Avaya Aura® Presence Services 6.2.5

Service Pack Release Notes

Issue 1.0
July 2014

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE

http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

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

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 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 Web site: http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Introduction

This document introduces the Avaya Aura® Presence Services Release 6.2.5 and describes known issues and the issues resolved in this release.

Product Notices

Important product changes and updates are documented in one or more Product Support Notice (PSN) articles. The PSN number defines the related document.

To read a PSN description online:

1. Open the browser, and navigate to http://support.avaya.com.
2. On the main menu, click Downloads and Documents.
3. In the Enter Your Product Here field, enter **Presence Services** or select **Avaya Aura® Presence Services** from the list.
4. In the Choose Release field, click 6.2.
5. Click Documents.
6. Check Product Support Notices.
7. Click Enter.
8. To open a specific PSN, click the PSN title link.

Release Note Contents

Applicability

This release is part of the Avaya Aura® 6.2 Feature Pack 4 (FP4) release. It **must** be applied in conjunction with FP4 updates for other Avaya Aura® applications in use within the same deployment. Please refer to the Compatibility Matrix on support.avaya.com and specific application documentation for required versions.

⚠ **IMPORTANT**

Presence Services 6.2.5 must be deployed with System Manager 6.3.8 or higher. This release of Presence Services is not compatible with older versions of System Manager. System Manager must be upgraded to 6.3.8 or higher prior to deploying Presence Services 6.2.5.

Application	Certified Version	Minimum Supported Version	Mandatory / Optional
Avaya Aura® System Manager	6.3.8	6.3.8	M
Avaya Aura® Session Manager	6.3.8	6.3.8	O
Avaya Aura® Communication Manager	6.3.x	6.3.x	O
Avaya Aura® System Platform	6.3.4	6.3.1	O
Avaya Aura® Application Enablement Services	6.3.x	6.3	O
Avaya one-X® Client Enablement Services	6.2.3	6.2.3	O
Avaya Communication Server 1000	7.6	7.5	O
IBM® Domino®	8.5.3	8.5.3	O
Microsoft OCS	2007 R2 Enterprise	2007 R2 Enterprise	O
Microsoft Lync®	Lync 2013	Lync 2010	O
Microsoft Exchange	Exchange 2010 SP1	Exchange 2010 SP1	O

For the most up-to-date application compatibility list, please refer to the Avaya Compatibility Matrix at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Software Development Kit

The Local Presence Service (LPS) SDK (Software Development Kit) is available as follows:

File name	Presence Services Compatibility
lps2_sdk_06_02_04_00-01_SNAPSHOT-24.zip	Presence Services 6.2.4 or higher
lps2_sdk_06_02_02_00-01_20130916.zip	Presence Services 6.2.2 – 6.2.4 (refer to *LPS SDK Compatibility* section of this document)

For more information about the Presence Services LPS SDK and other Avaya SDKs, please refer to Avaya DevConnect at http://devconnect.avaya.com.

Software Release History

Version	Release Type	Status	Release Date
PS-06.01.00.00.0502	Major / Minor	Generally Available	
PS-06.01.00.01-0504	Patch	Generally Available	
PS-06.01.00.02-0504	Patch	Generally Available	
PS-06.01.01.00-0610	Service Pack	Generally Available	
PS-06.01.01.01-0608	Patch	Generally Available	
PS-06.01.02.00-0903	Service Pack	Generally Available	Mar 2012
PS-06.01.02.01-0903	Patch	Generally Available	May 2012
PS-06.01.02.02-0903	Patch	Generally Available	May 2012
PS-06.01.02.03-0909	Patch	Generally Available	Jun 2012
PS-06.01.02.04-0909	Patch	Generally Available	Jul 2012
PS-06.01.05.00-1204	Feature Pack 1	Generally Available	Dec 2012
PS-06.01.05.01-1204	Patch	Generally Available	Jan 2013
PS-06.01.05.02-1204	Patch	Generally Available	Jan 2013
PS-06.01.05.03-1204	Patch	Recalled – Do not use	May 2013
PS-06.01.05.04-1204	Patch	Recalled – Do not use	May 2013
PS-06.01.05.05-1204	Patch	Generally Available	May 2013
PS-06.01.05.06-1204	Patch	Generally Available	May 2013
PS-06.01.05.07-1204	Patch	Generally Available	July 2013
PS-6.2.0.0-182	Feature Pack 2	Generally Available	May 2013
PS-6.2.0.1-182	Patch	Generally Available	May 2013
PS-6.2.0.2-182	Patch	Generally Available	Feb 2014
PS-6.2.1.0-201	Service Pack	Generally Available	May 2013
PS-6.2.1.1-201	Patch	Directed	May 2013
PS-6.2.1.2-201	Patch	Generally Available	May 2013
PS-6.2.1.3-201	Patch	Generally Available	June 2013
PS-6.2.1.4-201	Patch	Generally Available	June 2013
PS-6.2.1.5-201	Patch	Generally Available	July 2013
PS-6.2.1.6-201	Patch	Generally Available	July 2013
PS-6.2.1.7-201	Patch	Generally Available	July 2013
PS-6.2.1.8-201	Patch	Recalled – Do not use	August 2013
PS-6.2.1.9-201	Patch	Generally Available	August 2013
PS-6.2.1.10-201	Patch	Generally Available	August 2013
PS-6.2.2.0-304	Feature Pack 3	Generally Available	October 2013
PS-6.2.1.11-201	Patch	Generally Available	October 2013
PS-6.2.1.12-201	Patch	Generally Available	October 2013
PS-6.2.3.0-317	Service Pack	Generally Available	December 2013
PS-6.2.3.1-317	Patch	Generally Available	December 2013
PS-6.2.3.2-317	Patch	Generally Available	December 2013
PS-6.2.3.3-317	Patch	Generally Available	January 2014
PS-6.2.3.4-317	Patch	Generally Available	January 2014
PS-6.2.3.5-317	Patch	Generally Available	March 2014
PS-6.2.3.6-317	Patch	Generally Available	April 2014
PS-6.2.4.0-641	Feature Pack 4	Generally Available	June 2014
PS-6.2.4.1-641	Patch	Generally Available	June 2014
PS-6.2.4.2-641	Patch	Generally Available	July 2014
PS-6.2.5.0-85	Service Pack	Generally Available	July 2014

New Installations

New Install Quick Reference	Download	Prerequisite Downloads
Standalone (software-only)	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	*None*
Avaya Aura® Presence Services template for Avaya Aura® System Platform	*Supports Upgrades Only – Refer to Upgrades section below*	*None*
Avaya Aura® Solution for Midsize Enterprise template for Avaya Aura® System Platform	*Supports Upgrades Only – Refer to Upgrades section below*	*Refer to Midsize Enterprise documentation*
Avaya Aura® Presence Services for Avaya Aura® Virtualized Environment	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	PS-6.2.0.0-182-VM-29.ova (PLDS ID: PS000000049)

New installations of Presence Services 6.2.5, on platforms that are not currently running Presence Services, are only supported using the following deployment method:

- **Standalone (Software-only)**
  Download and install the Avaya Aura Presence Services 6.2.5 Software (PS-6.2.5.0-85.zip) on a clean system per the *Deploying Avaya Aura® Presence Services* User Guide.
- **Virtualized Environment (VE)**
  Download and install the Avaya Aura Presence Services 6.2.0 Software (PS-6.2.0.0-182-VM-29.ova) on a clean system per the *Deploying Avaya Aura® Presence Services* User Guide, delete and replace the PS-6.2.0.0-182.zip file with the PS-6.2.5.0-85.zip file and complete the installation as per the installation guide.
-

NOTE
At the time general availability of Presence Services 6.2.5 was announced no patches were available for download from support.avaya.com. It is important that any GA patches available at a later date be applied as part of all 6.2.5 deployments.

