



Release Notes for Avaya Aura[®] SIP Enablement Services (SES) Release 5.2.1 Service Pack 7

Release Notes Issue 1, 30 April, 2012

Contents

Bug Fixes and Improvements	2
Bug Fixes and Improvements in Release 5.2.1 Service Pack 7	2
Bug Fixes and Improvements in Release 5.2.1 Service Pack 6	2
Bug Fixes and Improvements in Release 5.2.1 Service Pack 5	2
Bug Fixes and Improvements in Release 5.2.1 Service Pack 4	2
Bug Fixes and Improvements in Release 5.2.1 Service Pack 3	3
Bug Fixes and Improvements in Release 5.2.1 Service Pack 2	3
Bug Fixes and Improvements in Release 5.2.1 Service Pack 1	3
Bug Fixes and Improvements in Release 5.2	4
Security Enhancements	4
Known Issues and Workarounds	5
Installation	5
Installing SES 5.2.1 Service Pack 7 on Duplicate Servers	5
Installing SES 5.2.1 Service Pack 7 on new HP DL360G7 servers	5
Upgrades	6
Simplex Edge or Simplex Combined Home/Edge – 4K users	6
Cabled Duplex Edge or Cabled Duplex Combined Home/Edge – 4K users	6
Simplex Home – 4K users	6
Cabled Duplex Home Pair – 4K users	6
Simplex Edge – 12K users	6
Cabled Duplex Edge Pair – 12K users	6
Restoring 4.0 or earlier data following a 5.2 Upgrade	7
Data Service administration	7
Best Practices	8
Releasing Disc Space	8
Install the IP Softphone Service Pack 9	8
Installation and Administration Guide (SIP Enablement Services 5.2)	8
Server Availability Management Processor (SAMP) firmware and operations	8
Root Certificates	8
Presence is case sensitive	8
Communication Manager Failover Service/Avaya Enterprise Survivable Server (ESS) configurations	8
SNMP administration on duplex systems	9
Trusted Hosts	9
ASCII Characters Only for WebLM License Path	9
Configuration considerations for Third-Party SIP phones	9

IMPORTANT: You must follow the activation/deactivation procedures described in this document. Failure to do so may cause problems.

NOTE: See [Installing 5.2.1 Service Pack 7 on Duplicate Servers](#) for important information.

NOTE: If you are using the new HP DL360G7 server:

- The HP DL360G7 server supports SES 5.2.1 SP4 and later only.
- See [Installing SES 5.2.1 Service Pack 7 on new HP DL360G7 servers](#) for important information.

Bug Fixes and Improvements

Bug Fixes and Improvements in Release 5.2.1 Service Pack 7

- A potential race condition in a network duplex setup resulting in a network outage no longer occurs.
- A security vulnerability involving command injection over the Web interface has been resolved.
- A potential deadlock condition involving the database no longer occurs.
- Failure of the “mon” application on some MBT systems has been resolved.

Bug Fixes and Improvements in Release 5.2.1 Service Pack 6

- Corrupt SIP messages no longer cause the SES SIP server to crash.
- The SIP Enablement Services Admin web interface “Edit Host” page has been fixed to allow for modifying the “Link Protocol” for SES Hosts. The “Link Protocol” is used for routing between SES Hosts (i.e. between an SES Edge and Home) and can be set to UDP, TCP or TLS.
 - *NOTE: make these changes during a scheduled maintenance period only to prevent a service outage.*
 - It is recommended that all SES Hosts in a distributed SES Edge with Homes configuration have the same “Link Protocol” type configured. This field does not apply to Home/Edge combo servers.
 - After making the configuration change, you may see a “Server Internal Error” message on the SIP Enablement Services “Admin” page. This indicates a web page timeout and may be ignored as the changes are being propagated to the database in the background. Once the change is complete, which can take up to 15 minutes, SSH into the SES Edge (where SES Master Admin resides) and observe that a line similar to the following has been added to /var/log/sip-server/ImpressLog.txt:

```
Jun 22 09:42:07 <SES Edge Hostname> [info] Host updated: <SES Host IP>
```

Where <SES Host IP> is the IP of the SES Host which was edited using the Admin web interface “Edit Host” page.
- Using the List Adjunct Servers page to edit or delete an Adjunct Server which has been assigned to multiple Adjunct Systems no longer causes a Database Error to be displayed.

