the local network.

    a. Navigate to `/var/lib/pgsql/9.1/data/`.

    b. Update the `pg_hba.conf` file as follows:

    From:

    ```
    #host    replication     postgres        127.0.0.1/32            ident
    #host    replication     postgres        ::1/128                 ident
    ```

    To:

    ```
    host    all             all             127.0.0.1/32            md5
    host    all             all             ::1/128                 md5
    ```

6. Restart the postgres server.

```
# service postgresql-9.1 restart
Stopping postgresql-9.1 service:                            [  OK  ]
Starting postgresql-9.1 service:                            [  OK  ]
```

7. Modify the OpenNMS database access configuration file using the passwords created earlier.

```
# vi /opt/opennms/etc/opennms-datasources.xml
<jdbc-data-source name="opennms"
```

```
                    database-name="opennms"
                    class-name="org.postgresql.Driver"
                    url="jdbc:postgresql://localhost:5432/opennms"
                    user-name="opennms"
                    password="opennms"/>
<jdbc-data-source name="opennms-admin"
                    database-name="template1"
                    class-name="org.postgresql.Driver"
                    url="jdbc:postgresql://localhost:5432/template1"
                    user-name="postgres"
                    password="opennms18"/>
```

Related links

[Network Management System configuration](#) on page 218

Starting OpenNMS

Procedure

1. Initialize and start OpenNMS.

```
# /opt/opennms/bin/runjava -s
# /opt/opennms/bin/install -dis
# service opennms start
Starting OpenNMS:                                         [  OK  ]
```

2. Verify that all the OpenNMS internal components are up and running.

```
# cd /opt/opennms/bin/
# ./opennms -v status
OpenNMS.Eventd         : running
OpenNMS.Trapd          : running
OpenNMS.Queued         : running
OpenNMS.Actiond        : running
OpenNMS.Notifd         : running
OpenNMS.Scriptd        : running
OpenNMS.Rtcd           : running
OpenNMS.Pollerd        : running
OpenNMS.PollerBackEnd  : running
OpenNMS.EnhancedLinkd  : running
OpenNMS.Ticketer       : running
OpenNMS.Collectd       : running
OpenNMS.Discovery      : running
OpenNMS.Vacuumd        : running
OpenNMS.EventTranslator: running
OpenNMS.PassiveStatusd : running
OpenNMS.Statsd         : running
OpenNMS.Provisiond     : running
OpenNMS.Reportd        : running
OpenNMS.Bsmd           : running
OpenNMS.Alarmd         : running
OpenNMS.Ackd           : running
OpenNMS.JettyServer    : running
opennms is running
```

Related links

[Network Management System configuration](#) on page 218

Configuring Linux firewall

Procedure

If your OpenNMS server platform is using a firewall, you must open the following ports:

- UDP 162: For receiving alarms or traps.
- TCP 8980: For accessing the OpenNMS web console.

Related links

Network Management System configuration on page 218

Accessing the OpenNMS web console

Procedure

1. You can access OpenNMS web console through `http://`*`<IP-or-FQDN-of - OpenNMS-server>`*`:8980/opennms`.
2. Use this user interface to configure OpenNMS and manage or monitor network devices called nodes.

   The default username and password used to login to the web console is admin/admin.

Related links

Network Management System configuration on page 218

Importing MIB files into OpenNMS

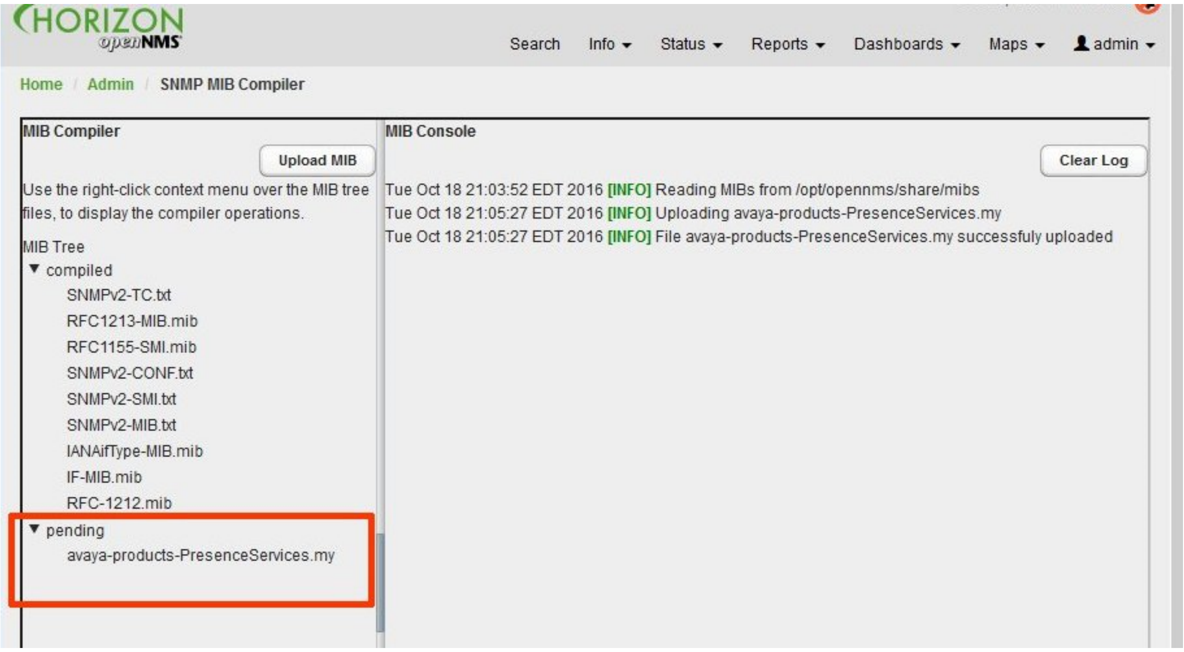
About this task

The exported MIB files must be imported into OpenNMS to interpret incoming SNMP alarms and convert them into OpenNMS events. Use the following steps to import the required MIB files.

Procedure

1. On the OpenNMS web console, navigate to **admin** > **Configure OpenNMS**.
2. In **Additional Tools**, click **SNMP MIB Compiler**.
3. Click **Upload MIB**, and select the `avaya-products-PresenceServices.my` MIB file for uploading.

   The system loads the MIB file into the pending area.

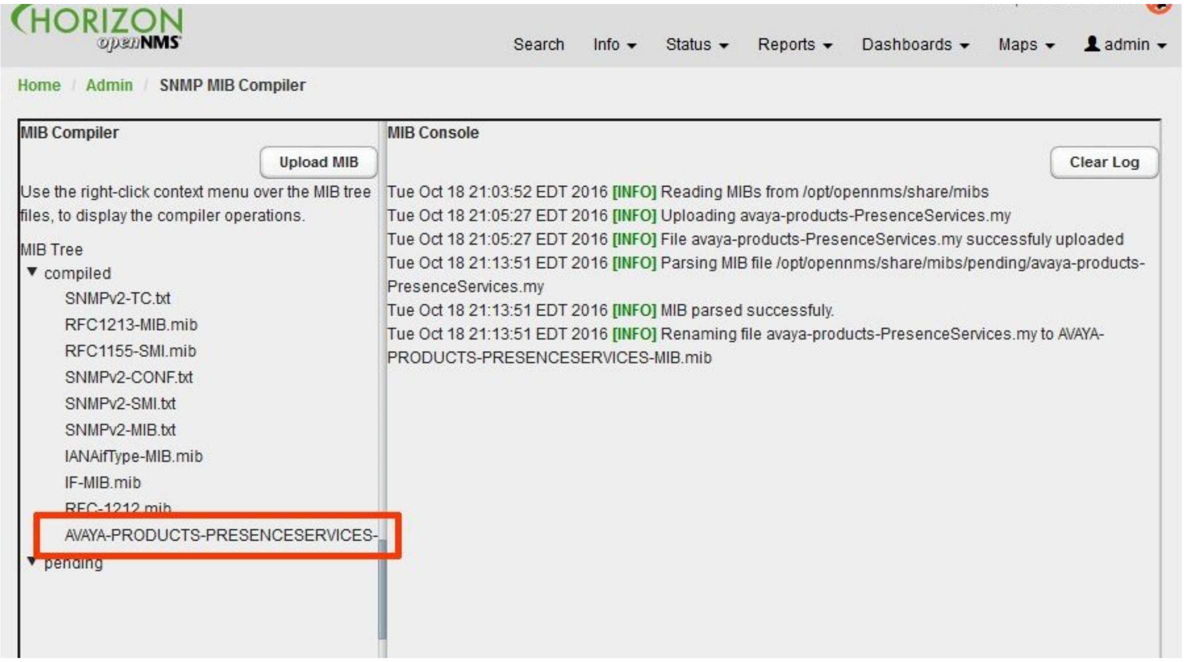


Use the right-click context menu over the MIB tree files, to display the compiler operations.

```
Tue Oct 18 21:03:52 EDT 2016 [INFO] Reading MIBs from /opt/opennms/share/mibs
Tue Oct 18 21:05:27 EDT 2016 [INFO] Uploading avaya-products-PresenceServices.my
Tue Oct 18 21:05:27 EDT 2016 [INFO] File avaya-products-PresenceServices.my successfuly uploaded
```

4. Right-click the `avaya-products-PresenceServices.my` file in the pending list and select **Compile MIB**.

   The MIB file will now appear in the MIB compiled tree.



Use the right-click context menu over the MIB tree files, to display the compiler operations.

```
Tue Oct 18 21:03:52 EDT 2016 [INFO] Reading MIBs from /opt/opennms/share/mibs
Tue Oct 18 21:05:27 EDT 2016 [INFO] Uploading avaya-products-PresenceServices.my
Tue Oct 18 21:05:27 EDT 2016 [INFO] File avaya-products-PresenceServices.my successfuly uploaded
Tue Oct 18 21:13:51 EDT 2016 [INFO] Parsing MIB file /opt/opennms/share/mibs/pending/avaya-products-
PresenceServices.my
Tue Oct 18 21:13:51 EDT 2016 [INFO] MIB parsed successfuly.
Tue Oct 18 21:13:51 EDT 2016 [INFO] Renaming file avaya-products-PresenceServices.my to AVAYA-
PRODUCTS-PRESENCESERVICES-MIB.mib
```

5. Right-click the `avaya-products-PresenceServices.my` file in the compiled list and select **Generate Events**.
6. Click **Save Events File**.

The system creates an OpenNMS event definition file for all Presence Services alarms defined in the MIB file.

Related links

Network Management System configuration on page 218

Modifying OpenNMS event definitions

About this task

The MIB compiler does not translate alarm severity or alarm parameters into the proper format for OpenNMS. You must edit each event to make it more usable and presentable in OpenNMS.

Procedure

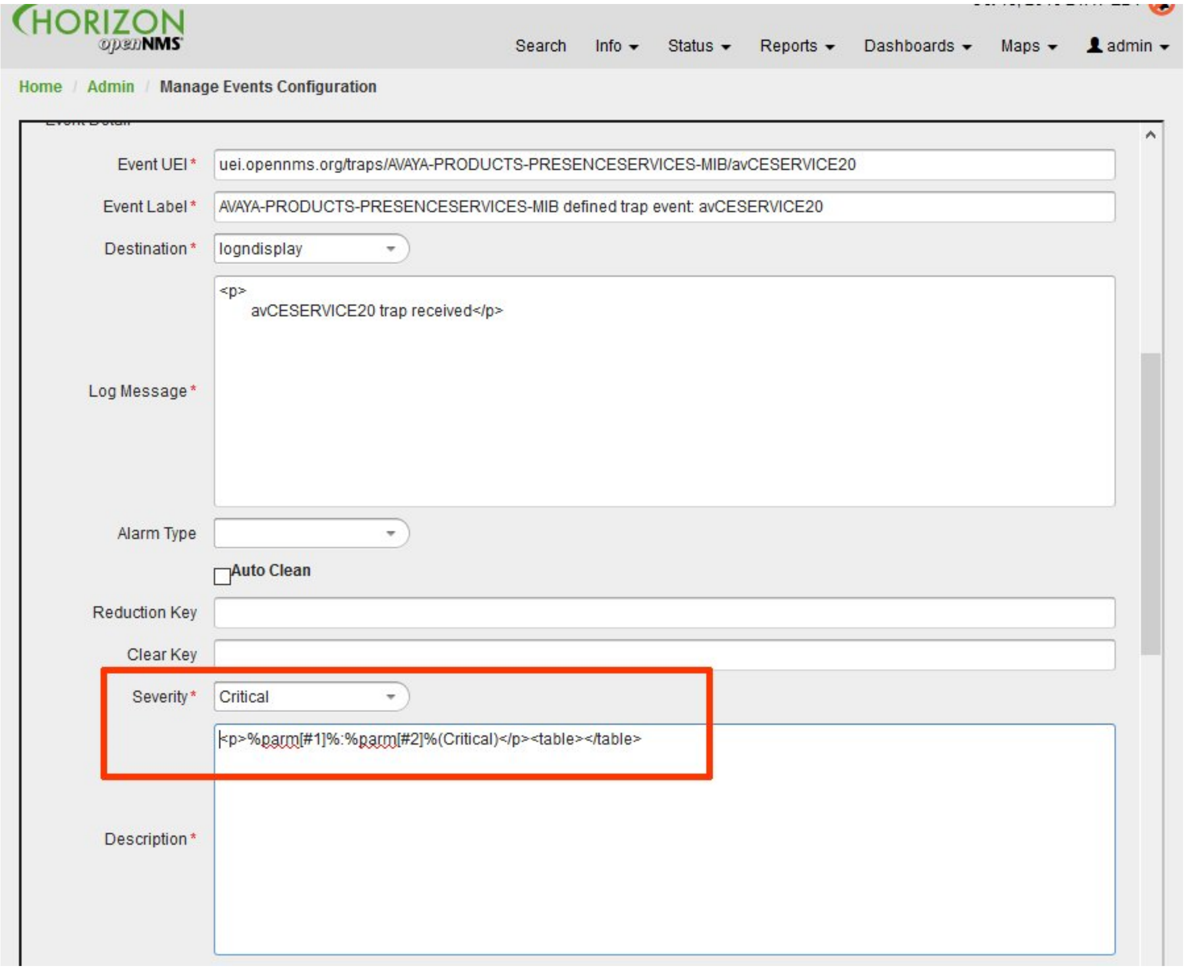
1. On the OpenNMS web console, navigate to **admin** > **Configure OpenNMS**.
2. In **Event Management**, click **Customize Event Configurations**.
3. In the **Select Events Configuration File** menu, select the **AVAYA-PRODUCTS-PRESENCESERVICES-MIB.events.xml** events configuration file.
4. Delete the **avCESERVICE1** trap event as the OID conflicts with the **avCESERVICE29** event.
5. Perform the following steps to customize all the events:
    a. Select the trap event and click **Edit**.

