Product Support Notice

PSN #	PSN003661u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 30-Mar-12. This is Issue #06, published date: 08-Mar-2018.		Severity/risk level	High	Urgency	Immediately
Name of problem	Renewal of expired or about to expire certificates of Avaya Aura® System Manager				

Products affected

Avaya Aura® System Manager Release 6.x and 7.0.x.

Problem description

System Manager uses certificates for communication over SSL.These certificates are issued during installation and have a validity of two years.

This PSN is applicable to System Manager Installations which have expired certificates or certificates that would expire in the next 30 days and have not auto renewed. Note: only System Manager release(s) 6.2 and greater have the certificate auto renew feature. Refer Validation section from this document to check certificates validity.

This PSN was updated on 08-Mar-2018 to reflect the correct System Manager versions that this PSN is applicable for. See 5th bullet in the Remarks section. The "CertificateRenewalUtility_v2.bin" has not changed.

Resolution

- **CertificateRenewalUtility_v2.bin** will fix the above mentioned problems in Avaya Aura® System Manager 6.x and 7.0.x Releases.
- Please refer the below section **Patch Notes** for more details on resolution.

Note: Download the latest utility from Avaya support site and verify md5sum of CertificateRenewalUtility_v2.bin with the value from PLDS (**7e86d3ab7ea050d0807c89bd7408d198**). If you have downloaded the utility prior to this PSN being re-published then please make sure you download the latest utility from the support site**.**

Workaround or alternative remediation

- For 6.1 and higher releases certificates can be renewed from System Manager Web Console if the certificates are already not expired.

Remarks

- **This PSN is customer installable. If the customer requests Avaya to apply this PSN, it is a chargeable activity.**
- Customers using third party certificates on System Manager need to re-install their third party certificates once this PSN is applied.
- The newly generated certificate will be valid for 2 years from the day the utility is executed. One cannot change the validity period for the certificates.
- Please note that Session Manager **PSN003617** should be implemented to reinitialize trust management between Session Manager and System Manager once this PSN is applied.
- This Certificate renewal utility is only applicable for 7.0.x and older releases of System Manager only. **This certificate renewal utility cannot be run on System Manager 7.1.x or later releases.**

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Customers are required to backup their systems before applying the PSN if System Manager is accessible

Download

Follow the instructions below to download the patch:

1. The patch is available via Avaya's PLDS software download system, which can be reached by performing the following steps from a browser:
2. Log into the support site (http://support.avaya.com) using your login ID and password.
3. Click on Downloads button under "Support by Product". This will redirect to downloads page. In "Enter Product Name" textbox type "system manager" and then select "Avaya Aura® System Manager".
4. Chose the release from "Choose Release" dropdown list corresponding to your System Manager installation (i.e. 6.0.x or

6.1.x or 6.2.x or 6.3.x or 7.0.x).

5. Click on the appropriate download link as per your System Manager Installation version. E.g.: Click "System Manager Release 6.0 Certificates Renewal Utility" if you have System Manager Release 6.0 installed.
6. Click on the link to the file "CertificateRenewalUtility_v2.bin" to download the utility.
7. Use download id "SMGR5260611" to download the path from PLDS.

Patch install instructions

Follow the instructions below to install the patch:

1) Copy System Manager Certificate Renewal Utility (**CertificateRenewalUtility_v2.bin**) from your system to the /tmp/ directory on the System Manager box.
2) Get access to the System Manager Command Line Interface using with root user
3) Verify md5sum of CertificateRenewalUtility_v2.bin with the value from PLDS (**7e86d3ab7ea050d0807c89bd7408d198**).
4) Run the following commands to make it executable:
   i) #cd /tmp/
   ii) #chmod +x CertificateRenewalUtility_v2.bin

5) Use the below applicable section to renew the certificates.