Bug Fixes and Improvements in Release 5.2.1 Service Pack 5

- SIP Enablement Services 5.2.1 SP5 supports the Midsize Business Template (MBT).

Bug Fixes and Improvements in Release 5.2.1 Service Pack 4

SIP Enablement Services 5.2.1 SP4 has the following enhancements:

- If either of the servers in a duplex configuration is up for a long, uninterrupted time (over one year), the communication mechanism between the two servers (“Heartbeat”) no longer fails. This applies to all hardware types.
- Personal Profile Manager now delivers buttons to the SIP telephone after it establishes a connection to Communication Manager, even when it initially had trouble establishing the connection to CM, without requiring Administrator intervention.

Bug Fixes and Improvements in Release 5.2.1 Service Pack 3

SIP Enablement Services 5.2.1 SP3 has the following enhancements:

- The "setnic" command now works on the S8800, so the communication interface configuration is preserved after a reboot.
- On large SES deployments with tens of thousands of users, the SES data services component no longer runs out of memory and impacts replication of provisioning data.
- S8800 servers in cabled duplex installation now interchange when there is a power outage in the primary server.
- On large SES deployments with tens of thousands of users, the SES data services component no longer over-utilizes the CPU and PostgreSQL database.
- The "hardware_info" command output now shows the number of CPUs (central processing unit) present (instead of the number of cores) and provides information about each CPU.
- In SES deployments containing Avaya IP Softphone IM/presence users, a race condition no longer occurs if many users disconnect without logging off at the same time. This condition occurred when SES SipServer tried to connect to multiple SIP endpoints at the same time. This condition could have resulted in stuck network sockets and malfunctioning presence.

Bug Fixes and Improvements in Release 5.2.1 Service Pack 2

SIP Enablement Services 5.2.1 SP2 has the following enhancements:

- The Get Status option under **SIP Server Management > Users > Search Registered Users** now works correctly. Previously the message "attempt number 1 in progress for" always appeared whatever the actual status.
- Previously, users may have had difficulty accessing and using the SES administrative Web pages due to performance issues with large distributed SES deployments with multiple homes serving many thousands of users. Optimization of certain SQL operations that run on the SES Edge database has resolved that performance issue.
- A rare SipServer crash when more than 4000 endpoints register with TCP or TLS to SES no longer occurs.
- Previously, when an SES host was configured with a fully qualified domain name for an outbound proxy and the far end did not answer the call within 30 seconds, the call would drop. The attempt to establish the call now continues for up to 3 minutes.
- A condition where SES sometimes sent duplicated presence information which led to an IP Softphone application crash (IM/presence users only) no longer occurs. This condition occurred in environments where it was possible to have multiple concurrent SIP registrations for the same user. For example, if a user had multiple SIP clients registered using the same extension (such as a desk phone plus a soft phone), or if their IP Softphone did not un-register from their last session prior to logging in to a new session.

Bug Fixes and Improvements in Release 5.2.1 Service Pack 1

SIP Enablement Services 5.2.1 SP1 has the following enhancements:

- The Add Conference Page now functions correctly.
- Previously, when an SES host was configured with an IP address for an outbound proxy and the far end did not answer the call within 30 seconds, the call would drop. The attempt to establish the call now continues for up to 3 minutes.

- Updates to SES 5.2.1 Admin Webhelp.