       For example, **avCESERVICE20**.

    b. Modify the **Severity** field from `Indeterminate` to a more appropriate level.

    c. Modify any parameters in the **Description** text from either `{1}` or `$1` to the OpenNMS format of `%parm[#1]%`.

    d. Repeat for each parameter in this event.



Event UEI * uei.opennms.org/traps/AVAYA-PRODUCTS-PRESENCESERVICES-MIB/avCESERVICE20

Event Label * AVAYA-PRODUCTS-PRESENCESERVICES-MIB defined trap event: avCESERVICE20

Destination * logndisplay

Log Message *

```
<p>
    avCESERVICE20 trap received</p>
```

Alarm Type

□ Auto Clean

Reduction Key

Clear Key

Severity * Critical

Description *

```
<p>%parm[#1]%:%parm[#2]%(Critical)</p><table></table>
```

6. Click **Save** and repeat for each trap event in the file.
7. After all the trap events have been updated, click **Save Events File**.
8. Click **Yes** to overwrite the existing file.

Related links

Network Management System configuration on page 218

Creating OpenNMS node elements

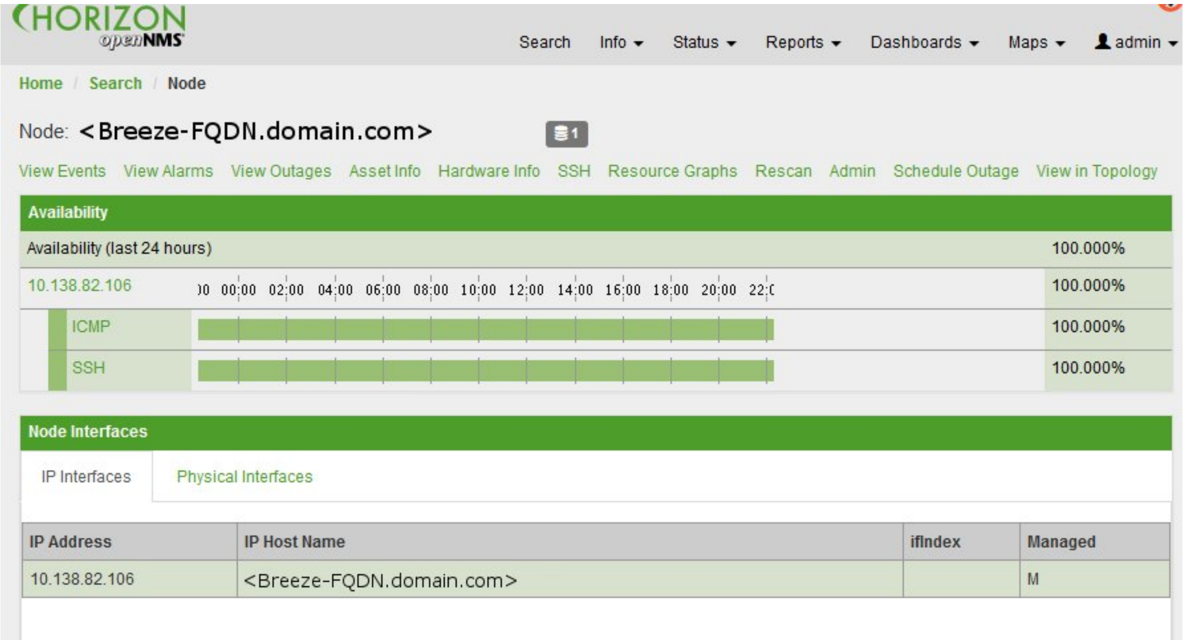
About this task

For OpenNMS to receive traps from Presence Services on the Avaya Breeze™ platform, you must define a node to represent the Avaya Breeze™ server. The following procedure describes how to create a node.

Procedure

1. On the OpenNMS web console, navigate to **admin** > **Configure OpenNMS**.

2. In **Provisioning**, click **Manually Add an Interface**.
3. Enter the IP address of the Avaya Breeze™ server management interface.
4. Click **Add**.
5. Click **Info** to navigate to the Nodes page.



Node: <Breeze-FQDN.domain.com>

Availability	
Availability (last 24 hours)	100.000%
10.138.82.106	100.000%
ICMP	100.000%
SSH	100.000%

IP Address	IP Host Name	ifIndex	Managed
10.138.82.106	<Breeze-FQDN.domain.com>		M

Related links

Network Management System configuration on page 218

Testing the OpenNMS installation

About this task

You can manually generate alarms or traps to test OpenNMS installtion on the Avaya Breeze™ platform using the CLI interface.

Procedure

1. Log in to the Avaya Breeze™ CLI interface and obtain root access.
2. Run the `presAlarmTest.sh` script to generate alarms for testing.
   - Use the `-l` option to list all available alarms.
   - Use the `-r` option to raise an alarm.
   - Use the `-c` option to clear an alarm.

```
# cd /opt/Avaya/snap_in/ps/bin/
# ./presAlarmTest.sh

Test Tool for raising/clearing all Presence Services alarms.
Usage: presAlarmTest -l|-r|-c
```

```
  Options: -l list all available alarms
           -r [alarm-event-code], raise a given alarm or leave alarm-event-code
blank to raise all alarms
           -c [alarm-event-code], clear a given alarm or leave alarm-event-code
blank to clear all alarms
           -h Prints this help

# ./presAlarmTest.sh -l
Available alarms:
  MESSAGE_ARCHIVE_UPLOAD_FAILURE_ALARM_CODE_MAJOR       IMArc_01
  MESSAGE_ARCHIVE_UPLOAD_FAILURE_ALARM_CODE_CRITICAL    IMArc_02
  GEO_REMOTE_DATACENTER_FAILURE_ALARM_CODE_CRITICAL     GR_01
  GEO_CONFIG_ALARM_CODE_MAJOR   GR_02
  HEALTH_MONITOR_CLUSTER_ALARM_MAJOR    HLTH_01
  HEALTH_MONITOR_SERVER_ALARM_MAJOR     HLTH_02
  HEALTH_MONITOR_CLUSTER_ALARM_CRITICAL HLTH_03

# ./presAlarmTest.sh -r IMArc_01

# ./presAlarmTest.sh -c IMArc_01
```

Related links

Network Management System configuration on page 218

Viewing the Alarm events in OpenNMS

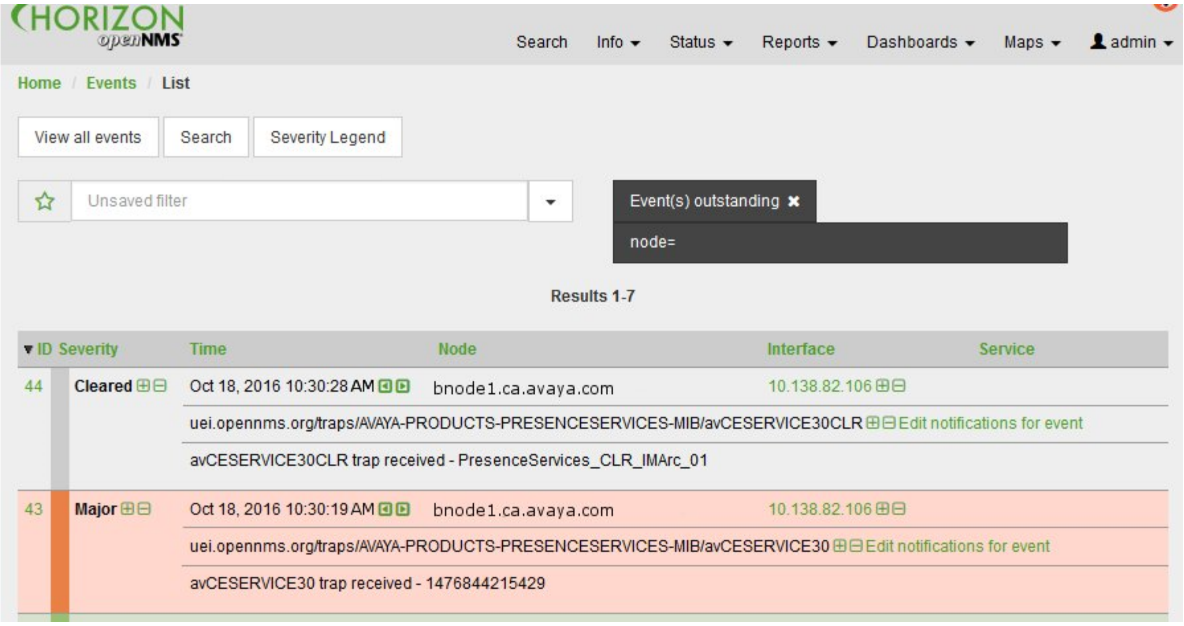
Procedure

1. On the OpenNMS web console, navigate to **Info** > **Nodes**.

   This page will display the node summary page for the Avaya Breeze™ server.

2. Click **View Events** to view any received alarms.

   The following image shows the raised and cleared events that were generated from the alarms raised and cleared in the earlier section.



Home / Events / List

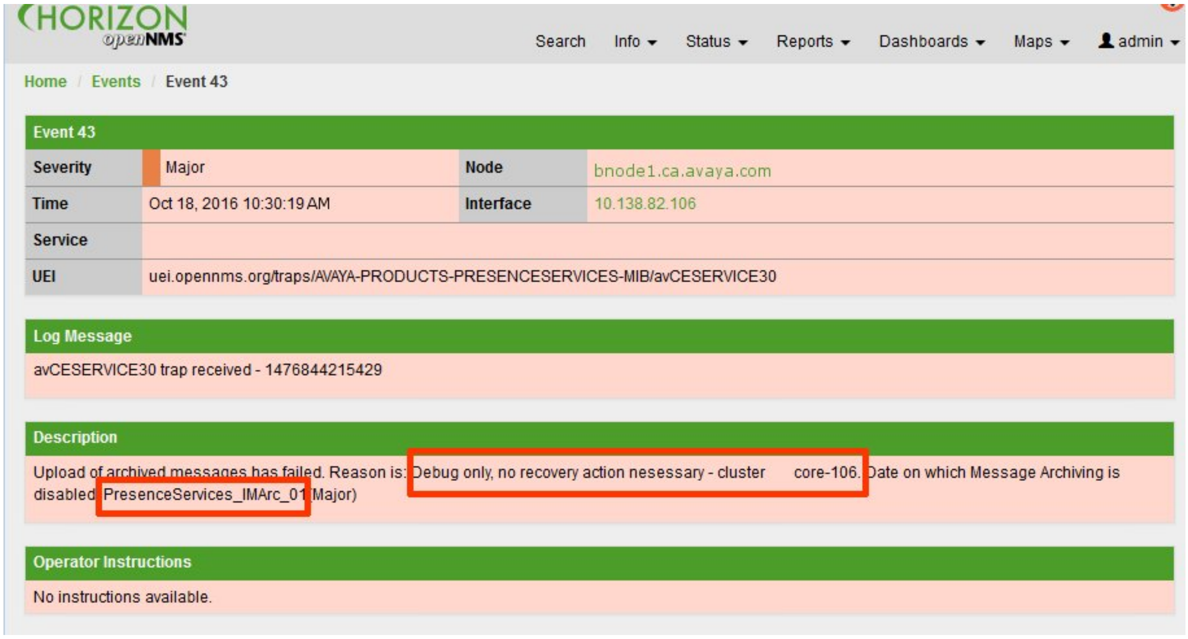
Results 1-7

ID	Severity	Time	Node	Interface	Service
44	Cleared	Oct 18, 2016 10:30:28 AM	bnode1.ca.avaya.com	10.138.82.106	
		uei.opennms.org/traps/AVAYA-PRODUCTS-PRESENCESERVICES-MIB/avCESERVICE30CLR Edit notifications for event			
		avCESERVICE30CLR trap received - PresenceServices_CLR_IMArc_01			
43	Major	Oct 18, 2016 10:30:19 AM	bnode1.ca.avaya.com	10.138.82.106	
		uei.opennms.org/traps/AVAYA-PRODUCTS-PRESENCESERVICES-MIB/avCESERVICE30 Edit notifications for event			
		avCESERVICE30 trap received - 1476844215429			

In this example, event 43 is a major alarm and event 44 is the clear event for the major event 43.