Upgrades

Upgrades to release 6.2.5 are supported from the following releases only:

Release	Minimum Required Version
Avaya Aura® Presence Services 6.2.0	PS-6.2.0.2-182 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Feature Pack 3	PS-6.2.3.4-317 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Feature Pack 4	PS-6.2.4.0-641 + any additional patch(es)

NOTE

Presence Services patches are not cumulative! Patches must be installed sequentially on each Service Pack. Only qualified personnel should attempt patch installation.

NOTE

Do not stop Presence Services prior to starting the upgrade process.

Upgrade Quick Reference	Download	Prerequsite Downloads
Standalone (software-only)	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	*None*
Avaya Aura® Presence Services template for Avaya Aura® System Platform	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	vsp-6.3.4.0.08007.0.iso (PLDS ID: PS000000081)
Avaya Aura® Solution for Midsize Enterprise template for Avaya Aura® System Platform	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	*Refer to Midsize Enterprise documentation*
Avaya Aura® Presence Services for Avaya Aura® Virtualized Environment	PS-6.2.5.0-85.zip (PLDS ID: PS060205000)	*None*
Avaya Aura® Presence Services Migration Tool for System Manager 6.3.8	ps-comm-profile-migration-6.2.4.0.zip (PLDS ID: PS000000072)	*None*

IMPORTANT

There are a number of significant changes to basic administration required for Presence Services users in this release. Please refer to the *Administering Avaya Aura® Presence Services* User Guide for complete details. In addition, if upgrading from 6.2.0 or 6.2.3 to 6.2.5 you must run the Presence Services Migration Tool on System Manager 6.3.8 prior to upgrading Presence Services. Failure to do so will result in total out-of-service condition of Presence Services functionality! There is no need to run the migration tool if you are upgrading from 6.2.4 to 6.2.5.

In order to run Presence Services 6.2.5, upgrades should be performed using one of the following methods:

- **Standalone (Software-only)**
  Download and install the Avaya Aura Presence Services 6.2.5 Software (PS-6.2.5.0-

85.zip) on an existing Presence Services 6.2.0, 6.2.3 or 6.2.4 deployment. See Software Installation and Upgrade.

- **Avaya Aura® Presence Services Template for System Platform**
Download and install the Avaya Aura Presence Services 6.2.5 Software (PS-6.2.5.0-85.zip) on an existing Presence Services 6.2.0 template on a certified platform running Avaya Aura® System Platform 6.3.4 (or later – check for applicable PCNs on support.avaya.com) per the *Deploying Avaya Aura® Presence Services* User Guide and Software Installation and Upgrade. Note: the Presence Services 6.2.0 template must already be running Presence Services 6.2.0, 6.2.3 or 6.2.4.
- **Avaya Aura® Solution for Midsize Enterprise**
Download and install the Avaya Aura Presence Services 6.2.5 Software (PS-6.2.5.0-85.zip) on an existing Avaya Aura® Solution for Midsize Enterprise 6.2.2 template on a certified platform running Avaya Aura® System Platform. Refer to Midsize Enterprise documentation and Software Installation and Upgrade. Note: the Midsize Enterprise 6.2.2 template must already be running Presence Services 6.2.0, 6.2.3 or 6.2.4.
- **Avaya Aura® Presence Services for Avaya Aura® Virtualized Environments**
Download and install the Avaya Aura Presence Services 6.2.5 Software (PS-6.2.5.0-85.zip) on an existing Avaya Aura® Presence Services VMware Ready™ vApp running Presence Services 6.2.0, 6.2.3 or 6.2.4 within the virtualized environment as per *Deploying Avaya Aura® Presence Services* User Guide and Software Installation and Upgrade.

NOTE
At the time general availability of Presence Services 6.2.5 was announced no patches were available for download from support.avaya.com. It is important that any GA patches available at a later date be applied as part of all 6.2.5 deployments.

Patches

Be sure to apply any applicable service packs and patches posted on support.avaya.com to the system after applying this release. Check support.avaya.com frequently for important software updates as documented in Product Support Notices.

Capacity Limits

Avaya Aura® Presence Services 6.2.5 supports the following:

Endpoint Mode	# Endpoints supported	Avg # Contacts per user	Max # Contacts + Watchers per user	# Subscriptions/ Minute/node	# Presence updates per second/node
SIP	16,000 max on single node, 125,000 on 8 node cluster*	25	150**	300	30
H.323 (XMPP)	16,000 max on single node, 125,000 on 8 node cluster*	25	150**	300	**30**

** Clustered deployments of Presence Services are limited to a maximum of 8 nodes in a cluster and all nodes in a cluster must reside on the same subnet.*

*** By default, the following setting on the XCP web interface is enabled, with a value of 150: Presence Session Manager -> System Parameters -> Roster Configuration. This limits the total number of contacts + watchers that any non-SIP user can have. For instance, if H323 UserX adds 100 contacts (ie UserX watches 100 contacts), then no more than 50 users can add UserX as a contact (ie max 50 users can watch UserX). Conversely, if 150 users add UserX as a contact (ie 150 users watch UserX), then UserX can add no contacts (ie UserX can watch no-one). When this limit is reached, Presence Services sends an error message to client devices in response to an attempt to add an additional contact. In this situation, many Aura client devices currently allow the contact to be added; but that contact's presence will not be rendered (eg the contact's presence state will appear as Unknown).*

Feature	Restriction
AES Collector	2500 configured station monitors per collector (limited to 1/node)
IBM Domino Collector	16K users per collector (limited to 1 collector/node) – Domino limit may apply as each collector can only communicate with a single Domino server. There is a limit of one collector per node.
Microsoft Exchange Collector	16K users per collector (limited to 1 collector/node) – Exchange limit may apply as each collector can only communicate with a single Exchange server. There is a limit of one collector per node.
Clustering	8 nodes per cluster; 1 cluster per System Manager
High Availability	1 backup node per cluster

Avaya Presence / IM Clients

Avaya Aura® Presence Services supports many Avaya clients such as:

- Avaya Aura Agent Desktop
- Avaya one-X® Communicator (minimum version 6.2)
- Avaya one-X® Agent
- Avaya one-X® Attendant

- Avaya one-X® Mobile 6.2 (via CES server 6.2.3 or greater, telephony presence via AES integration)
- Avaya Flare® Experience (PC, iOS, Android, etc)
- Avaya one-X® Deskphone 96X0 Series & 96X1 Series SIP and H.323 (H.323 presence via AES integration) (minimum version 6.2)
- Avaya H.323 and DCP deskphones (presence via AES integration)
- Avaya Communicator 2.0

Please check with your sales representative or business partner if you have questions about Avaya clients not listed here.