Bug Fixes and Improvements in Release 5.2

SIP Enablement Services 5.2 has the following enhancements:

Security Enhancements

- Addresses security vulnerabilities documented in the following Avaya Security Advisories:
 - ASA-2009-114 kernel security and bug fix update (RHSA-2009-0331)
 - ASA-2009-057 ntp security update (RHSA-2009-0046)
 - ASA-2009-023 bind security update (RHSA-2009-0020)
 - ASA-2009-001 vim security update (RHSA-2008-0617)
 - ASA-2009-038 openssl security update (RHSA-2009-0004)
 - ASA-2009-002 libxml2 security update (RHSA-2008-0988)
 - ASA-2008-472 httpd security and bug fix update (RHSA-2008-0967)
 - ASA-2008-461 ed security update (RHSA-2008-0946)
 - ASA-2008-467 net-snmp security update (RHSA-2008-0971)

For more information on these Security Advisories, visit support.avaya.com.

Known Issues and Workarounds

Installation

Installing SES 5.2.1 Service Pack 7 on Duplicate Servers

NOTE: These instructions do not apply newly installed HP DL360G7 servers. See [Installing SES 5.2.1 Service Pack 7 on new HP DL360G7 servers](#).

These instructions do apply to duplicate HP DL360G7 running older service packs.

1. Establish CLI sessions to both the "A" and "B" servers
2. Run the "server" command to identify which server is primary and which is the backup.
3. Run the command "out-of-service" on the backup server.
4. If necessary, deactivate and remove the former SES patch. Activate the new patch on the backup server.
5. Run the command "in-service" on the backup server.
6. Run the command "interchange" on either one of the servers. Make sure the servers have switched roles by running the "server" command on both servers.
7. Repeat steps 3 to 5 on the server which is now in the backup role. This server was the primary server before you interchanged them in step 5.
8. Make sure the setup is stable by running the "server" command on both servers and making sure one server reports the role "Active (In service Primary)" and the other is "Active (In service Backup)".

Installing SES 5.2.1 Service Pack 7 on new HP DL360G7 servers

1. Establish a CLI session to the server.
2. Install the HP DL360G7 server with SES5.2.1 GA CD. Choose IBMX3550 as the HW type.
3. Run initial setup. Choose a simplex configuration and define the IP address.
4. Ensure that SES is out of service during the installation of SP5. When asked if to start the SES services during initial setup, choose "no".
5. Reboot the server.
6. When the server is up, make sure the servers are out of service, download SES SP5 and activate it.
7. For a simplex configuration - reboot the server.
8. For a duplex configuration - perform the following steps for both servers:
 - a. Run initial setup. Choose a duplex configuration.
 - b. Power down the servers.
 - c. Remove the AC cable for at least 20 seconds and then reconnect.
 - d. Power up the servers.
 - e. Wait for the 2 servers to synchronize their database (DRBD).
 - f. Place both servers in service.
 - g. If needed, perform a system restore operation on the primary server (only the "SES_files" option is supported).

NOTE:

1. *The common installer was not fixed to support the new HP DL360G7 server. Therefore, version upgrades via the web pages are blocked unless SP5 is deactivated. Installation from a CD is as described above.*
2. *Make sure that when in service, both servers in a duplex setup have the same Service Pack installed at all times.*

Upgrades

Upgrading from release 5.0 and later to release 5.2 requires less time than upgrading from previous versions. You must upgrade SIP Enablement Services servers in an enterprise starting with the Edge server. Home servers can be on either previous release but not previous than 5.0.

When upgrading from release 4.0 or earlier to release 5.2, a required update to the database and initial data replication must occur after the system reboot when the upgrade is complete. You can monitor the progress of these activities by using the **Status Summary Maintenance** web page or by a new command, “sds-monitor”.

IMPORTANT: These activities must be completed before proceeding to upgrade the next SIP Enablement Services server in the enterprise.

When upgrading a duplicated SIP Enablement Services server pairs, these activities also must occur, when the first upgraded server in the pair becomes the primary server of the pair. Wait for these activities to be completed on the primary server before upgrading the backup server of the duplex pair.

NOTE: These activities are performed only once when upgrading a duplex pair, so you do not have to monitor after the upgrade of the second server.

After you reboot the server successfully using the new release, use **Status Summary** or the “sds-monitor” command to monitor the progress and wait until initial replication is completed before proceeding to the next Home server. If the server is part of a duplex pair, the upgrade of the backup server in the duplex pair cannot be started until **Status Summary** or the “sds-monitor” command indicates that the initial replication is completed.