3. To view the details of the alarm, click on the green link on the event number.

   The %parm[#xx]% parameters from the event definition have been updated with the actual alarm data as received from the Avaya Breeze™ server. The following example shows two highlighted parameters in the **Description** field.



Home / Events / Event 43

Event 43

Severity	Major	Node	bnode1.ca.avaya.com
Time	Oct 18, 2016 10:30:19 AM	Interface	10.138.82.106
Service			
UEI	uei.opennms.org/traps/AVAYA-PRODUCTS-PRESENCESERVICES-MIB/avCESERVICE30		

Log Message

avCESERVICE30 trap received - 1476844215429

Description

Upload of archived messages has failed. Reason is: Debug only, no recovery action nesessary - cluster core-106. Date on which Message Archiving is disabled: PresenceServices_IMArc_01 (Major)

Operator Instructions

No instructions available.

Related links

[Network Management System configuration](#) on page 218

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 9: 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 9: 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>/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>\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 PEM file**.
5. Change directories to `<Openfire install dir>\resources\security`, where <Openfire install dir> is the directory where Openfire is installed.

    The default is `C:\Program Files (x86)\Openfire`.
6. Import the certificate into the Openfire truststore using a descriptive alias.

    For example, `SystemManagerRootCA`.

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

Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store

Procedure

1. Log in to the System Manager web console.
2. Click **Security** > **Certificates** > **Authority** > **CA Structure & CRLs**.
3. Click **Download pem file**.
4. Save the pem file.

   The default downloaded file name is `SystemManagerCA.cacert.pem`.
5. Upload the pem file to Microsoft Front End server.
6. Run Microsoft Management Console with Certificate snap-in on Computer account.
7. Click **Console Root** > **Certificates (Local Computer)** > **Trusted Root Certification Authorities Select Certificates** > **All Tasks** > **Import**.
8. In the Certificate Import Wizard, follow the steps of the wizard and select / import the uploaded pem file to the **Trusted Root Certification Authorities.**
9. To verify the imported certificate, click **Console Root** > **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates list.**
10. Select **System Manager CA** from certificate detail page.
11. Verify that the Serial number and the expiratory date of the newly imported certificate matches the System Manager CA.
12. Restart the Front End server services after completing certificate import.

    Refers to the section “Restarting the Front End server service” section”

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 9: 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 9: Single-server Cluster Federated with Ignite Openfire example values” section.

On the Openfire server, update the issuer information of the Certificate Signing Request. For Openfire 3.x, the certificates are found in **Server** > **Server Settings** > **Server Certificates**. For Openfire 4.x, the certificates are found in **Server** > **TLS/SSL Certificates** > **Server Federation Stores** > **Identity store** > **Manage Store Contents**. For more details, refer to the Openfire documentation.

Procedure

1. 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.

2. 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

About this task

On the Openfire server, the certificates used to identify the Openfire instance needs to be updated with the signed certificate generated by the Certificate Authority (System Manager). For Openfire 3.x, the certificates are found in **Server** > **Server Settings** > **Server Certificates**. For Openfire 4.x, the certificates are found in **Server** > **TLS/SSL Certificates** > **Server Federation Stores** > **Identity store** > **Manage Store Contents**. For more details, refer to the Openfire documentation.

Procedure

1. Using a text editor, open the PEM file that you created in the “Signing the Openfire CSR on System Manager” section.
2. Copy and paste the System Manager CA certificate, and click **Save**.
3. Copy and Paste the *OF domain* certificate and click **Save**.
4. Delete any pending DSA certificate pending verification. Restart Openfire if necessary and return to the Certificate settings page. Generate self-signed DSA certificates.
5. Click **Click here to restart HTTP server**.
6. Log in to the Openfire server.
7. On the Openfire server, navigate to **Server** > **Server Settings** > **Server Certificates**.
8. 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 243	
2	Create an end entity.	Creating an end entity on System Manager on page 244	
3	Create the signed identity certificate using the CSR.	Creating the Signed Identity Certificate using the CSR on page 244	

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.

Table continues…

Presence component	Connection type	Identity certificate	Comments
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' 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.

Table continues…

Presence component	Connection type	Identity certificate	Comments
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** > **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, 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 19: 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 53

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 54
	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
			Table continues…
	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 64
	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)	

Table continues…

Group	Service Attribute	Description	Reference
	Domino Calendar Request Rate *	Calendar request per minute rate to the calendar server. (Must be greater than 0) (* 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 57
	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)	

Group	Service Attribute	Description	Reference
	Exchange Server Password *	Password the Exchange collector will use when connecting to Exchange server (* requires collector restart)	
	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 208
	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	

Table continues…

Group	Service Attribute	Description	Reference
	Message Archiving Remote Password	Password of the remote SFTP site to upload archived IM's	
	Message Archiving Remote Path	Remote directory name under user home to upload archived IMs. This is an option attribute.	
	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 212
	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 188
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 146
	Inter-PS Domain Name List	Comma separated list of federated Presence Server domains (example: alphaps.eg.com,betaps.eg.com).	
System	Number of Users	Intended number of users on this cluster.	Planning on page 22

Table continues…

Group	Service Attribute	Description	Reference
		Valid range: [500-250000]	Administering Presence Services System service attributes on page 34
	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 not be able to exchange Presence and IMs.	—
	Enable Inter-Tenant Presence and IM	Enables Presence and IMs to be exchanged between Aura users with different tenant IDs. When disabled, users with different tenant IDs will not be able 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 can subscribe to that user's presence.	—

Table continues…

Group	Service Attribute	Description	Reference
	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 152
	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, Cisco Jabber, and Nextplane. Valid inputs are generic, openfire, avaya, cisco, or nextplane. 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 152
	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, Cisco Jabber, and Nextplane. Valid inputs are generic, openfire, avaya, cisco, or nextplane. 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 152
	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, Cisco Jabber, and Nextplane. Valid inputs are generic, openfire, avaya, cisco, or nextplane. Case insensitive.	

Table continues…

Group	Service Attribute	Description	Reference
	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 federation. When enabled, both server to server port and federation domain list must be configured.	XMPP federation on page 152
	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, Cisco Jabber, and Nextplane. Valid inputs are generic, openfire, avaya, cisco, or nextplane. 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.	

Table continues…

Group	Service Attribute	Description	Reference
Security	Presence Security Policy	Valid inputs are Secure Mode, Best Effort Security, and No Security. The default value is Best Effort Security. • Secure Mode: Only TLS transport must be configured for Presence Services. • Best Effort Security: Any transport is acceptable for Presence Services. • No Security: Only TCP transport must be configured for Presence Services.	—
	XMPP Client to Server Secure Communication (TLS) Mode	Valid inputs are required, optional, and disabled. The default value is optional. • Required: TLS must be used for communication to succeed. • Optional: Either TCP or TLS is acceptable for communication to succeed. • Disabled: TCP must be used for communication to succeed.	

Table continues…

Group	Service Attribute	Description	Reference
	XMPP Server to Server Mutual Authentication	Option to control mutual authentication on incoming server-to-server connections. Valid inputs are required, optional, and disabled. • Required: Far-end must present a valid certificate for verification. • Optional: Far-end certificate verification is desired but not needed. • Disabled: Far-end certificate is not requested.	

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 Equinox® 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 20: 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 264
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 265
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 147
4	Assign Presence Profile to user on System Manager.	M	M	M	M	Assigning Presence Profile to a user on System Manager on page 266
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 267
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 268
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 269
9	Export certificate chain that signs Presence Services identity.	M	M	M	—	Exporting certificate chain that signs the Presence Services identity on page 274
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 275
11	Administer Presence and IM on the device.	M	M	M	—	Checklist for administering Presence and IM on a device on page 281

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

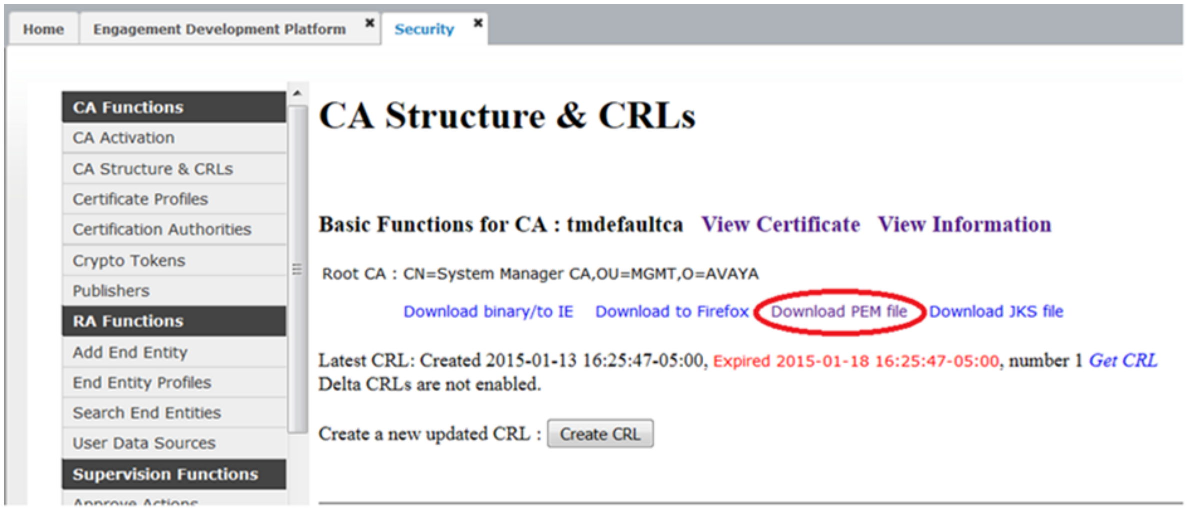
To establish a secure SIP connection to Session Manager, recent versions of SIP devices require that the certificate chain that signed the Session Manager identity be imported into truststore of the platform hosting the device.

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**.



CA Structure & CRLs

Basic Functions for CA : tmdefaultca View Certificate View Information

Root CA : CN=System Manager CA,OU=MGMT,O=AVAYA

Latest CRL: Created 2015-01-13 16:25:47-05:00, Expired 2015-01-18 16:25:47-05:00, number 1 Get CRL
Delta CRLs are not enabled.

Create a new updated CRL :

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

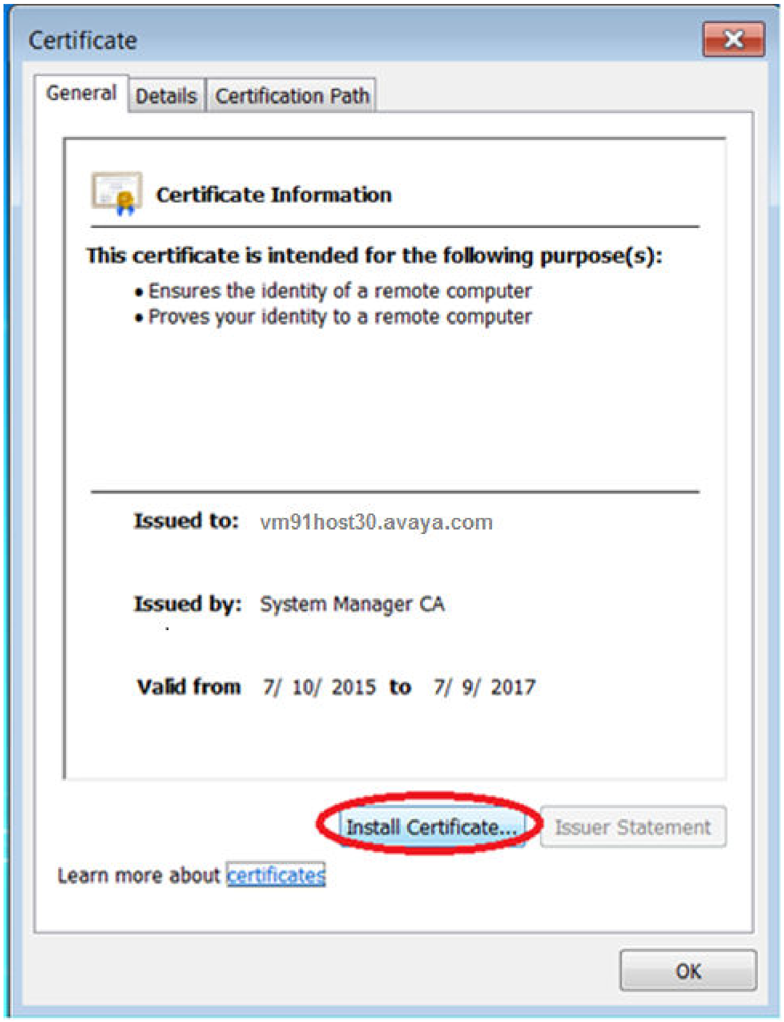
This is the second of two steps required to establish trust between SIP devices and Session Manager. The following example procedure shows how to import the certificate chain into a Windows 7 platform. For more information, consult Avaya endpoint documentation.