NOTE

The Presence Services "ACL=Confirm" feature is only supported when used in conjunction with the Avaya one-X® Communicator 6.2 (or greater) release.

When updating Presence Services to a new release or service pack, please check client documentation to determine if a new version of the client is required to maintain optimum performance.

Resolved Issues and Enhancements

This release introduces support for the following new features:

- **Presence Services (PS) upgrades are no longer linked to the completion of DRS replication**
  Previously PS upgrades would not complete until DRS (Data Replication Service) replication between PS and System Manager (SMGR) was complete. In PS 6.2.5.0 PS upgrades will complete without waiting for DRS to complete. This will reduce the chances of upgrade failures.

NOTE

Although upgrades to PS 6.2.5.0 will now complete even if DRS replication has not completed, the Presence Services application will not be usable until DRS replication between Presence Services and System Manager is finished. The time required for DRS replication to complete depends on the number of users configured with a Presence Profile. It may take up to 10 minutes for DRS replication to complete if 16K users are configured.

- **Support for TLS connectivity between Presence Services and Openfire**
  Presence Services now supports TLS for the server to server XMPP connection with Openfire. See deployment instructions at the end of this document.

- **OpenSSL upgraded to 1.0.1g**
  OpenSSL has been upgraded from 0.9.8o to 1.0.1g

- **Improved AES collector performance**
  The Presence Services AES collector has been enhanced to speed up performance during system recovery. Previously it would take approximately 20 minutes to process the subscription requests for 2500 endpoints via the AES collector. In PS 6.2.5 the time required to process 2500 subscription requests has been reduced to approximately 3 minutes.

- **Support for TLS 1.2**
  Presence Services now supports TLS 1.2.

- **Presence Services supported in Multi Device Access (MDA) solutions**
  Presence Services is now compatible with solutions using MDA. Please refer to the MDA whitepaper for further details and specific limitations.
  https://downloads.avaya.com/css/P8/documents/100181252

NOTE

Presence/IM is limited to one IM-enabled client per user when using MDA.

Resolved Issues and Enhancements

The Presence Services 6.2.5 service pack is cumulative and contains all fixes and enhancements contained in earlier Presence Services releases plus the following:

Tracking #	Issue
PRES-3721	OOD NOTIFY sent to SM is missing Event header
PRES-3699	RFE: The "IM Gateway" field in PS comm profile should be provisionable
PRES-3694	PS to SM link is 500 service unavailable when registering 9k SIP users
PRES-3688	CFD: AES Collector publishes tuple with activity=cf when call-forwarding is enabled on CM
PRES-3677	RHN Errata Alert: tzdata enhancement update
PRES-3674	Change in SMGR IP address is not picked up by Presence Services
PRES-3641	Client con't connect to Backup PS after HA Fallover
PRES-3636	1XM (CES) + 1XC: Removing note reverts to previous note
PRES-3634	LPS PUBLISH sporadically returning 500 Session Creation Failure
PRES-3632	NPEs logs when the user identity is wrong
PRES-3629	Improve Error Messages when Rules Engine Exceptions occur in the Migration Tool
PRES-3619	ME HA: Presence Session Manager sporadically stopped after a failover initiated by power down of the primary server
PRES-3614	Upgrade hangs while executing and never completes
PRES-3622	RFE: modify install/upgrade to remove synchronous DRS load (get_initial_load.sh)
PRES-3606	Upgrade of HA node results in incorrect HA and monit status
PRES-3580	Install hardening
PRES-3578	Deleting user from SMGR does not delete ACL rules in PS
PRES-3559	Phone reboot intermittently while registered as MDA with team button and presence configured
PRES-3557	Invalid redirection in 2 scripts creates files "1" and "2"
PRES-3507	Polite block directed presence for external users
PRES-3461	PS cannot handle SSL negotiation for ClientHello having TLS1.0 base version and flexible to negotiate up to TLS1.2
PRES-3251	RFE: install sysstat RPM to enable capture of SAR data
PRES-2869	RFE: Replace SSL-C library with OpenSSL

Please refer to previous release notes and PCNs for information about updates introduced in earlier releases.

Known Issues and Workarounds

The following issues were known at the time of the release of Presence Services 6.2.5:

Tracking #	Issue
PRES-3725	vi: Status change of DCP desk phone is not updated to Watcher **Problem Description**: When using ASAI v6 with the PS AES collector older analog and digital desk phones which do not support user login/logout events will be reported as Offline to watchers. **Workaround:** Administrators can work around this issue by using ASAI v5 when setting up the PS AES collector.
PRES-3633	Changing into DENY from Allow, wont reflect properly into the Presence state of the User **Problem Description**: In cases when a user changes the ACL setting from Allow to Deny on a client the change does not take effect until the end user has logged out and logged back in on the client. **Workaround:** After changing the ACL setting from Allow to Deny the end user will need to log out and then log back in.
PRES-3153, GRIP 9522	Cluster: SIP clients have no presence status updates after a single node restart **Problem Description**: On cluster deployments if a single node in the cluster is restarted SIP endpoints will not re-subscribe right away and as a result the presence status displayed on the watchers will be incorrect. This issue will automatically correct itself when the SIP re-subscribe timer expires or when the affected users logout and log back in. This issue will be addressed when the endpoints have adopted support for presence out-of-dialog REFER messages. The Avaya Aura® core components include this support in the Feature Pack 4 release. **Workaround:** Affected users must log out and log back in, or wait until the SIP re-subscribe timer expires.
PRES-2600	DRS status page shows double entries of Presence 6.1 and Presence 6.2 for presence after upgrade ME from 6.1 to 6.2.2 **Problem Description:** DRS status page shows double entries of Presence 6.1 and Presence 6.2 for presence after upgrade ME from 6.1 to 6.2.2 **Workaround:** If there are no other PS servers running 6.1 against that System Manager, the psreplica_6.1 can be deleted on System Manager
PRES-2317	XMPP Federation: Aura user cannot be added into a chat room initiated by Federated user **Problem Description:** If an endpoint on Openfire invites a federated Aura user into a chat room the Aura user is unable to enter the chatroom. **Workaround:** At present no workaround is available.
Note:	If an SMGR upgrade is required as part of upgrading to PS 6.2.5.0 please note that there is a limitation in the SMGR upgrade logic which results in the system wide ACL setting to revert to a value of ALLOWED. So if the system setting in SMGR is ACL=Confirm, after an SMGR upgrade the administrator will need to change the ACL setting from ACL=Allowed to ACL=Confirm. This limitation in the SMGR upgrade logic will be addressed in SMGR 7.0.