These activities are not required when upgrading from release 5.0 or later to release 5.2. However, *it is recommended that you check the status of the “sds-monitor” before proceeding to upgrade the next server (if applicable).*

After upgrading all Home servers in the enterprise, backup the data on the Edge 5.2 server.

Approximate server upgrade times for upgrading from release 4.0 or earlier to release 5.2 are as follows:

Simplex Edge or Simplex Combined Home/Edge – 4K users

1.5 hours

Cabled Duplex Edge or Cabled Duplex Combined Home/Edge – 4K users

2 hours

Simplex Home – 4K users

1.5 hours (Edge 5.0 upgrade must be completed first)

Cabled Duplex Home Pair – 4K users

2 hours (Edge 5.0 upgrade must be completed first)

Simplex Edge – 12K users

2.5 hours

Cabled Duplex Edge Pair – 12K users

3 hours

NOTE: These times are significantly improved for upgrading from release 5.0 or later to release 5.2.

Restoring 4.0 or earlier data following a 5.2 Upgrade

After upgrading all SIP Enablement Services servers from release 4.0 or earlier to release 5.2, you must restore the data backed up from the release 4.0 servers on all systems in the enterprise. Like the upgrade, the data restore of each system must be consecutive, starting with the Edge followed by each Home. You must monitor the completion of data service replication using the **Status Summary Maintenance** web page or the "sds-monitor" command before restoring the next SIP Enablement Services server in the enterprise.

Data Service administration

- *Applicable only to releases earlier than 5.0.*
Upgraded Avaya SIP Enablement Services 5.0 servers will automatically administer the new SES data services. Installers of new servers must use the Admin Setup function under Server Configuration on the SES Administration web pages to administer data services for the first time.
- **Use of Special Characters in File Names.**
You should not use special characters, such as apostrophe in the file names. Use of special characters when saving/restoring a file name can cause failure of the save/restore.

Important note for Upgrades and Migrations of Server Duplication from SIP Enablement Services releases earlier than 5.2:

If you are using the SIP Enablement Services in a cable redundant scheme please follow the next upgrade procedure. Failing to do so might result in an out of synchronization of the databases in the duplicated server.

1. Establish CLI sessions to both the "A" and "B" servers
2. Run the "server" command to identify which server is primary and which is the backup.
3. Run the command "out-of-service" on the server that is in the backup role.
4. Wait one minute and then run the command "out-of-service" on the server that is in the primary role.
5. Upgrade both servers in the redundant pair.

Please note that clicking on "Continue" following reboot of each server may result in a "session has expired" message. If this occurs, close all browser windows, start a new browser session with the server, go to the "Manage Software" maintenance page and select "Join the existing upgrade" to complete the upgrade.

6. After completing the upgrade, make sure that the "Make Upgrade Permanent" step is performed on both servers.
7. Run the command "in-service" on the "A" server in the redundant pair.
If the servers' SAMP cards are interconnected, this will cause the "B" server to reboot. Wait for it to finish rebooting.
8. Wait 5 minutes and then run "in-service" on the "B" server.

The wait is required because behind the scenes, there may be a full replication of the database partition from the "A" server to the "B" server in progress. The "B" server cannot be placed into service until that replication is completed.

NOTE: This procedure is only relevant when upgrading to SIP Enablement Services 5.2.x from previous releases. In the future once both duplicated servers are running 5.2.x the user may upgrade using the standard upgrade procedure.

Best Practices

Releasing Disc Space

Remove previous service packs from the disc using the “Manage Updates” page to release disc space.

Install the IP Softphone Service Pack 9

The PKI certificate in Avaya IP Softphone expired on July 23, 2011. As a result, the TLS connections used by SES and IP Softphone for sending SIP messages cannot be established. This affects both Instant Messaging and Presence information reported by and to the IP Softphone. Therefore, Avaya recommends that you upgrade to the IP Softphone Service Pack 9 when it is available. This Service Pack provides a new PKI certificate. Refer to Avaya's website: support.avaya.com for more information.