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**.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: vm91host30.avaya.com

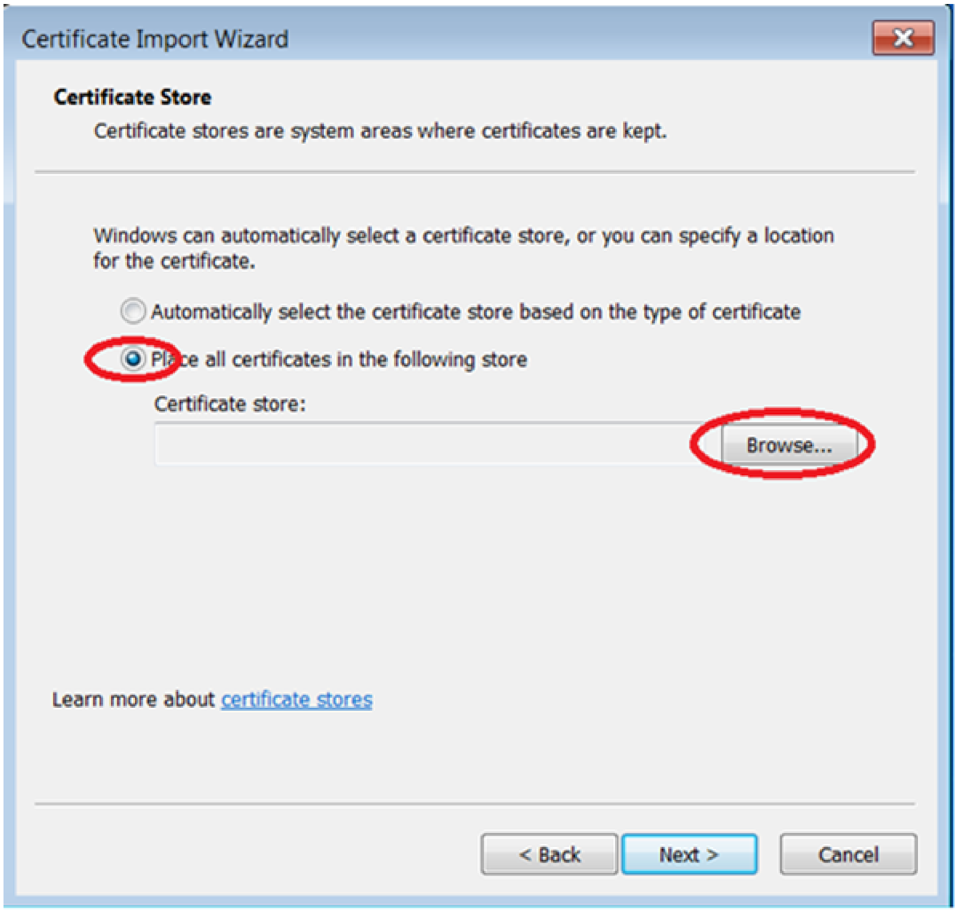
Issued by: System Manager CA

Valid from 7/ 10/ 2015 to 7/ 9/ 2017

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.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

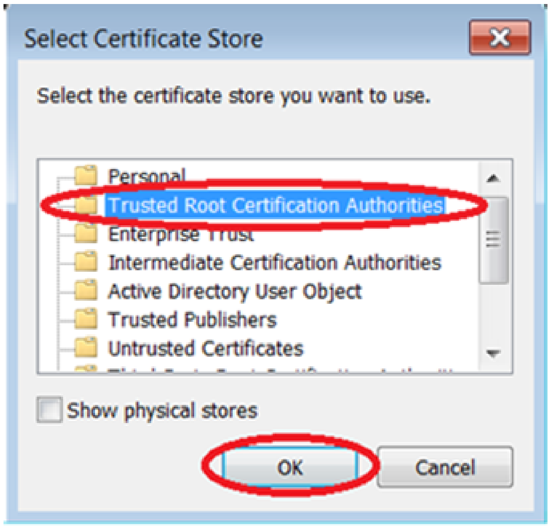
● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

The system displays the Select Certificate Store window.

7. Select **Trusted Root Certificate Authorities**, and click **OK**.

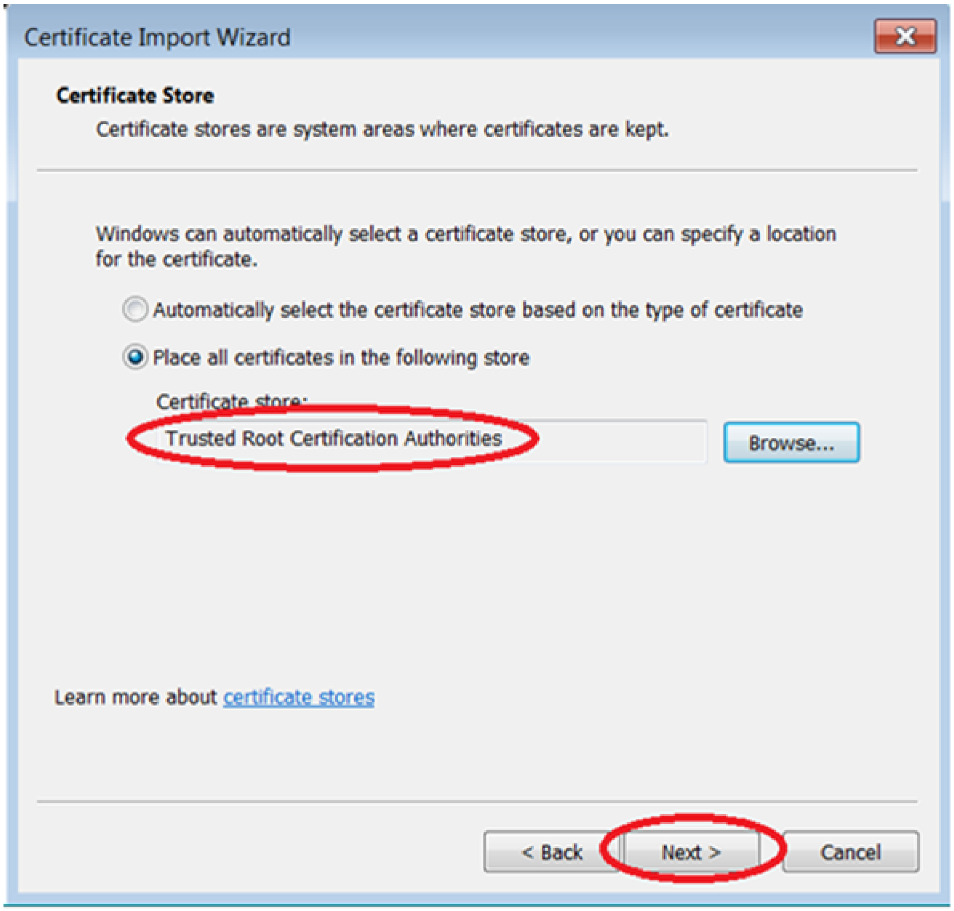


Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
□ Show physical stores
OK
Cancel

8. In the Certificate Import Wizard window, select **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

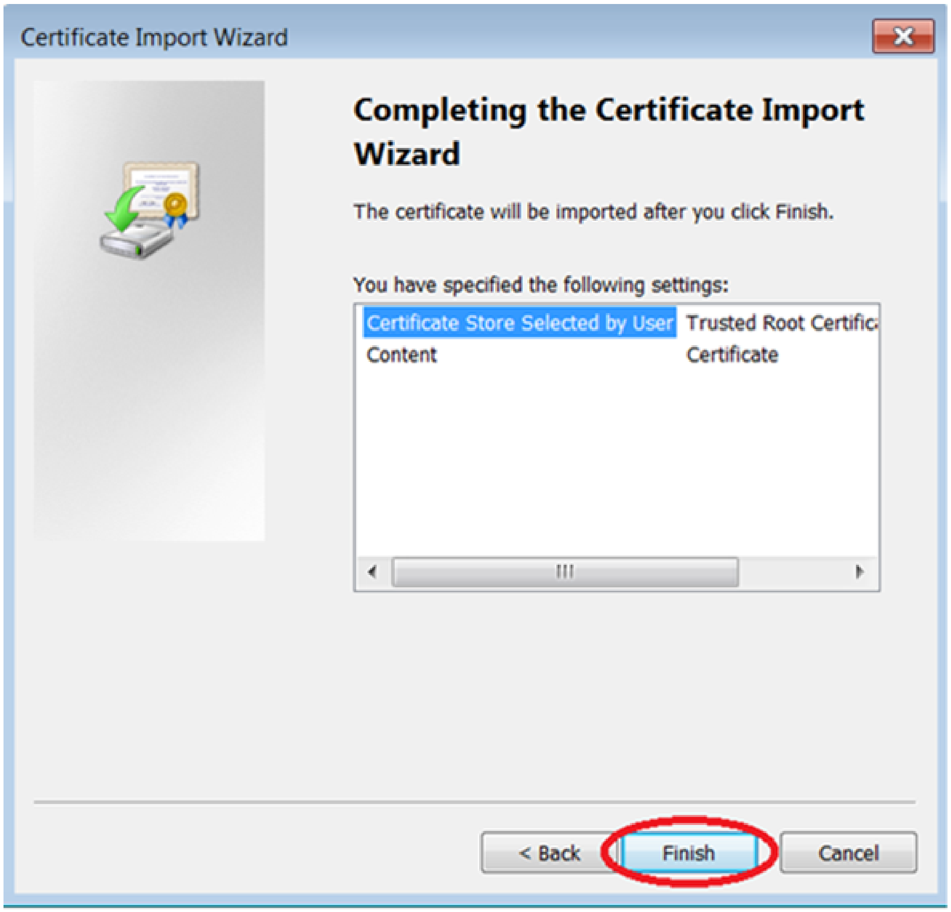
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

9. In the Completing the Certificate Import Wizard window, click **Finish**.



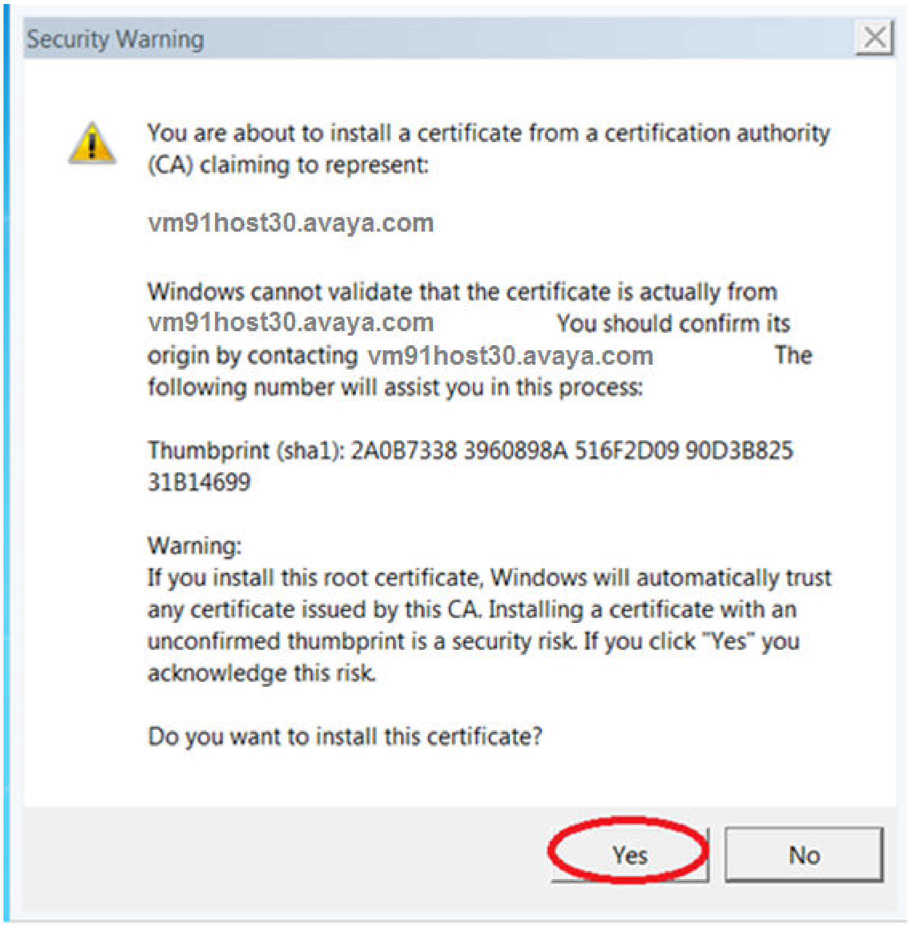
Completing the Certificate Import Wizard

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

10. If the certificate had not been previously installed on this server, then the system displays a Security Warning window. Select **Yes**.