	Workaround: After an upgrade of the SMGR, change the ACL value to Confirm if that is the value that existed prior to the SMGR upgrade.
Note:	BoCo client: After blocking/unblocking watcher, presence does not flow to watcher **Problem Description:** This issue is the result of a problem in the BoCo endpoint and will only impact customers that are using this third party (BoCo) endpoint. User A = Various User B = BoCo client hosted by Openfire server User A attempts to add User B as contact Confirmation dialog appears on User B's BoCo client, User B selects Block As expected, User A is added to User B's buddy list as "Blocked, on Openfire server the Subscription state is set to "none", and User A cannot see User B's presence (eg depending on User A's client type, User B's status may be shown as "Unknown") User B now Unblocks User A, but User A cannot see User B's presence. For example, depending on User A's client type, User B's status may be shown as "Available" after User B unblocks, but subsequent presence state changes by User B are not seen by User A. If User B now blocks and unblocks User A again, it appears to fix the problem, but in fact this is not the case. In this situation, a one-time presence state change is sent to User A, but subsequent state changes on User B are not seen on User A. Root cause appears to be: when User B unblocks User A, BoCo client does not change Subscription state on Openfire server from "none" to "From". Observed with BoCo client version 3.4.4.3 69105 Appears to be an issue with BoCo client rather than Openfire server. Issue not observed if attempted on Openfire server with a non-BoCo client such as Gajim (http://gajim.org/) Reproducible in federated or non-federated deployment. That is, this problem is observed whether User A is another Openfire/BoCo user hosted by the same Openfire server, or for instance an Aura/OneX Communicator user hosted by a federated Avaya Aura Presence Services server **Workaround:** From Openfire Server -> Users - > Select user -> Roster state, manually change subscription state from “none” to “From” (in this scenario) or "Both" (if User B also wishes to watch User A). See attached screenshot.
Note:	**Problem Description**: After an Avaya contact is removed from a XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user. **Workaround** Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back in to the Avaya client
Note:	Secondary DNS parameter change: The current implementation only supports a change of the Primary DNS network parameter via System Platform User interface. Furthermore, the /etc/resolv.conf system file must contain only two line entries for • search domain • nameserver
Note:	For ME deployments changing the FQDN of a Presence Server does not automatically modify the Manage Elements table. As a result, the administrator must modify the "name" of the manage element in SMGR to match the PS's FQDN short name AFTER the NPC (Network Parameter Change) changes have completed. It is recommended that this name change be implemented immediately after the NPC changes have completed

	to ensure that subsequent IP address changes to the PS do not result in a new Manage Element in the SMGR.
Note:	Installations with Lync Federation using Avaya Aura SIP endpoints cannot use an Aura SIP Domain that is the same as the Lync SIP TLS Federated Domain. Doing so will result in lack of presence for Aura SIP endpoints. Ensure that the Aura SIP Domain used by SIP endpoints is different than the Lync Federation domain.

Changes Affecting Upgrades to 6.2.4 and 6.2.5

The changes and notes outlined below are only applicable for upgrades from 6.2.0 and 6.2.3 to 6.2.5. These changes and notes are not applicable for upgrades from 6.2.4 to 6.2.5.

Avaya Aura® Presence Services 6.2.4 and Avaya Aura Feature Pack 4 introduce significant changes that affect upgrades:

- An Avaya Aura System Manager (System Manager) enrollment password is required during an Avaya Aura Presence Services upgrade, but in FP4 this is no longer exposed on the System Manager web interface (System Manager Home > Services > Security > Certificates > Enrollment Password).

- Avaya Aura System Manager FP4 (6.3.8) generates SHA-256 root certificates; Avaya Aura Presence Services 6.2.4 supports SHA-256 certificates; and SHA-256 support is available in Avaya Aura Presence Services 6.2.0 via PS-6.2.0.2-182 (aka PS 6.2.0 patch 2), and Avaya Aura Presence Services 6.2.3 via PS-6.2.3.4-317 (aka PS 6.2.3 patch 4).

- Avaya XMPP communication addresses (System Manager Home > Users > User Management > Manage Users > Communication Profile > Communication Address > Type = Avaya XMPP) have been renamed to Avaya Presence/IM.

- Avaya Presence/IM communication addresses are no longer automatically created; they must be configured on System Manager (similar to other communication addresses such as Avaya SIP and Avaya E.164).

- Domain Substitution Rules have been removed (previously at System Manager Home > Elements > Presence) and Router Service Name is no longer prompted for within the Presence Services installer.

- When a System Manager administrator configures an Avaya Presence/IM communication address (in user@domain format), the user portion is entered by the administrator, and the domain portion is selected from a pull-down, which is populated based on SIP routing domain instances (System Manager Home > Elements > Routing > Domains > Type = SIP). A System Manager administrator can use the same or a different SIP routing domain when configuring Avaya Presence/IM and Avaya SIP communication addresses.

- In FP4, multiple presence domains are supported. That is:
    - Prior to FP4, the domain portion of all Avaya XMPP communication addresses (System Manager Home > Users > User Management > Manage Users > Communication Profile > Communication Address > Type = Avaya XMPP) on a Presence Services server were identical.

  - In FP4, it is possible to define multiple instances of SIP routing domains (System Manager Home > Elements > Routing > Domains > Type = SIP) and it is possible to create one user with an Avaya Presence/IM communication address (System Manager Home > Users > User Management > Manage Users > Communication Profile > Communication Address > Type = Avaya XMPP) in one SIP routing domain, and another user with an Avaya Presence/IM communication address in a different SIP routing domain.

- Presence Profile (System Manager Home > Users > User Management > Manage Users > Communication Profile > Presence Profile) is mandatory in order to enable presence for a user, and a new mandatory System attribute has been introduced. Additionally, the attribute previously named "Primary PS Server SIP Entity" has been renamed to "SIP Entity" – this read-only attribute is automatically populated by the system.

- Presence Services federation with third-party XMPP or Microsoft OCS/Lync servers has undergone significant improvements. As a result of these improvements, an RTC Collector or XMPP Collector no longer needs to be configured (previously visible from the Presence Services XCP Controller web interface at Components -> RTC Collector, or Components -> XMPP Collector). During an upgrade to Presence Services 6.2.4, any instances of an RTC Collector or XMPP Collector are automatically removed.

- In FP4, the Postgres configuration directory has been renamed from /var/lib/pgsql/data to /var/lib/pgsql/9.2/data. Among other things, the configuration file in this directory may be used to enable remote access to Presence Services' Postgres database from applications such as Avaya one-X Client Enablement Services (CES) which use the Local Presence Service (LPS) SDK (Software Development Kit).