System Manager Standalone Server or Geo Redundant Primary/Active Server:

i) If third party certificates are not installed on server, run following command to renew the certificates.
   #sh CertificateRenewalUtility_v2.bin
ii) If third party certificates are installed, run following command to remove already installed third party certificate and install System Manager CA issued certificates with two years validity.
   #sh CertificateRenewalUtility_v2.bin -FORCE

System Manager GEO Redundant Secondary/Standby Server:

i) Login to Primary System Manager Web console with admin user.
ii) Set the enrollment password if it is invalid or not already configured and note down the new enrollment password. You will need to provide a valid enrollment password when the certificate renewal utility is run on secondary System manager.
iii) If third party certificates are not installed on server, run following command to renew the certificates.
   #sh CertificateRenewalUtility_v2.bin
iv) If third party certificates are installed, run following command to remove already installed third party certificate and install System Manager CA issued certificates with two years validity.
   #sh CertificateRenewalUtility_v2.bin –FORCE

6) Wait for the utility to finish its execution.
7) Log on to System Manager Console, and verify whether the System Manager UI is displayed correctly.
8) Once certificates are renewed one, re-install third party certificates as applicable.

Service-interrupting?

Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 20+ minutes.

Verification

To verify the successful installation of the Patch:

- User should be able to login into System Manager successfully.
- All the certificates will now be valid for next two years.
- This can be verified by accessing System Manager Console

  For System Manager 6.0.x Release
  1. Log into System Manager Web console.
  2. Click Elements →Application Management →System Manager.
  3. Select System Manager and click on More Actions → Configure Identity Certificates.

4. Select Container TLS Service and View and verify the validity period.

For System Manager 6.1.x Release

1. Log into System Manager Web console.
2. Click Application Management →System Manager.
3. Select System Manager and click on More Actions → Configure Identity Certificates.
4. Select Container TLS Service and View and verify the validity period.

For System Manager 6.2.x Release

1. Log into System Manager Web console.
2. Click Element →Inventory.
3. Select Manage Elements
4. Select System Manager and click More Actions
5. Click on Configure Identity Certificates
6. Verify the validity period for all certificates

For System Manager 6.3.x and 7.0.x Geo Redundancy – Active Server

1. Log into Primary System Manager Web console.
2. Click Services →Inventory.
3. Select Manage Elements
4. Select System Manager and click More Actions
5. Click on Configure Identity Certificates
6. Verify the validity period for all certificates

For System Manager 6.3.x and 7.0.x Geo Redundancy - Secondary Server

1. Log into Primary System Manager Web console.
2. Click Services →Inventory.
3. Select Manage Elements
4. Select Secondary System Manager and click More Actions
5. Click on Configure Identity Certificates
6. Verify the validity period for all certificates

Enabling Geo-Redundancy

1. Log into Primary System Manager Web console.
2. Verify the Notification on dashboard is not showing as “Secondary Server status : Not Reachable”
3. In System Manager 6.3.8 and earlier releases, please set the Enrollment password and make sure admin password of Web console does not contain “& and %” characters.
4. Enable the GEO configuration only if Secondary is in standby mode (not active mode).
5. Once the GEO is enabled successfully.
6. Login to Secondary Server Web console and verify the GEO state.
7. If user unable to login to Secondary System Manager due to login page stuck with error message “Initialize data in progress”

   Or,

   If user is able to login to Secondary System Manager and an Empty Dashboard is appearing

   Then restart JBoss on Secondary System Manager server.

   - Log in to CLI of secondary System Manager as root user
     #service jboss restart

   Wait for 15 minutes for JBoss service on secondary server to come up and then perform step 7 once again
8. Login to Secondary Server Web console and check the Notification on dashboard: If it shows “Primary Server status: Not Reachable”

   Then restart System Monitor on both servers

   - Log in to CLI of System Manager as root user
     #service systemMonitor restart
9. Perform step 8 again after 5 minutes.
10. Check the geo status on secondary System Manager. It should be enabled.

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Patch rollback instructions

Once the certificates have been renewed you cannot get the old certificates back. If you had 3rd party certificates installed and they were overwritten using this utility then one cannot recover them. If you have any questions around this please contact Avaya support.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

N/A

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

N/A

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.