You are about to install a certificate from a certification authority (CA) claiming to represent:

vm91host30.avaya.com

Windows cannot validate that the certificate is actually from vm91host30.avaya.com You should confirm its origin by contacting vm91host30.avaya.com The following number will assist you in this process:

Thumbprint (sha1): 2A0B7338 3960898A 516F2D09 90D3B825 31B14699

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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

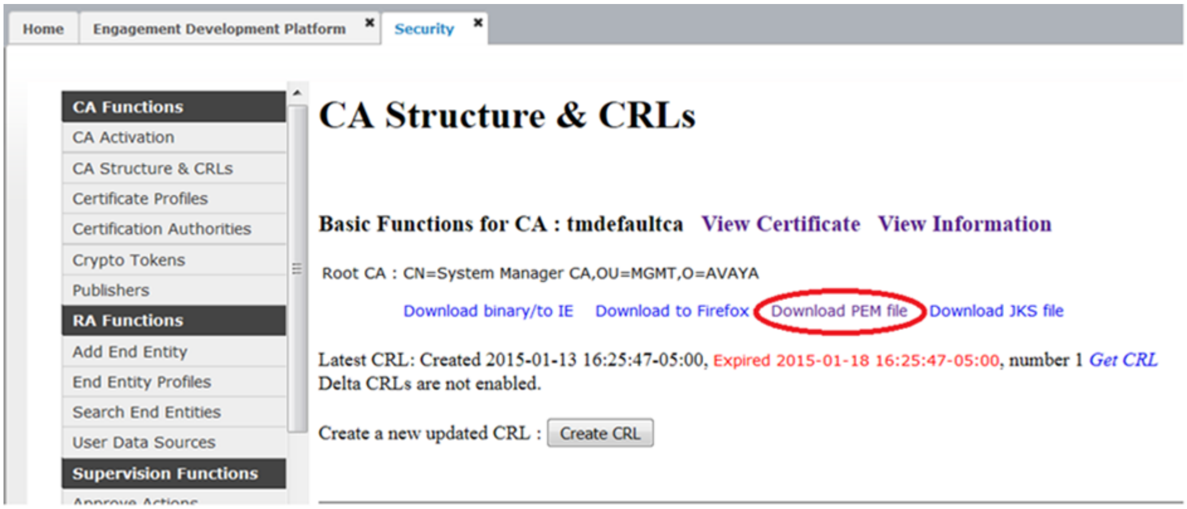
This is the first of two steps required to establish trust between devices and Presence Services for XMPP services. The following example shows how to export the certificate chain when the Certificate Authority is System Manager.

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**.



CA Structure & CRLs

Basic Functions for CA : tmdefaultca View Certificate View Information

Root CA : CN=System Manager CA,OU=MGMT,O=AVAYA

Latest CRL: Created 2015-01-13 16:25:47-05:00, Expired 2015-01-18 16:25:47-05:00, number 1 Get CRL
Delta CRLs are not enabled.

Create a new updated CRL :

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:**

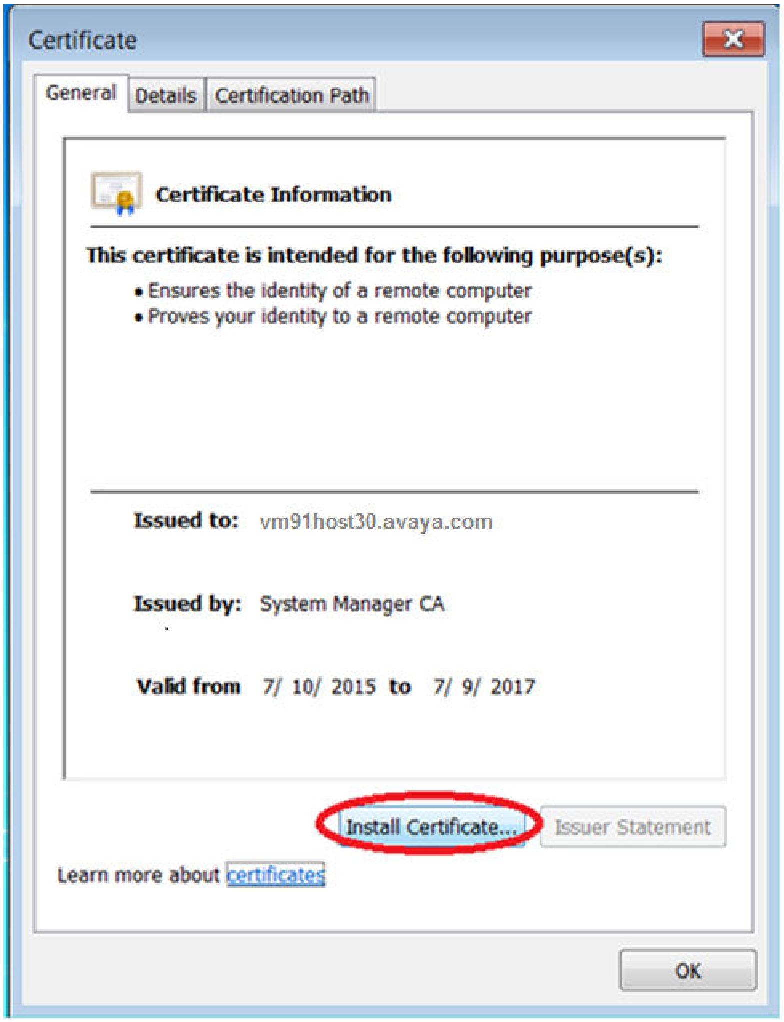
If System Manager is the Certificate Authority for both Session Manager and Presence Services , then there is no need to repeat this task if it was already performed in "Importing certificate chain that signs the Session Manager identity"

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**.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: vm91host30.avaya.com

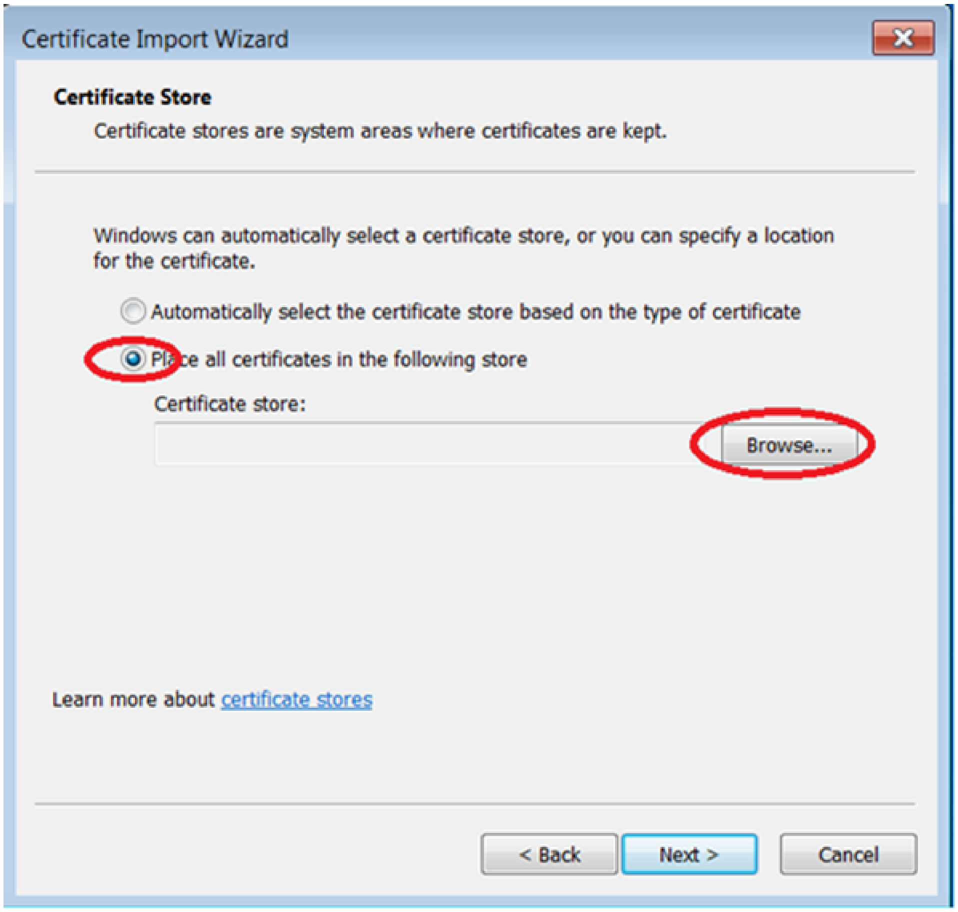
Issued by: System Manager CA

Valid from 7/ 10/ 2015 **to** 7/ 9/ 2017

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.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

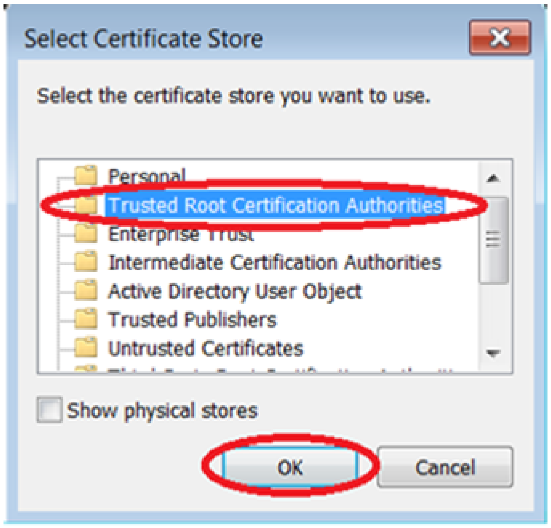
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

The system displays the Select Certificate Store window.

7. Select **Trusted Root Certificate Authorities**, and click **OK**.

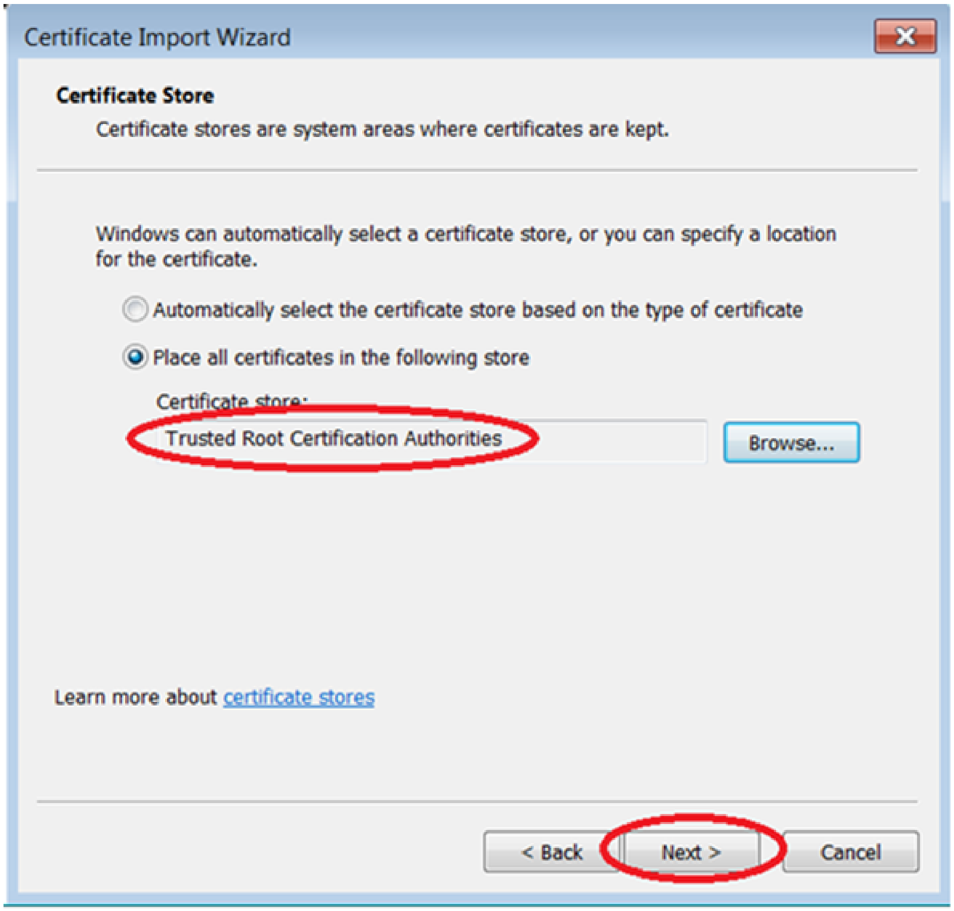


Select the certificate store you want to use.