Mandatory Steps Required Prior to Upgrade to 6.2.5

1. If upgrading from 6.2.0 or 6.2.3 a SHA2 patch must be applied to the Presence Services server prior to upgrading System Manager, otherwise TLS connectivity between System Manager and Presence Services will fail after the System Manager upgrade. Ensure that Avaya Aura Presence Services is running one of the following loads:

   - PS-6.2.0.2-182 (aka PS 6.2.2 Patch 2)
   - PS-6.2.3.4-317 (aka PS 6.2.3 Patch 4)

2. On Avaya Aura® System Manager, record the enrollment password, which is available on the System Manager web interface (prior to SMGR FP4) at Home > Services > Security > Certificates > Enrollment Password. This will be required during step 9.

3. On Avaya Aura® System Manager, it is recommended that all users with an Avaya XMPP communication address (System Manager Home > Users > User Management > Manage Users > Communication Profile > Communication Address > Type = Avaya XMPP) be recorded. This can be done using System Manager's user export capability, available at System Manager Home > Users > User Management > Manage Users > More Actions > Export All Users. This will be required if performing the post-System Manager-upgrade steps in 5a and 5b. This can potentially take a long time, so if the installation includes a large number of users, consider exporting a selective subset of users.

4. Prior to upgrading Avaya Aura® Presence Services to 6.2.5, Avaya Aura System Manager must first be upgraded to FP4. Upgrade Avaya Aura System Manager to 6.3.8 (GA) or higher.

5. After the System Manager upgrade, verify the following:

   - For every user with an Avaya XMPP communication address that existed in the FROM load (as recorded in step 3), that user still exists, and the presence communication address still exists, but its type has been renamed to Avaya Presence/IM. For example, in the FROM load, if a user existed in System Manager Home > Users > User Management > Manage Users > Communication Profile, with a Communication Address of Type Avaya XMPP and value userA@example.com, then after the upgrade that user should still exist, with a communication address of Type Avaya Presence/IM and value userA@example.com. Similar to step 3, if the installation includes a large number of users, it can potentially take a long time to export all users, so a selective subset of users can be exported for comparison against the users recorded in step 3.

   - A new SIP routing domain instance has been created (System Manager Home > Elements > Routing > Domains > Type = SIP), if it didn't already exist, which matches the domain of the Avaya Presence/IM communication addresses described above.

It is recommended that steps 6-9 be done immediately after steps 4-5.

6. Prior to upgrading Presence Services to 6.2.5, a Presence Services Element must be defined in System Manager:

   - If it doesn't already exist, create an entry with Type = Presence Services at System Manager Home > Services > Inventory > Manage Elements.

   - Populate the Group Member Id field within the Attributes tab, as described in the user guide included with the Presence Services Communication Profile Migration Tool (below).

7. Prior to upgrading Presence Services to 6.2.5, a SIP Entity must be configured at System Manager Home > Elements > Routing > SIP Entities, with a name that exactly matches the Presence Services instance at System Manager Home > Services > Inventory > Manage Elements, as described in the user guide included with the Presence Services Communication Profile Migration Tool.

8. Prior to upgrading PS to 6.2.5, assign a Presence Profile to each presence-enabled user:

   - In PS 6.2.5, in order to support presence/IM, a user in System Manager must have a Presence Profile assigned (System Manager Home > Users > User Management > Manage Users > Communication Profile > Presence Profile), and a mandatory System attribute must be configured. The System attribute is used to "home" a user to a Presence Services instance. Note that this is required whether a user is homed to a Presence Services server in a clustered or standalone deployment.

   - To simplify the creation of Presence Profiles for each presence-enabled user (where "presence-enabled" = a user with an Avaya Presence/IM communication address), administrators are encouraged to use the Presence Services Communication Profile Migration Tool. This utility is available on PLDS (PLDS ID: PS060205000) and includes a user guide.

   - Once the utility has been executed, verify that every user with an Avaya Presence/IM communication address (System Manager Home > Users > User Management > Manage Users > Communication Profile > Communication Address > Type = Avaya Presence/IM) has a Presence Profile (System Manager Home > Users > User Management > Manage Users > Communication Profile > Presence Profile) with a non-blank System attribute defined.

9. Upgrade Avaya Aura Presence Services, as described at Software Installation and Upgrade.

⚠ **IMPORTANT**

Presence Services administration should be avoided in a “mixed” FP3/FP4 Aura deployment. Continuing to administer changes while in this mode of operation may result is loss of service! It is recommended that both System Manager and Presence Services are both upgraded within the same maintenance window or, if that is not possible, avoid any presence-related configuration changes prior to upgrading Presence Services to 6.2.5.

⚠ **IMPORTANT**

If an SMGR upgrade is required as part of upgrading to PS 6.2.5.0 please note that there is a limitation in the SMGR upgrade logic which results in the system wide ACL setting to revert to a value of ALLOWED. So if the system setting in SMGR is ACL=Confirm, after an SMGR upgrade the administrator will need to change the ACL setting from ACL=Allowed to ACL=Confirm. This limitation in the SMGR upgrade logic will be addressed in SMGR 7.0.

Federation changes, upgrade implications (upgrades from 6.2.0 and 6.2.3 only)

Collectors automatically removed during upgrade to Presence Services 6.2.5

As described in *Administering Avaya Aura® Presence Services* User Guide, Presence Services federation with third-party XMPP or Microsoft OCS/Lync servers has undergone significant improvements in FP4. As a result, an RTC Collector or XMPP Collector no longer needs to be configured (previously visible from the Presence Services XCP Controller web interface at Components -> RTC Collector, or Components -> XMPP Collector). During an upgrade from 6.2.0 or 6.2.3 to Presence Services 6.2.5, any instances of an RTC Collector or XMPP Collector are automatically removed.

Implications to Microsoft OCS/Lync federation

Prior to FP4, federation to a Microsoft OCS/Lync server would have included the following:

- RTC Collector configured, visible from the Presence Services XCP Controller web interface at Components -> RTC Collector.
- Any OCS/Lync user was configured in System Manager with an Avaya Presence/IM (formerly Avaya XMPP) communication address, and Microsoft SIP (formerly MS OCS SIP) communication address.
- On an OCS/Lync device, there was no visibility as to which individual Aura users were watching the OCS/Lync user. Rather, the OCS/Lync device would have received a request for a single PS administrative user to watch the OCS/Lync user; the OCS/Lync user may have been asked (depending on device setting) to authorize this single PS administrative user (by authorizing this user, the OCS/Lync user had implicitly allowed all Aura users to watch him/her); and this single PS administrative user would have typically been visible in the buddy list of the OCS/Lync device (because Microsoft's default behavior is to establish a two-way watch).
- Only supported if Presence Services ACL policy is Allow.

