Avaya Aura® Session Manager Release 6.2 Service Pack 2 Release Notes

Release 6.2
Service Pack 2
July 2012
Issue 2.0

© 2012 Avaya Inc.
All Rights Reserved.

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 may be incorporated in future releases

For full support information, please see the complete documents, ***Avaya Support Notices for Software Documentation***, **document number 03-600758 and *Avaya Support Notices for Hardware Documentation*, document number 03-600759.**

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

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 of 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 following Web site:
http://www.avaya.com/support.

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.

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

Contents

Product Support Notices 4
Operational Assistance 7
General Topics 9
Communication Manager Interoperability 9
System Manager Interoperability 9
Session Manager Upgrades 9
SIP Phone Firmware 9
Technical Support 11

Avaya Aura® Session Manager 6.2 Service Pack 2 Release Notes

Product Support Notices

Some product changes are also documented as Product Support Notices (PSN). The PSN number defines the related document and appears in the Problem column in the tables.

To read the PSN description online:

1 Go to the Avaya support site at http://support.avaya.com.

2 Click on Downloads and Documents.

3 Enter **Avaya Aura Session Manager**, then under Release Version select **6.2.x**.

4 Select **Product Support Notices.**

5 Click on the PSN title link to open the PSN

Avaya Aura Session Manager 6.2 Service Pack 2 Enhancements

The table below gives details of some of the enhancements included in **Avaya Aura Session Manager 6.2 Service Pack 2** software release.

Table1:Enhancements to Avaya Aura® Session Manager Release 6.2 Service Pack 2

Keywords	Enhancement	ID Reference
Call admission control	Entity-based call counts shows total call completions within the time window, instead of current snapshot	wi00985526
Call admission control	Bandwidth counting error with certain Coverage Answer Group scenarios is fixed	wi01003645
Contacts	Storing an email address for contacts with email matching the SIP handle works correctly	wi00990261
Contacts	Adding (or updating) a contact with a first name only no longer returns the first name as the last name.	wi00994479
Contacts	Contact added by a system administrator now correctly appears on the endpoint	wi00995179
Emergency numbers	Dialplan is rebuilt immediately if emergency numbers are added, changed, or deleted.	wi00986794
Endpoint administration	Unnecessary NOTIFYs are not sent to Endpoints in different "Location Groups"	wi00984507
Endpoint administration	Expires parameter in first NOTIFY is the same as the Expires parameter in response to SUBSCRIBE	wi00994046
Endpoints	Endpoint Management Agent SIP NOTIFYs are delayed while an incremental or full CM sync is being done	wi01003690
Endpoints	SM sends a reply to an off-hook CANCEL from Toshiba phones	wi01013708
Endpoints	SM properly ensures CM dialplan is always sent down to registered endpoints.	wi01015982
Help	Help link that were not available for some Bulk import and export pages are now available	wi00978034
Jgroups	SM properly handles jgroups cluster merging and prevents thread leaks	wi00997977
login	If a customer login password begins with '=', the '=' is handled correctly	wi01008660
ME	Change to SMGR enrollment password is not ignored by certain scripts	wi01005521
Message waiting	SM propertly handles MWI updates for multiple CS1000s	wi00995804
Security module	Security module software restart timer defaulted to 5 minutes so that the software is restarted if it encounters an initial failure.	wi00997992
Security update	[RHSA-2012:0426-01] Moderate: openssl security and bug fix update	wi01004496
Security update	[RHSA-2012:0428-01] Important: gnutls security update	wi01004499

Security update	[RHSA-2012:0451-01] Important: rpm security update	wi01004502
Sip monitoring	SM will perform sip monitoring tests immediately if a route-through fails	wi00998039
SIP tracer	SIP Tracer Viewer in SMGR updated to be more robust	wi01007516
TLS	"RX error" counter on TLS connections now increments correctly when CM fragments SIP messages	wi00980956

Operational Assistance

This software also offers the following helpful tips and workarounds:

Table2: Avaya Aura® Session Manager Release 6.2 Service Pack 2 Assitance

Keywords	Issue	ID Reference	Workaround
Administration	Problem detected when selecting SM instances in the sip firewall management screen	wi00373427	Select entries in the tables by clicking on the checkbox beside each entry and not using the "All" button.
Administration	If a "domain" is attempted to be deleted in Routing Administration and this domain is associated with Session Manager user SIP handles (in the UPM application), a confusing error message is displayed in the GUI	wi00726949	Session Manager user SIP handles associated with the domain that will be deleted should be changed to a different domain prior to the deletion attempt.
Contacts	When a user is deleted from SMGR, the user will be removed from other users' contact lists. Once the user is "hard deleted", the deleted user will re-appear on external contact lists of users who had entered private information for the deleted user.	wi00730483	Administrator should use "hard delete" in a timely way to avoid the temporary disappearance of contacts.
Contacts	Phone cannot change primary number of the contact added	wi00927081	6.0 SIP Phone FW will not be able to successfully set the primary number for each of the phone's contacts.
Dial Patterns	Editing a dial pattern fails if the same pattern is deleted by another user concurrently	wi00942946	No workaround available. Please contact Support for assistance.
Local hostname resolution	On occasion, trusted SIP entities whose contact addresses are defined using LHNR, will not be trusted for up to 90 seconds after service is started. If these SIP entities are SM Failover Group peers, new calls may be affected for up to 90 seconds after the failed SM is restored to service.	wi01021029	These entities can be defined in external DNS in place of LHNR if an external DNS server is administered.
Locations	Adding a location name with an apostrophe in it causes unstable GUI behavior	wi00940889	Select a location name that does not contain an apostrophe.