Trusted Root Certification Authorities

□ Show physical stores

8. In the Certificate Import Wizard window, select **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

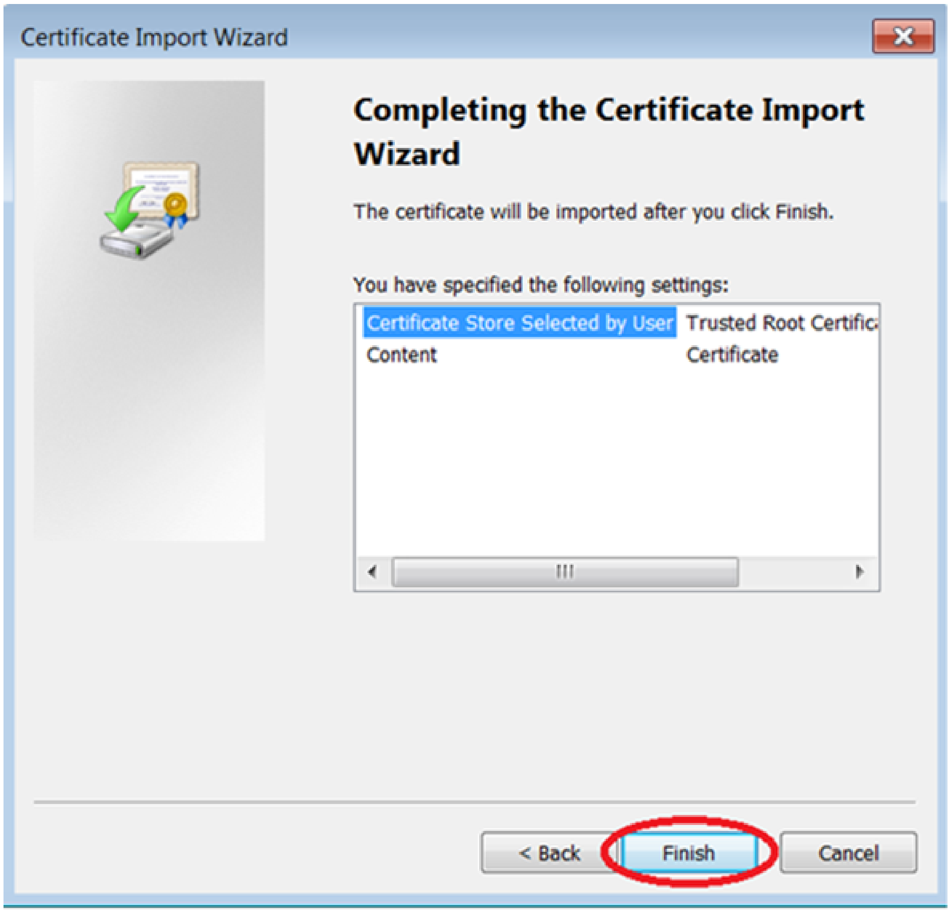
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

9. In the Completing the Certificate Import Wizard window, click **Finish**.



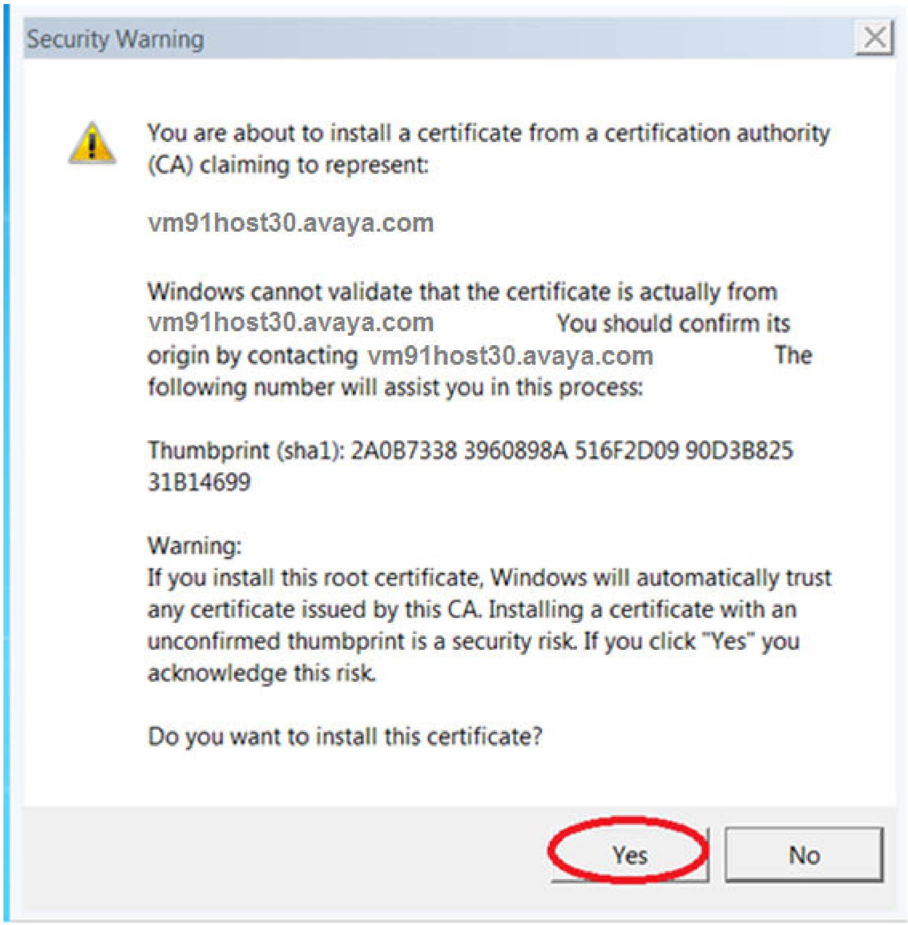
Completing the Certificate Import Wizard

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

10. If the certificate had not been previously installed on this server, then the system displays a Security Warning window. Select **Yes**.



You are about to install a certificate from a certification authority (CA) claiming to represent:

vm91host30.avaya.com

Windows cannot validate that the certificate is actually from vm91host30.avaya.com You should confirm its origin by contacting vm91host30.avaya.com The following number will assist you in this process:

Thumbprint (sha1): 2A0B7338 3960898A 516F2D09 90D3B825 31B14699

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

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 21: Checklist for administering Presence and IM on a device

No.	Task	Device category				Notes/Reference
		1	2	3	4	
1	Administer Communication Profile password on the device.	M	M	M	—	Password is required to authenticate the user for XMPP on Presence Services. See Assigning Communication Profile Password to a user on System Manager on page 265.
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.

Table continues…

No.	Task	Device category				Notes/Reference
		1	2	3	4	
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 29. - 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 29. 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.
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 147.

Manual presence state expiration time

You can administer the Presence Server to define the expiration period of presence state that is set manually. When the manual presence state period expires, the presence state changes to automatic and a notification is sent to other users of your new presence state. Your manual presence state expires based on the configuration in the Manual state expiration time section. For example, if you set your presence state manually to Busy, and the Manual state expiration time for Busy is set to 600, then your Busy presence state expires after 600 seconds and the presence state changes to automatic. When your presence state changes, a notification is sent to other presence users of your new presence state.

This feature is supported on OneX and Equinox clients. You can select one or more of the following presence states manually:

- Available
- Busy
- Away
- Do-Not-Disturb
- Out-of-Office
- Offline

Configuring manual presence state expiration time

Procedure

1. On the System Manager web console, navigate to **Elements** > **Avaya Breeze™** > **Configuration**.
2. Click **Attributes**.
3. On the **Service Clusters** tab, in the **Cluster** field, click the Presence Services cluster.
4. In the **Service** field, click the Presence Services service.
5. On the Attributes Configuration page, navigate to the **Manual state expiration time**.
6. **(Optional)** To override the default value of a presence state, select the **Override Default** check box against the presence state that you want to configure.
7. In the **Available** field, in **Effective Value**, type the expiration time in seconds.
8. Click **Commit**.

Chapter 11: Performance

Capacity and scalability specification

Table 22: 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 a 10-server cluster[1], and 250,000 on two 10-server clusters[1]	175,000 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 10 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 10-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 10-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
H.323 (XMPP)	Up to 16,000 on a single server, 125,000 on a 10-server cluster[1], and 250,000 on two 10-server clusters[1]	125,000 on a single cluster and 350,000 on a dual cluster[2]	25	100[3]	300	30	44

Table 23: 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 10 servers and a maximum of two clusters for each cluster System Manager.

Table continues…

Feature	Restriction
High Availability	• Up to 16,000 users: total of 2 servers in the cluster • Up to 32,000 users: total of 3 servers in the cluster • Up to 48,000 users: total of 4 servers in the cluster • Up to 64,000 users: total of 5 servers in the cluster • Up to 80,000 users: total of 6 servers in the cluster • Up to 96,000 users: total of 8 servers in the cluster • Up to 112,500 users: total of 9 servers in the cluster • Up to 125,000 users: 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 more details about the Presence Services port information, see the “Accessing the port matrix document” section.

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.

Table continues…

Alarm name	Causes	Resolutions
Message Archive upload failed	Messaging Archiving attributes have been misconfigured. For example, an invalid Remote Server Address has been entered.	Reconfigure the **Message Archiving** attributes on System Manager at **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
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.

Table continues…

Alarm name	Causes	Resolutions
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. • 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

Table continues…

Alarm name	Causes	Resolutions
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”.

Table continues…

Alarm name	Causes	Resolutions
Cluster Health Check failed	• Duplicate domains: Presence/IM domains can be configured at: - **Local Presence/IM domains** at **Elements** > **Routing** > **Domains** - **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	• 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** - **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`.

Alarm name	Causes	Resolutions
	enabled, exceeds the number supported on the cluster.	

Number of contact rosters exceeds the system limit

Solution

1. Expand the capacity of the overall system by adding more virtual machines.

   For more information, see “Deployment”.

2. If the system is at the highest supported deployment profile, request users to reduce the number of presence buddies in their contact list.

Number of provisioned users is over the configured attribute limit

Cause

The system raises a health check alarm when the number of provisioned users exceeds the limit configured in the service attribute.

Solution

1. Perform one of the following:

   - Increase the value of the **Number of Users** service attribute.

     A service restart is required after the configuration change to take effect.

     The number of users cannot exceed to what is supported by the Avaya Breeze™ profile. For more information see *Chapter 5: Planning – Cluster considerations*.

   - Unassign some users from the cluster by changing their Presence Services communication profile.

2. Assign users to different service profiles to distribute the roster allocation across the users so that the system limit is not exceeded.

Number of configured users is over the support limit

Cause

The system raises a health check alarm if the number of users configured in the server global or cluster service attribute is greater than the maximum number of users supported by the Avaya Breeze™ VM profile.

Solution

Perform one of the following:

- Change the Avaya Breeze™ VM profile by adjusting the number of CPUs and/or the total amount of physical memory available.

  A service restart is required after the configuration change to take effect.

  For more information see *Chapter 5: Planning – Cluster considerations*.
- Change the value of the Number of Users service attribute to match the currently deployed Avaya Breeze™ VM profile.

No DNS SRV records found for any Presence domain for XMPP Federation

Cause

The system raises a health check alarm if the XMPP federation is enabled but the Presence Services domain is configured for the cluster does not have SRV record defined that resolves to this cluster.

Solution

Configure proper SRV records for presence domains that can be resolved into current cluster. For more information, see ““Administering DNS SRV records for local Presence Services domains”.

Signaling security health check alarms

Solution

Depending on the security policy set, verify the following service attributes in the Security group:

- If **Security policy** is `Secure Mode`
  a. Ensure that the SIP Entity links are using TLS.
  b. Ensure that the **XMPP Client to Server Secure Communication (TLS) Mode** field is set as `Required`.
  c. Ensure that the **XMPP Federation <x>** > **Enable Secure Communication (TLS) <X>** field is set as `True`.

- If **Security policy** is `No Security`:
  a. Ensure that the SIP Entity links are using TLS.
  b. Ensure that the **XMPP Client to Server Secure Communication (TLS) Mode** field is set as `Disabled`.
  c. Ensure that the **XMPP Federation <x>** > **Enable Secure Communication (TLS) <X>** field is set as `False`.
- If **Security policy** is `Best Effort`, any transport type is accepted.

Cluster misconfigured health check alarms

Load Balancer is not enabled on a multi-node cluster

Solution

Ensure that the Load balancer checkbox is enabled in the Avaya Breeze™ Cluster Configuration page.

No FQDN is configured for a Service IP IP_ADDRESS

Cause

No FQDN is configured for a Service IP IP_ADDRESS, where IP_ADDRESS is a cluster IP address in a multi-node cluster or a Security Module IP address in a single-node cluster.

Solution

Presence services SIP Entity must have an FQDN defined. This FQDN must have a local host name resolution mapped to server signaling IP address at **System Manager** > **Session Manager** > **Network Configuration** > **local host name resolution**.

Server does not have an associated Presence Services managed element

Solution

Ensure that there is an inventory managed element of type `Presence Services` at **System Manager** > **Inventory** > **Management Elements**.