Following an upgrade to PS 6.2.5:

- The RTC Collector is automatically removed.
- Any OCS/Lync users that were previously configured in System Manager remain unchanged.
- Following the PS 6.2.5 upgrade, the first time an OCS/Lync user logs in to the OCS/Lync device, that user may be prompted to authorize "self" as a watcher (where self = the Avaya Presence/IM communication address of the OCS/Lync user configured in System Manager). The user should allow this, by accepting the authorization request. This

replaces the PS administrative user, and by authorizing this watcher, the OCS/Lync user has implicitly allowed all Aura users to watch him/her.

- If the OCS/Lync device had previously displayed the PS administrative user within the contact list, then it will continue to do so after PS 6.2.5 upgrade, but this user is no longer valid, and the OCS/Lync user will always see this user's presence state as Unknown. The OCS/Lync user is encouraged to remove this user, but this is not mandatory.

- Note that, after the PS 6.2.5 upgrade, a much better federation experience is possible (support for non-Allow ACL policy; may not be necessary to configure OCS/Lync users in System Manager; ability for OCS/Lync presentities to see individual Aura watchers). See the *Presence Services federation with third-party servers* chapter of *Administering Avaya Aura® Presence Services* User Guide*.*

Implications to XMPP federation

All known pre-FP4 XMPP Federation deployments take advantage of “Phase 2 Federation”, as described in the following section of *Administering Avaya Aura® Presence Services 6.2.3*: Chapter 4 Configuring Presence Services > Configuring Presence Components > XMPP Federation > Federation Solutions.

Prior to FP4, PS federation to an XMPP (Openfire) server would have included the following:

- No XMPP Collector configured.

- External users, hosted by the third-party server, are not configured in System Manager.

- All ACL policies (Confirm, Allow, Block) are supported.

- When a user logged in to a third-party device hosted by the third-party server, s/he may be asked (depending on third-party server/device settings) to authorize individual Aura watchers as they attempted to add this user as a contact, and the list of watchers was likely visible from the third-party device.

Following an upgrade to PS 6.2.5, there are no changes. All contacts will still be visible (and authorized) within the buddy list of both third-party and Aura devices; presence state changes continue to be seen on both third-party and Aura watchers; and IMs can continue to be exchanged in both directions.

Determining Installed Version of Software

The currently installed version of Presence Services can be verified by logging in to the shell of the Presence Services machine and issuing the command:

```
/opt/Avaya/Presence/presence/bin/swversion.sh
```

Refer to the table in the Software Release History section to determine the installed release based on the version string.

Software Installation and Upgrade

You can upgrade to Presence Services 6.2.5 from 6.2.0, 6.2.3 or 6.2.4 on all supported platforms described in the Upgrades section of this document.

⚠ **IMPORTANT**

Do not stop Presence Services prior to starting the upgrade process.

Preparing for the Upgrade

⚠ **IMPORTANT**

There are a number of significant changes to basic administration required for Presence Services users in this release. Please refer to the *Administering Avaya Aura® Presence Services* User Guide for complete details. In addition, upgrades to 6.2.5 from either 6.2.0 or 6.2.3 must run the Presence Services Migration Tool on System Manager 6.3.8 prior to upgrading Presence Services. Failure to do so will result in total out-of-service condition for Presence Services functionality! The migration tool does not need to be run on upgrades from PS 6.2.4.

1. Take a backup of the existing Presence Services deployment and archive the backup file on a different server. Refer to *Administering Avaya Aura® Presence Services* for backup instructions.
2. Ensure that the operating system is Red Hat Enterprise Linux 5.7, 32-bit.
3. If Presence Services is deployed on System Platform, validate that all VMs are running the latest certified System Platform version.
4. If Presence Services is deployed on VMware, validate the ESXi server is running a supported 5.1 or 5.5 version.
5. Check the system status as described in Verifying Presence Services Health and ensure the system is operational.
6. Log in to System Manager Web Console, click Services > Replication.
7. Ensure that the Presence Services replica group is in a Synchronized state.
8. Click Security > Services > Certificates > Enrollment Password. Make a note of the existing enrollment password as you might need the enrollment password at some point

later during the installation. Also, ensure that the value for the Time Remaining field is sufficient for the duration of the installation process.

9. SSH to the Presence Services server. Login as a *cust* user. Change the user to root by providing the required credentials and from the shell issue the **`service postgresql-9.2 status`** command to ensure that the postgresql service is in a running state. If the postgresql service is not in a running state, issue the **`service postgresql-9.2 start`** command to start the service.
10. The PS installation requires a live network connection to a supported SMGR server. Note the following precautions to ensure the PS installation can execute with the highest chances of success:
    a. Ensure the network between SMGR and PS is in operational order.
    b. Ensure the SMGR server hostname is reachable from PS.
    c. Ensure the PS server hostname is reachable from SMGR.
    d. Check to ensure the network interface TCP MTU size is appropriately negotiated. Execute this command to ensure certs can be obtained from the SMGR:
        i. wget --no-check-certificate -q -O - https://<SMGR hostname>/ws/grservice/getgrstate/test
        ii. An XML block returned within a few seconds indicates success.
        iii. If the above command hangs, there may be an issue with the MTU size. Troubleshoot network connectivity. PS installation will fail if the above command fails.

Installing the Service Pack

⚠ **IMPORTANT**

Presence Services 6.2.5 must be deployed with System Manager 6.3.8 or higher. This release of Presence Services is not compatible with older versions of System Manager. System Manager must be upgraded to 6.3.8 or higher prior to deploying Presence Services 6.2.5.

⚠ **IMPORTANT**

If a System Manager upgrade is required as part of upgrading to PS 6.2.5.0 please note that there is a limitation in the current System Manager upgrade logic which results in the system wide ACL setting to revert to a value of ALLOWED. So if the system setting in System Manager is ACL=Confirm, after an SMGR upgrade the administrator will need to change the ACL setting from ACL=Allowed to ACL=Confirm. This limitation in the upgrade logic will be addressed in System Manager 7.0.

1. Download the Presence Services 6.2.5 zip file to the Presence Services server.
2. SSH to the Presence Services server as *cust.*
3. Change the user to *root* by providing required credentials.
4. Change to the directory where the zip file is located, and extract the file via the following command: **`unzip PS-6.2.5.0-85.zip –d PS-INSTALLER-6.2.5.0`**
5. Change to the installer directory: **`cd PS-INSTALLER-6.2.5.0`**

6. Edit the file named autoUpgrade_PS.properties and add/edit the following line: SCEP_PASSWORD=<*current System Manager enrollment password (without brackets)*>
   The enrollment password was obtained in Step 8 of Preparing for the Upgrade.
7. From the command line, type **`./PS-6.2.5.0-85.sh –ci autoUpgrade_PS.properties`**

Verifying Successful Software Installation

1. Once the install completes successfully, check the system status Check the system status as described in Verifying Presence Services Health and ensure the system is operational.
2. Consult Post Installation procedures within Release 6.2 *Deploying Avaya Aura Presence Services* User Guide for relevant post-upgrade checks.