Locations	Can't delete a location if it is assigned to a user as a home location - no user feedback	wi00940893	Users whose home location is set to the location that needs to be deleted should be assigned a different location prior to the deletion attempt.
NIC	Bonded NIC speed/duplex setting is not being applied to both physical interfaces	wi00957650	No workaround available. Please contact Support for assistance.
Online Help	There is no ‘Load default configuration’ option in the ‘More Actions’ list box item on Firewall configuration screen	wi00406988	'Load default configuration’ is not in the ‘More Actions’ button anymore. Instead it is in new button named “Load ASM Default configuration” for ASM and “Load BSM Default Configuration” for Survivable Remote
Routing	Editing dial pattern sometimes gives incorrect error message about no routing policy assigned to dial pattern.	wi00822060	This error might happen when editing multiple fields at once. To resolve, edit one field at a time.
Routing	(6.1) Attempting to start routing import while an import job is currently running fails without an informative error message	wi00927429	Ensure that the current import job has completed prior to starting additional imports.
Routing	Routing import reports failure but continues to import successfully	wi00970149	No workaround available. Please contact Support for assistance.
Routing	Ordering of data file affects import of SIP entity with outbound proxy	wi00979888	When importing a SIP entity configured with an outbound proxy, import the outbound proxy first since it is also a SIP entity.
Security	Calls are dropped after 32 seconds for SM-CM TCP connections that employ SIPS signaling.	wi00937163	If telephones in the enterprise are configured to use SIPS URIs, SM-CM link shall be set to TLS. SIPs requires end-to-end TLS connections.
Security	Security module's identity certificate is lost on BSM upgrade	wi00961940	Any third party identity certificates will need to be readministered.
Security module software	if the security module (secmod) is taken off line, link monitored SIP entities may become unreachable for about 30 seconds after it is started. If these SIP entities are SM Failover Group peers, new calls may be affected during this outage.	wi01024865	Stop/restart all SM services together instead of taking only the secmod down.
SIP Monitoring	SIP Entity with () in name causes SIP Monitoring Display to crash	Wi00995816	Don’t include “(“ or “)” in the SIP Entity name

General Topics

Communication Manager Interoperability

Avaya Aura Session Manager Release 6.2 supports Avaya Aura Communication Manager Release 5.1 and later. Please see the Avaya Aura Communication Manager 6.2 Release Notes for further details about software enhancements and issues.

System Manager Interoperability

Avaya Aura System Manager Release 6.2 Service Pack 2 and later supports Avaya Aura Session Manager Release 6.2 Service Pack 2. Please see the Avaya Aura System Manager 6.2 Release Notes for further details about software enhancements and issues. Session Manager 6.2 is not compatible with previous releases of System Manager, System Manager must be upgraded to 6.2 before upgrading Session Manager to 6.2.

Session Manager Upgrades

Upgrades from Session Manager 6.0 Service Pack 1 and any Session Manager 6.1 Service Pack to Session Manager 6.2 are supported. Session Manager 6.0 Service Pack 1 is the baseline for future upgrade paths. It is required that all servers be upgraded to SM6.0 SP1 before attempting to upgrade to future software loads. Session Manager 6.2 is not compatible with previous releases of System Manager, System Manager must be upgraded to 6.2 before upgrading Session Manager to 6.2.

Upgrade Compatibility and Sequence

When installing service pack updates to the Avaya Aura solution related to Session Manager, it is important that the different components are upgraded in the correct order to ensure platform stability and manageability of the network as part of the upgrade process. When applying service pack updates, upgrades should be done in the following order, ensuring each component's compatibility based upon the release notes for each product's service pack release notes.

1) System Platform that the System Manager template is running on
2) System Manager
3) Session Manager (one at a time ensuring active-active configuration of Session Manager minimizes service impact)
4) System Platform that the Communication Manager template is running on
5) Communication Manager

Emergency Number Dialing for Unregistered Endpoints

If multiple locations have been defined in System Manager, there must be at least one emergency call dial pattern entered with originating location = ALL. Alternatively, every location with a location specifc emergency number dial pattern must be defined with an associated IP address pattern. If these criteria are not met, unregistered endpoints will not be able to place emergency calls.

SIP Phone Firmware

Session Manager 6.2 supports SIP 96X0 phone firmware 2.6 or higher and SIP 96X1 phone firmware 6.0 or higher. Some features may require SIP 96x1 firmware 6.2 for proper operation.

Call Preservation configurations

In order to fully utilize the Call Preservation feature in SM6.2, the following products are supported in the solution:

Avaya Aura® Session Manager 6.2
Avaya Aura® Communication Manager 6.2 Service Pack 2 or greater
AudioCodes Mediant™ 3000 Gateway 2.0 or G860 Media Gateway 3.0
Avaya Aura® Experience Portal 6.0 Service Pack 1 (6.0.1.0.0809) with Intelligent Customer Routing

Technical Support

Support for Session Manager is available through Avaya Technical Support.

If you encounter trouble with Session Manager:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
    - Logging into the Avaya Support Web site http://www.avaya.com/support
    - Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

    You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

    Note: If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to http://www.avaya.com for further information.

When you request technical support, provide the following information:

- Configuration settings, including Session Manager configuration and browser settings.
- Usage scenario, including all steps required to reproduce the issue.
- Screen shots, if the issue occurs in the Administration Application, one-X Portal, or one-X Portal Extensions.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

    Tip: Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Support Web site.

For information about patches and product updates, see the Avaya Support Web site http://www.avaya.com/support.