Managed element is not assigned to the current cluster

Solution

Ensure that there is an inventory managed element of type `Presence Services` at **System Manager** > **Inventory** > **Management Elements**.

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**.

Unable to get _People View

Cause

The Domino Calendar collector uses the _People database view available in the Domino server. However, for some Domino servers with localized templates, this _People view name is based on the locale of the template. For example, the German template contains the view _Personen, instead of _People. This causes the calendar collector to fail. The log message on the Presence Services server for this error condition is: `Unable to get _People View`. This log message is a FINE level log message.

Solution

To fix this issue, the Domino administrator must create the _People view.

Vysper fails to start when no domains are created in System Manager

Cause

When no domains are created in System Manager, Vysper fails to start and reports the following error:

```
2017-01-17 08:50:24,471 [context-init-thread]
presence.bootstrap.PsBootStrapServletListener ERROR - ContextInitThread#run() Exception
while initializing, Unregister from CAR Error reading domains
java.lang.IllegalArgumentException: Error reading domains
    at com.avaya.presence.xmpp.gw.XmppGateway.initVysper(XmppGateway.java:142)
    at com.avaya.presence.xmpp.gw.XmppGateway.start(XmppGateway.java:83)
    at com.avaya.presence.bootstrap.PsBootStrapServletListener
$ContextInitThread.run(PsBootStrapServletListener.java:487)
```

Solution

1. Configure domains on System Manager.
2. Restart Presence Services.

Related links

Restarting Presence Services on page 233

Configuring Presence/IM routing domain on System Manager on page 264

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.

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 the appropriate Avaya Breeze™ replication group.
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.

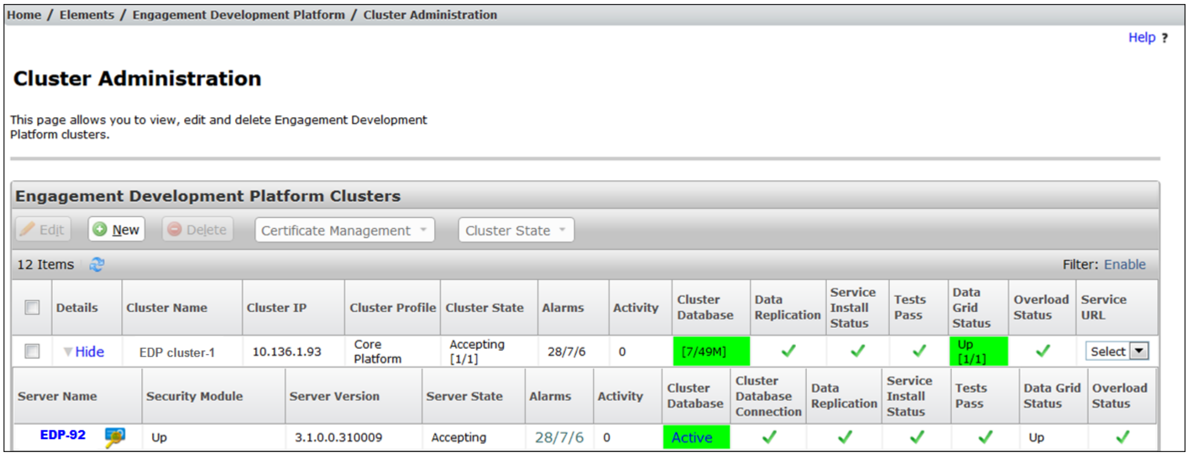
Verifying that Presence Services snap-in is ready to support Presence and IM

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:


Home / Elements / Engagement Development Platform / Cluster Administration
Help ?

Cluster Administration

This page allows you to view, edit and delete Engagement Development Platform clusters.

Engagement Development Platform Clusters

Edit
New
Delete
Certificate Management
Cluster State

12 Items

Filter: Enable

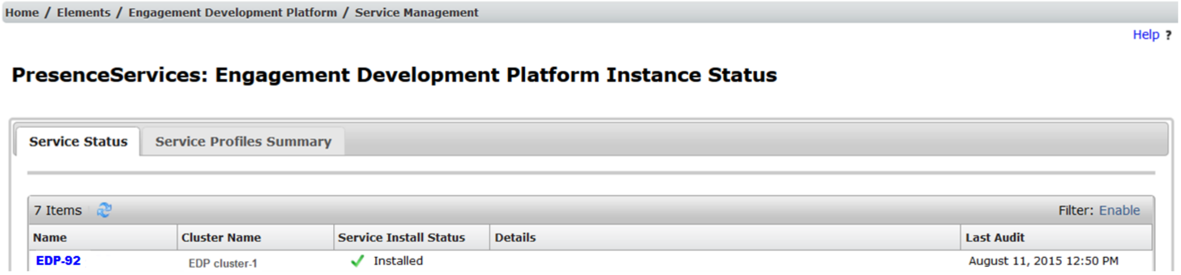
□	Details	Cluster Name	Cluster IP	Cluster Profile	Cluster State	Alarms	Activity	Cluster Database	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status	Service URL
□	▼Hide	EDP cluster-1	10.136.1.93	Core Platform	Accepting [1/1]	28/7/6	0	[7/49M]	✓	✓	✓	Up [1/1]	✓	Select

Server Name	Security Module	Server Version	Server State	Alarms	Activity	Cluster Database	Cluster Database Connection	Data Replication	Service Install Status	Tests Pass	Data Grid Status	Overload Status
EDP-92	Up	3.1.0.0.310009	Accepting	28/7/6	0	Active	✓	✓	✓	✓	Up	✓

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:


Home / Elements / Engagement Development Platform / Service Management
Help ?
Service Status
Service Profiles Summary
7 Items
Filter: Enable

PresenceServices: Engagement Development Platform Instance Status

Name	Cluster Name	Service Install Status	Details	Last Audit
EDP-92	EDP cluster-1	✓ Installed		August 11, 2015 12:50 PM

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.	
Administering		
Administering Avaya Breeze™	Find the procedures to administer and configure Avaya Breeze™.	System administrators and support personnel
Administering Avaya Aura® System Manager	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

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product** > **Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
7. 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.

- 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

presAlarmTest

Run this script on Avaya Breeze™ to trigger or clear Presence Services alarms.

Syntax

`presAlarmTest [-l] [-r] [-c] [-h]`

Options:

- `-l`: Lists all available alarms.
- `-r [`*`alarm-event-code`*`]`: Raises a given alarm or omits the alarm-event-code to raise all alarms.
- `-c [`*`alarm-event-code`*`]`: Clears a given alarm or omits the alarm-event-code to clear all alarms.
- `-h`: Prints the help.

Sample output 1

```
# cd /opt/Avaya/snap_in/ps/bin/
# ./presAlarmTest.sh

Test Tool for raising/clearing all Presence Services alarms.
Usage: presAlarmTest -l|-r|-c
  Options: -l list all available alarms
           -r [alarm-event-code], raise a given alarm or leave alarm-event-code blank
to raise all alarms
           -c [alarm-event-code], clear a given alarm or leave alarm-event-code blank
to clear all alarms
           -h Prints this help
```

Sample output 2

```
# ./presAlarmTest.sh -l
Available alarms:
  MESSAGE_ARCHIVE_UPLOAD_FAILURE_ALARM_CODE_MAJOR       IMArc_01
  MESSAGE_ARCHIVE_UPLOAD_FAILURE_ALARM_CODE_CRITICAL    IMArc_02
  GEO_REMOTE_DATACENTER_FAILURE_ALARM_CODE_CRITICAL     GR_01
  GEO_CONFIG_ALARM_CODE_MAJOR   GR_02
  HEALTH_MONITOR_CLUSTER_ALARM_MAJOR    HLTH_01
  HEALTH_MONITOR_SERVER_ALARM_MAJOR     HLTH_02
  HEALTH_MONITOR_CLUSTER_ALARM_CRITICAL HLTH_03
```

Sample output 3

```
# ./presAlarmTest.sh -r IMArc_01
```

Sample output 4

```
# ./presAlarmTest.sh -c IMArc_01
```

presCleanup

Use this script to force clean Presence Services on Avaya Breeze™. You must run this script with root user privileges after Presence Services has been uninstalled from System Manager.

Syntax

```
presCleanup.sh [-db] [-log] [-grid] [-all]
```

Options:

- `-db`: Cleans the Presence Services database.
- `-log`: Deletes the Presence Services log files.
- `-grid`: Undeploys any Presence Services processing units and associated directories.
- `-all`: Cleans the Presence Services database, deletes the Presence Services log files, and Undeploys any Presence Services processing units and associated directories.

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>
```

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
```

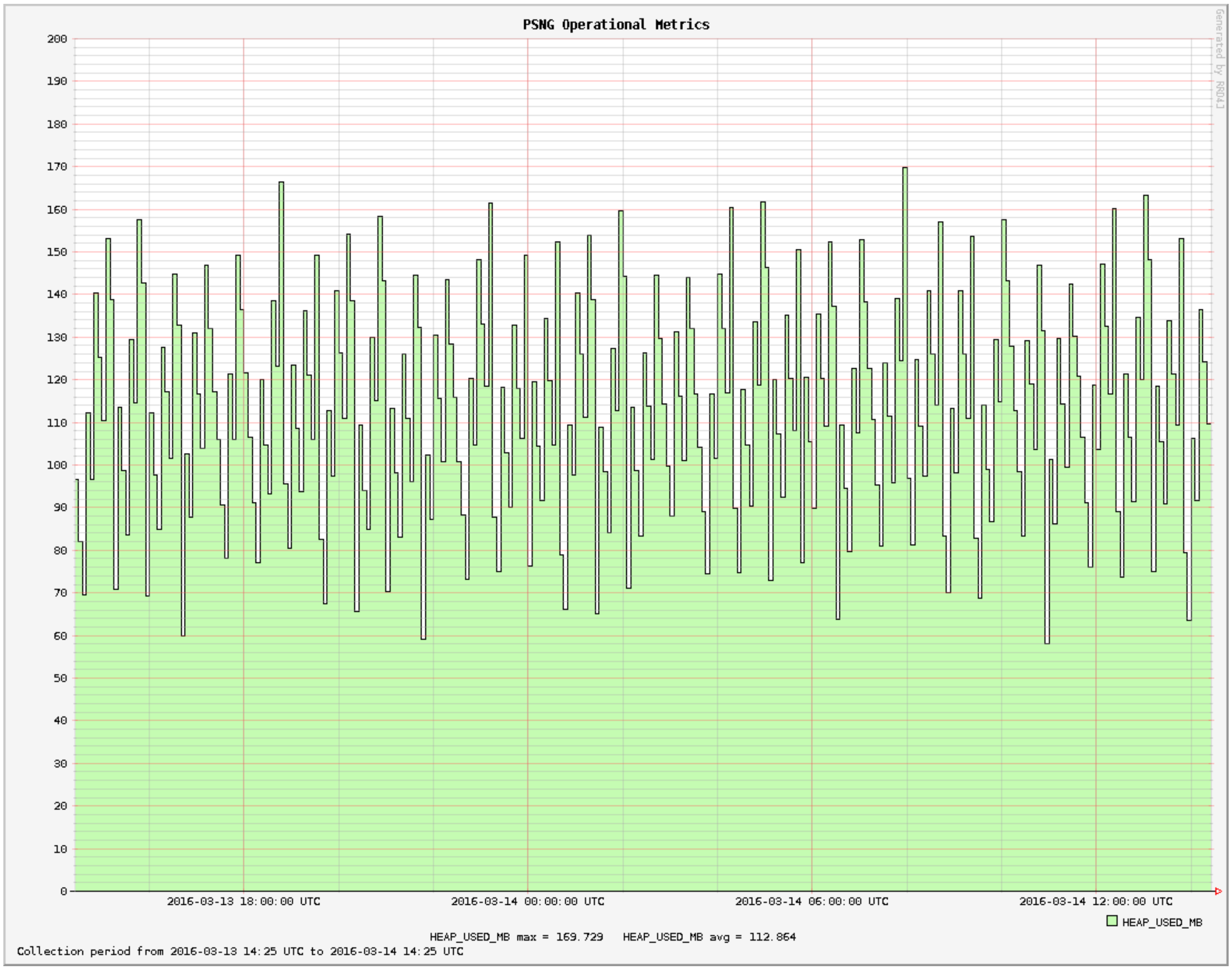
Sample output 2

```
# 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.



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
```

presUnlock

Use this script to:

- List users locked out due to too many failed login attempts.
- Allow unlocking of users based on login name.

Syntax

`presUnlock [-h] [-u` *`login_name`* `[unlock]]`

Options:

- `-h`: Displays the help.
- `-u` *`login_name`*: Displays the details of the locked user. Use **all** to select all users.
- `unlock`: Unlocks a particular user. You cannot use this parameter with **all**.