Rolling back the Service Pack Installation

The documented procedure for performing a rollback is inconsistent. Following is the procedure to roll back from PS 6.2.5 (FROM load) to an earlier release (TO load):

1. This procedure requires that a backup was performed within the TO load. For instance, if rolling back from PS 6.2.5 to PS 6.2.4, the administrator must have backed up the PS 6.2.4 data into the archive directory via the backup.sh tool. The procedure to perform a backup is described in the “backup.sh tool” section of the *Administering Avaya Aura® Presence Services* User Guide.
2. SSH to the Presence Services server as root. Change to the installer directory (ie the directory into which the 6.2.5 installer file was unzipped, per step 4 of the “Installing the Service Pack” section of this document).
3. The system must be capable of displaying an X11 window. If necessary, enable X11 forwarding as described in the section named “Running Presence Services installation script”, within either the *Deploying Avaya Aura® Presence Services* User Guide, or the *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment* User Guide.
4. From the command line, enter **`./PS-6.2.5.0-85.sh –cu`** . The graphical uninstaller window opens. From the pull-down menu, choose **Uninstall**, and follow the prompts to completion.
5. Install the FROM load (eg PS 6.2.4). For instructions to install the FROM load, see either the *Deploying Avaya Aura® Presence Services* User Guide, or the *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment* User Guide, or the “Installing the Service Pack” section of this document.
6. After successfully installing the FROM load, restore the data from the archive directory via the restore.sh tool. The procedure to perform a restore is described in the “restore.sh tool” section of the *Administering Avaya Aura® Presence Services* User Guide.

NOTE
At the time general availability of Presence Services 6.2.5 was announced no patches were available for download from support.avaya.com. It is important that any GA patches available at a later date be applied as part of all 6.2.5 deployments.

Software Removal

1. Remove the newly deployed Presence Services application in the following scenarios:
    a. For Standalone/Software Only, perform an uninstall and a force clean. For more information on uninstallation, see the *Implementing Avaya Aura Presence Services* guide.
    b. For System Platform, uninstall the template. For more information on uninstallation, see the *Deploying Avaya Aura Presence Services* User Guide.
    c. For VMware, power-off the new VM and then delete it. For more information, see *Deploying Avaya Aura® Presence Services on VMware® in Virtualized Environment*.

NOTE
If you do not delete the old VM, you can power-on the old VM (ensuring the new VM is off/deleted) and skip the remaining steps in this procedure.

2. Reinstall/re-deploy the former PS version following installation/deployment procedures for the previous version.
3. Transfer the backup archive to the newly deployed system.
4. Use /opt/Avaya/Presence/presence/bin/restore.sh -f <archive file name> to restore the backup archive.
5. When the system finishes the restore process, log in to the XCP Controller Web interface and verify that all the processes are in a running state.

Verifying Presence Services Health

The following steps are intended to be a brief guide to aid in executing a minimal set of health checks of components involved in the Presence Services solution.

1. Access the PS XCP controller at https://<PS_IPAddress>:7300/admin and verify all the components are green.
2. Use the **`monit summary`** command to make sure that all processes shown are in “running” or ”accessible” state.
3. Run **`$PRES_HOME/presence/bin/presstatus`** tool to check the PS components status. Make sure that license is not expired and the user count under the user management component is correct
4. Make sure that the PS replica status is in a synchronized state. This can be checked from System Manager: **dashboard → services → replication**, choose appropriate replica group (eg psreplica_6.2fp4), locate node under Replica Node Host Name, check Synchronization Status. If Green synchronized, fine. If Yellow "Repairing" or Yellow

"Synchronizing", just wait and it should clear eventually. If Red Not Polling, or if it remains in Yellow for a long period of time, select and choose Repair

5. Run following command on Presence Services to confirm that the users are provisioned:
   ```
   psql -U postgres -d xcp -c "select count(*) from users;"
   ```
6. Make sure that alarms are working by generating a test alarm using the following utility:
   ```
   $SPIRIT_HOME/scripts/utils/generateTestAlarm.sh
   ```
   (Alarms can be viewed on the System Manager: dashboard →services → events → alarms section)

Managing Presence in a mixed Aura solution (System Manager FP4 and Presence Services pre-FP4)

⚠ **IMPORTANT**
Presence Services administration should be avoided in a “mixed” FP3/FP4 Aura deployment. Continuing to administer changes while in this mode of operation may result is loss of service! It is recommended that both System Manager and Presence Services are both upgraded within the same maintenance window or, if that is not possible, avoid any presence-related configuration changes prior to upgrading Presence Services to FP4.

As described earlier, the methodology for creation of Avaya Presence/IM (formerly XMMP) communication addresses differs between FP4 and pre-FP4.

In Aura (System Manager and PS) FP3 or earlier:

- Avaya XMPP communication addresses are automatically created, and this is triggered by PS.
- This can occur when Presence Services initially replicates with System Manager, or (if Presence Services is already replicating with System Manager) when a user is created/modified on System Manager.
- Creation of an Avaya XMPP communication address is based on a user’s Login Name (System Manager Home > Users > User Management > Manage Users > Identity > Login Name); domain substitution rules (System Manager Home > Elements > Presence); and Router Service Name configured within the Presence Services installer.
- A single presence domain is supported.

In Aura (System Manager and PS) FP4:

- Avaya Presence/IM communication addresses are configured by an System Manager administrator, similar to Avaya SIP or Avaya E.164 communication addresses.
- Domain substitution rules are no longer exposed at System Manager Home > Elements > Presence, and Router Service Name is no longer prompted for within the Presence Services installer.
- Multiple presence domains are supported, as defined at System Manager Home > Elements > Routing > Domains > Type = SIP.

Following are some examples of how presence is managed in various scenarios.

Fresh install of System Manager FP4 and PS FP4:

- Configure one or more SIP routing domains.

- During/after user creation, configure an Avaya Presence/IM communication address, using a SIP routing domain to populate the domain portion of the communication address.

Upgrade both System Manager and PS to FP4:

- During the System Manager upgrade, a SIP routing domain instance is automatically created based on existing Avaya XMPP communication addresses
- During the System Manager upgrade, presence communication addresses are preserved, but are renamed from type = *Avaya XMPP* to *Avaya Presence/IM*
- After upgrading PS, during/after user creation on System Manager, configure an Avaya Presence/IM communication address, using a SIP routing domain to populate the domain portion of the communication address.