Installation and Administration Guide (SIP Enablement Services 5.2)

Before beginning any installation or upgrade, you must check for the latest documentation for Release 5.2 available in the Avaya's website: support.avaya.com.

Server Availability Management Processor (SAMP) firmware and operations

When performing a fresh new installation of SIP Enablement Services on the S8510, S8500B, or S8500C servers, the initial_setup script will install the proper version of the Server Availability Management Processor (SAMP) firmware. It is recommended for proper operation of the Avaya SIP Enablement Services server that you do not upgrade the SAMP firmware independently of the SIP Enablement Services software, even if a newer version is available. SIP Enablement Services software includes the SAMP firmware for its operations.

Root Certificates

Use the “tls-certmanage” command to manage trusted root certificates. You must place Root certificates first in */var/home/ftp/pub* (the default directory for the Download Files maintenance web page or anonymous ftp, if enabled) before running the command.

Usage of tlscertmanage is as follows:

tlscertmanage -l	Lists all CA certificates on the system
tlscertmanage -i file	Installs a CA
tlscertmanage -r #	Removes a CA (specify #)
tlscertmanage -help	Generates the USAGE screen

Presence is case sensitive

Presence will not be reported properly if the case of a handle in the one-X™ Desktop Edition SIP contact list does not exactly match the case of the administered user handle. Ensure that the user handles administered on the SIP Enablement Services Administration web-interface pages and the one-X™ Desktop SIP contact information are using the same case characters.

Communication Manager Failover Service/Avaya Enterprise Survivable Server (ESS) configurations

The default media server connection between Avaya SIP Enablement Services 5.x and Communication Manager is SSH (secure shell protocol). Communication Manager configurations with ESS use the C-LAN's IP address to connect on ESS failover. C-LANs support only telnet, which requires that Telnet is selected as the required SMS Connection Type when configuring the ESS media server in the SIP Enablement Services Administration web interface.

SNMP administration on duplex systems

You must administer the SNMP destinations at both the primary and the backup servers of a duplex system through the Maintenance web pages. You can make a connection to the backup server using the physical IP address of the backup server. To access the Maintenance web pages on the backup server, enter the physical IP address of the backup server in the web browser. For example, in `http://999.16.99.201/admin`, 999.16.99.201 is the physical IP address of the backup server.

Trusted Hosts

There are third-party proxies that do not support proxy authentication, and therefore you must configure them manually as Trusted Hosts. You can provision them through the SIP Enablement Services Administration web pages.

IMPORTANT: Before configuring any entity as a Trusted Host, ensure that the entity will properly validate SIP requests before forwarding them to Avaya SIP Enablement Services since the server will "trust" (for example, not challenge/authenticate) all requests received from the configured entity.

ASCII Characters Only for WebLM License Path

When installing a WebLM license using the Internet Explorer web browser on a PC with a non-U.S. version of Microsoft Windows - for example, Japanese Windows, the full path name to the license file should contain only ASCII characters and not international or special characters.

Configuration considerations for Third-Party SIP phones

Some third-party SIP telephones have the ability to perform features locally that are typically provided by Communication Manager. For example, when a call is made from a Cisco 7940/7960 SIP phone with the local Caller ID Block feature enabled, the called endpoint still displays your number. To work around this issue, you should use the Calling Number Block FNE in Avaya Communication Manager instead of the local feature in the phone. Another example of a feature that some SIP phones can perform locally is Call Forwarding, but this feature is generally provided by Communication Manager. In general, you should always use Communication Manager to provide these types of features to ensure the consistency of the user experience across all types of telephones and to prevent unexpected interactions with other Communication Manager features. It is highly recommended to disable the local phone version of these types of features, if possible.

Check component compatibility

Ensure that all your components are upgraded to the latest available. For maximum compatibility and interoperability between VoIP resources, such as the TN2602AP IP Media Resource 320 and Avaya SIP Enablement Services, you must upgrade the firmware to the latest vintage available for the Communication Manager release.

For more detailed compatibility information, visit the Downloads section in the Avaya Support website, support.avaya.com.