Sample output 1

```
# presUnlock -u user0@avaya.com
Display locked user details:
User Login Name = user0@avaya.com

 loginName       | numFailedAttempts | lastFailedTime           | isUserLocked
-----------------+-------------------+--------------------------+--------------
 user0@avaya.com | 3                 | 2016-12-22T17:08:40-0500 | true
(1 rows)
```

Sample output 2

```
# presUnlock -u all
Display locked user details:

 loginName       | numFailedAttempts | lastFailedTime           | isUserLocked
-----------------+-------------------+--------------------------+--------------
 user0@avaya.com | 3                 | 2016-12-22T17:08:40-0500 | true
 user1@avaya.com | 3                 | 2016-12-22T17:10:22-0500 | true
(2 rows)
```

Sample output 3

```
# presUnlock -h
Description: This script provides the capability to view users that are locked out, and
to unlock a specific user
This script can only be run by administrative access
Usage:       presUnlock [-h] [-u <login_name> [unlock]]

Options:

-h                    Show this help.
-u <login_name>       Select user by loginname. Use 'all' to select all users.
   [unlock]           Use this additional argument to unlock a particular user. Can not
be used with 'all'.
```

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.

Index

Special Characters

_configure
    Avaya Presence Services attributes 140
_Configuring Avaya Breeze server Trusted Certificate 91
_People 299
_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT 138, 295

A

access control policy 54
Access control policy 53
accessing port matrix 305
accociated contacts 216
adding
    DNS A record for Avaya session border controller for enterprise to a microsoft DNS sever 103
    DNS reverse pointer record for Avaya Session Border Controller for Enterprise to a Microsoft DNS server ... 103
adding Lotus Notes handle to Aura user 82
administrator log in
    Avaya SBCE 106
    SBCE 106
AES Collector 12, 54, 55
    Geographic Redundant deployment 57
    network routing configuration 57
alarm 289
    CLR_IMArc_01 289
    CLR_IMArc_02 289
    CluMon_01 289
    IMArc_01 289
    IMArc_02 289
    PresServ_CLR_CluMon_01 289
Application Enablement Services collection 267
architecture 14
Aura client 150
Avaya Breeze 29
Avaya Breeze cluster 32
Avaya Breeze Entity Link 29
Avaya Breeze server 31
Avaya Breeze SIP Entity 29
Avaya Multimedia Messaging 195
    checklist 196
    interoperability 193
Avaya Multimedia Messaging interoperability 198
Avaya Multimedia Messaging Service Attributes 199
Avaya Multimedia Messaging SIP Entity 197
Avaya SBCE
    administrator login 106
    configuration 104

C

CA certificate
    importing 184
capacity 285
certificate 150
certificate management 261
certificate signing request 241
Certificate Signing Request 178
certificate validation
    Openfire 165
change history 10
checklist 262
    configuring Microsoft Federation with external domains 98
    configuring Microsoft Federation with internal Avaya Aura domain and external Microsoft domain 139
    federation 146, 147
    for configuring microsoft federation with internal and external domains using inter-PS federation 142
    geographically redundant Presence Services clusters . 38
    IM 281
    Microsoft Federation 85
    multi-server cluster 36
    presence 281
    Presence Services deployment 24
    XMPP federation 152
Checklist
    integrating Domino Calendar with Presence Services . 66
Cisco domain 168
Cisco Jabber 168
    configuring 170
    federation 168
    Presence Services 170
Cisco Jabber CSR 181
CLR_IMArc_01 289
CLR_IMArc_02 289
CluMon_01 289
cluster 90, 233
Cluster considerations
    Planning 22
Cluster Truststore 237
Communication Manager application 96
Communication Profile Password 265
configuration 23
    end point policy groups 120
    media interfaces 114
    Microsoft Edge external signaling interface 112
    routing profiles 121, 123
    server configuration profiles 116
    server interworking profiles 115
    Session Manager external signaling interface 113
configuration checklist

configuration checklist *(continued)*
- Microsoft Federation with external domains 98
- Microsoft Federation with external Microsoft domain . 139
- Microsoft Federation with internal Avaya Aura domain 139

configuring 143–145, 284
- Avaya SBCE 104
- DNS 103
- inter-PS federation for domain 2 143
- inter-PS federation to domain 1 145
- Microsoft Federation with external domains 98
- microsoft front end static routing 144
- Microsoft internal domain federation 144
- microsoft trusted application pool 144
- routing between session manager and session border controller 132
- SBCE 104
- SIP federated domain 131

Configuring 212
Configuring Avaya Breeze attributes 94
Configuring Avaya Breeze server Identity Certificate 92
Configuring Avaya Breeze server Trusted Certificate 91, 93
Configuring DNS A Records 86
configuring domain 2 143
Configuring Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route 88
configuring Zang federation
- Zang events 185

contact management
- Aura client 150

courses 305
create
- End Point Flows 128
- signaling manipulation script 127

creating
- End Point Flows 128
- signaling manipulation script 127

creating Aura user 70
creating End Point Flows 128
creating signaling manipulation script 127
CSR 178, 241

D

device administration 261
device configuration 261
Disable Certificate Verification
- Openfire 157

DNS 33, 169
DNS administration 261
DNS configuration 261
DNS resolution 163
DNS server 95
DNS SRV 160, 162, 197
DNS SRV records
- Avaya Multimedia Messaging conference services 205

DNS SRV records *(continued)*
- external XMPP federation system conference services 206

domain 1 configuration 142
domain 2 configuration 143
Domino Calendar 66
Domino Calendar web service 64
Domino Calendar web service database 67
Domino collector 64
Domino Collector 12, 64
- Geographic Redundant deployment 66
- network routing configuration 66

Domino enterprise deployment 64

E

enable
- external topology hiding 124
- internal topology hiding 125

Enable Certificate Verification
- Openfire 157

enabling
- external topology hiding 124
- internal topology hiding 125

Enrollment Password 301
Entity Link 30
Entity Profile 239
EULA 34
event definitions 228
exchange collector 57
Exchange Collector 12, 61
- Geographic Redundant deployment 63
- network routing configuration 63

exchange collector overview 57
export certificate
- Session manager identity 268

F

feature comparison 19
federation 83
finding port matrix 305
firewall
- configuring 226

FQDN 36

G

geographically redundant deployment 37
Geographic Redundancy 42
Geographic Redundant Avaya Breeze Cluster 41
Geographic Redundant deployment
- DNS 166
- DNS SRV records 166

getHomeCapabilities 298

H

H.323 mode 261
hard delete 208
home Avaya Multimedia Messaging Cluster 198

I

identity certificate 246
IM 18, 212
IM1: Message Archiving Enabled 210
IM2: Message Archiving Remote Server Address 210
IM3: Message Archiving Remote User 210
IM4: Message Archiving Remote Password 210
IM5: Message Archiving Remote Path 210
IM6: Message Archiving Remote Upload Frequency 210
IM7: Message Archiving Remote Upload Failures Threshold 210
IMArc_01 289
IMArc_02 289
IM Blocking in Do Not Disturb state 188
importing certificate 58
Importing the System Manager Default CA certificate into Microsoft Front End server Trust Store 88, 239
installing 34
    snap-in 34
Instant Message Broadcast Tool 190
    using 190
integrating Domino Calendar with Presence Services
    Checklist 66
integrating exchange collector with presence services 60
Inter-Domain
    IM 206
    Presence 206
Inter-PS federation 146, 148
Inter-Tenant
    IM 207
    Presence 207
Inter-Tenant Presence and IM 207

K

key configuration information
    XMPP federation 152
key customer configuration information 195

L

licensing 21
Linux 236
Load Balancer is not enabled on a multi-node cluster 297
loading snap-ins
    service 34
load snap-ins 34
Local Presence Service 12, 13
logging level 300
LPS 12, 13

M

Managed Element 33
manual presence state
    configuring 284
    expiration time 283
Message Archiver 208
    enabling 210
MIB 221
MIB files
    importing 226
Microsoft Edge
    configuring TLS client profile 108
    external signaling interface configuration 112
Microsoft Edge Border Rule
    setup 126
Microsoft Edge CA
    retrieving certificate 107
microsoft edge server
    SIP federated domain configuration 131
Microsoft Exchange server
    exporting certificate 59
Microsoft federation
    external domains 98
microsoft federation with internal and external domains using inter-PS federation 141
Microsoft Front End server Trusted Application Pool, Trusted Application and Static Route 212
Microsoft Real Time Communication (RTC) Federation 83
Microsoft SIP user handle
    System Manager 85
microsoft trusted application 144
multi-server deployment 35
Multi-tenancy 211
Multi-User Chat 204

N

Network Management System 218
network outage 298
new identity certificate
    System Manager 242
next-generation SIP mode 261
NextPlane
    XMPP federation 168
node elements 229
No DNS SRV records found for any Presence domain for XMPP Federation 296, 297
non-Presence/IM capable 261
Number of configured users is over the support limit 296

O

Offline IM Storage 212

Openfire Certificate 236, 237
OpenNMS 218, 223
  alarms event 231
  starting 225
  System Manager configuration 218
OpenNMS installation
  test 230
OpenNMS web console 226
overview 12
overview MS exchange 57

P

port 288
Port management 215
Port Management 215
port matrix 305
Prerequisites
  Zang federation 183
presAlarmTest 307
presCleanup 308
presClients 308
presCollectMetrics 310
presence 12
Presence/IM routing domain 264
presence-aware application 12
presence component 246
presence model 18
presence profile
  prerequisites 87
Presence Profile 266
presence services
  configuring microsoft federation attributes 137
Presence Services 15, 17
  Service Attributes 249
Presence Services Cluster FQDN 33
Presence Services deployment
  checklist 24
Presence Services Security Module HTTPS identity certificate 200
Presence Services session
  create 61
  import 61
presentity 12, 216
presGraphMetrics 312
presHealthCheck 313
PresServ_CLR_CluMon_01 289
presStatus 315
presUnlock 314
product compatibility 20
profile 179
providing access to a Aura user 78
PS connector 13

R

receive Microsoft Edge connections
receive Microsoft Edge connections *(continued)*
  configure TLS client profile 110
receive Session Manager connections
  configure TLS client profile 111
related documentation 304
repairing replication 301
restart 90, 233
  cluster 233
Restarting
  Front End service 90
retrieving
  Microsoft Edge CA certificate 107
root CA certificate 56
  Windows 238
root certificate
  cisco jabber 176
roster 216
roster limit
  configure 217
Roster limit is exceeded 295
Roster Limit Maximum Number of Contacts 217
Roster size enforcement 216
routing 149
routing configuration
  between session manager and session border controller 132
routing policy setup
  session manager 135

S

SAN 176, 235, 236
sanp-in service
  delete 43
SBCE
  administrator login 106
  configuration 104
scalability 285
Security Module HTTPS Identify Certificate 235, 236
Security Settings
  Openfire 156
  TCP 155
self-signed certificate
  cisco jabber 172
sending SMS
  private contacts 187
  REST APIs 187
Server does not have an associated Presence Services managed element 297, 298
server reachability 163
Server to Server Settings
  Openfire 155
Service Attributes 249
service port 215
Session Manager
  configuring TLS client profile 109
  external signaling interface configuration 113

Session Manager *(continued)*
- routing 149

Session manager identity 268
session manager routing policies and regular expression to Avaya session border controller for enterprise for domain 1 143
session manager routing policies and regular expression to Avaya session border controller for enterprise for domain 2 145
setting
- Avaya session border controller for enterprise entity and entity link 133
- cluster attributes for external domain microsoft federation 137
- required certificates for session manager 133
- session manager regular expression 136
- session manager routing policy 135

setting up
- Microsoft Edge Border Rule 126

setup
- certificates for session manager 133

Signaling security health check alarms 296
signed Cisco certificate 182
Signed Openfire Certificate 241
signing the Domino Calendar web service database 68
single-server deployment 24
SIP dialog 33
SIP Entity 30
SIP federated domain configuration 131
SIP mode 261
SIP SIMPLE 18
smgrPresenceUserAccessControl 316
snap-in
- loading 34

snap-in service
- uninstall 43

soft delete 208
Software Inventory web service 189
SRV 169
start 90, 233
stop 90, 233
Subject Alternative Name 176, 235, 236
subscribe
- for status with Microsoft RTC 97
- publish status to Microsoft RTC 97

support 306
support IM 301
support Presence 301
System Manager CA signed Certificate 242
System Manager LHNR 33, 40
system service attributes 34

T

TCP 155, 158
third-party CA
- dentity certificate 246

TLS 159
TLS client profile configuration
- Microsoft Edge 108
- receive connections from Microsoft Edge 110
- receive connections from Session Manager 111
- Session Manager 109

training 305
trusted certificate 149
two-way 216

U

upgrading Microsoft Federation
- considerations 52

user administration 261
user and endpoint administration 147, 261, 265, 269, 274, 275
user configuration 261
user level access control 317
user management
- Aura client 150

V

videos 306
VMware vSphere Client 26
Vysper 300

W

watcher 12, 216
WebSphere identity certificate 202
Windows 237

X

XMPP 18
XMPP connection 33
XMPP federation 151, 158, 159
- Cisco Jabber 168
- Geographic Redundant deployment 165
- NextPlane 168

Z

Zang federation
- configuation 185
- configuration 185
- configure users 186

Zang Federation 183
- enabling 184