Upgrade System Manager to FP4, but PS remains at pre-FP4:

- During the System Manager upgrade, a SIP routing domain instance is automatically created based on existing Avaya XMPP communication addresses
- During the System Manager upgrade, presence communication addresses are preserved, but are renamed from type = *Avaya XMPP* to *Avaya Presence/IM*
- After the System Manager upgrade, domain substitution rules are no longer externally visible on System Manager, but are internally retained within System Manager and PS.
- The pre-FP4 PS continues to trigger creation of presence communication addresses, based on a user's Login Name; the domain substitution rules that were previously defined in System Manager pre-FP4 (and are still internally retained in the pre-FP4 PS); and the Router Service Name that was configured when the PS was initially installed.
- As such, an System Manager administrator should not configure Avaya Presence/IM communication addresses on System Manager.
- Despite this, if an System Manager administrator does configure an Avaya Presence/IM communication address on System Manager in this mixed (System Manager FP4, PS pre-FP4) deployment, following is the system behavior:
  - If the domain of the Avaya Presence/IM communication address aligns with the domain substitution rules and Router Service Name internally stored within PS, then the Avaya Presence/IM communication address will be valid (ie it can be used for IM and presence), and it will not be removed from System Manager.
  - If the domain of the Avaya Presence/IM communication address does not align with the domain substitution rules and Router Service Name internally stored within PS, then the Avaya Presence/IM communication address will be invalid (ie it cannot be used for IM and presence), and either PS will automatically trigger its

replacement on System Manager with a valid communication address (if the user’s Login Name matches the domain substitution From rule), or the existing communication will remain on System Manager but will not be usable.

Configuring TLS between Presence Services and OpenFire

The following section is specific to SSL/TLS. For a full description of the steps required to federate between Avaya Aura® Presence Services and Openfire, see the section named "XMPP Federation Configuration" within the *Administering Avaya Aura® Presence Services* User Guide. In particular, ensure that SRV records are added to the DNS server, as described in the above document.

Certificates

For both PS and Openfire a CA signed certificate must be used to established trust. The certificate on PS is already a CA signed certificate by default and is signed by the System Manager. While not a requirement, Openfire can also be set-up to use a System Manager CA signed certificate. The System Manager cannot sign DSA certificate requests so we leave the DSA certificate as self-signed on Openfire. The process is below:

System Manager

1) Log onto System Manager
2) Navigate to Security->Certificates->Authority
3) Under RA Functions click Add End Entity
4) Create a username & password (i.e. openfire & Password1!)
5) Add the Openfire XMPP domain as the CN name
6) Add the Openfire IP Address as the Unstructured Name, IP Address [optional]
7) Add the Openfire FQDN as the Unstructured Name, Domain name (FQDN) [optional]
8) Select ENDUSER as the Certificate Profile
9) Select tmdefaultca as the CA
10) Check the Administrator box
11) Complete the entry by clicking Add End Entity

Openfire

1) Log onto Openfire
2) Navigate to Server Settings->Server Certificates
3) Click 'here' under the Signing Request
4) Enter the Openfire XMPP domain as the Name
5) Add the Organizational Unit (i.e. PS)
6) Add the Organization (i.e. Avaya)
7) Add the City (i.e. Ottawa)
8) Add the State (i.e. Ontario)
9) Add the Country Code (i.e. CA)
10) Click Update information
11) Copy the **RSA** certificate request

System Manager

1) Log onto System Manager
2) Navigate to Security->Certificates->Authority
3) Under System Functions click Public Web

4) On the EJBCA website click Create Server Certificate under Enroll
5) Enter the username and password created before (i.e. openfire & Password1!)
6) Paste in the **RSA** certificate request
7) Select PEM Certificate and click OK
8) Save the certificate to desktop

Openfire

1) Log onto Openfire
2) Navigate to Server Settings->Server Certificates
3) Click 'here' under the Signing Request
4) Open the certificate in WordPad
5) Copy the certificate into the Certificate Authority Reply and click Save
6) Delete the DSA Pending Verification certificate
7) Restart Openfire
8) Navigate to Server Settings->Server Certificates
9) Click here in the warning message "One or more certificates are missing. Click **here** to generate self-signed certificates" to re-generate the DSA self-signed certificate
10) Restart Openfire
11) The result will be a CA signed RSA certificate and a self-signed DSA certificate

On PS the following configuration is required on the CM instance for XMPP Federation:

XMPP Outgoing Server Director

Enable XMPP dialback authentication = No

SASL Authentication Credentials

Host where these credentials apply = of.ottps.avaya.com [Openfire XMPP Domain]
Enable SASL external authentication = Yes
External authentication ID = ps.mike.avaya.com
Username = pressrv73.aceott.avaya.com
Password = <empty>
Confirm Password = <empty>

SSL Settings

SSL mode = tls-required
Full path to SSL key file = /opt/Avaya/Presence/jabber/xcp/certs/Avaya-host-key.pem
Full path to SSL cert file = /opt/Avaya/Presence/jabber/xcp/certs/Avaya-host-key.pem
Full path to root CA cert file = /opt/Avaya/Presence/jabber/xcp/certs/generic.trusts
Require valid client side certificates = No [Yes is also valid]
Full path to Certificate Revocation List file = <empty>
Verify depth = 10 (default)
Enable weak ciphers = No (default)

XMPP Incoming Server Director

Enable XMPP dialback authentication = No

SASL Authentication Credentials

SASL realm = ps.mike.avaya.com [PS presence domain]
SASL hostname = of.ottps.avaya.com [OF hostname]
Enable SASL external authentication = Yes

External authentication ID = of.ottps.avaya.com

SSL Settings

SSL mode = tls-required
Full path to SSL key file = /opt/Avaya/Presence/jabber/xcp/certs/Avaya-host-key.pem
Full path to SSL cert file = /opt/Avaya/Presence/jabber/xcp/certs/Avaya-host-key.pem
Full path to root CA cert file = /opt/Avaya/Presence/jabber/xcp/certs/generic.trusts
Require valid client side certificates = Yes [**PS 6.2.5.0 <build60 set to NO, build 60 set to YES and build 61 can be either YES or NO**]
Full path to Certificate Revocation List file = <empty>
Verify depth = 10 (default)
Enable weak ciphers = No (default)

On Openfire the following configuration <u>must</u> exist:

xmpp.server.certificate.verify = false (As the PS domain is not added in the certificate Openfire cannot validate the PS certificate)
sasl.mechs = EXTERNAL (specifies external SASL authentication)
xmpp.server.dialback.enabled = false (needs to be set so TLSPolicy=required)
xmpp.server.certificate.accept-selfsigned = false (cannot use SASL External with self-signed certificates)

Technical Support

Support is available through the Avaya Global Technical Support Center.

If you encounter any problems, you can:

1. Retry the action. Carefully follow the instructions in the printed or online documentation.
2. Refer to the documentation that is shipped with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages that the system displays. See the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support by logging in to the Avaya Support website at http://support.avaya.com.

Before contacting Avaya Support, please keep the following information handy:

- Problem description
- Detailed steps to reproduce the problem, if any
- The release version in which the issue occurs
- The status of the Presence Services and System Manager software. If the software is an upgrade, then the release from which the software is upgraded.
- Log files
    - Collect the output from **`$PRES_HOME/presence/bin/getpslogs.sh`**
    - Collect the output from System Platform cdom **`getlogs`** if Presence Services is installed on System Platform.
    - Collect the logs from the presence-enabled client.

You might be asked to provide one or more files to Technical Support for analysis of your application and the environment.

For information about patches and product updates, see the Avaya Support website at http://support.avaya.com.