



Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN # PSN005295u

Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: Aug. 31, 2018. This is Issue #02, published date: Dec.10, 2018

Severity/risk level Medium Urgency Immediately

Name of problem AADS/AMM/AAWG installation fails when third-party certificates are used on Aura elements (System Manager, Session Manager) but not on AADS/AMM/AAWG.

Products affected

Avaya Aura® Device Services Release 7.1.x and earlier
Avaya Aura Multimedia Messaging 3.4.x and earlier
Avaya Aura Web Gateway 3.4.x and earlier

Problem description

When System Manager is used as the CA for generating certificates for AADS/AMM/AAWG, it will only send the trust chain for the System Manager CA to AADS/AMM/AAWG. If Aura elements including System Manager or Session Manager are using third-party (public or private) CA-signed certificates, AADS/AMM/AAWG will not receive the third-party trust chain from System Manager during AADS/AMM/AAWG installation.

Since the AADS/AMM/AAWG installation UI does not provide a way to add the third-party trust chain when System Manager is used to generate the AADS/AMM/AAWG identity certificate, the installation fails.

Resolution

n/a

Workaround or alternative remediation

Prerequisites:

Use this procedure under the following circumstances:

- Third-party CA-signed certificates are used for System Manager or Session Manager and other Aura elements.

Note: Must be using Internet Explorer

1. Manually create the AADS/AMM/AAWG identity certificate from the System Manager web UI.
 - I. Add an End Entity in the System Manager web UI.
 - a. Go to: Security->Certificates->Authority->Add End Entity
 1. Ensure the End Entity Profile is set to: INBOUND_OUTBOUND_TLS
 2. Fill in Username (make up any name)
 3. Fill in the Password (enrollment code) in the password field and confirm it
 - i. Note: This is not the same as the enrollment password. The password will be needed in a later step.
 4. Scroll down to CN, common name and enter the FQDN for the AADS/AMM/AAWG cluster
 5. Under Subject Alternative Name, add a "DNS" entry for the server's FQDN
 6. Pick Certificate Profile as "ID_CLIENT_SERVER"
 7. Ensure that CA is tmdefaultca
 8. Ensure Token is set to: P12 file
 9. Click Add.
 10. Ensure the profile is created.
 - i. Click Search End Entities.
 - ii. Enter the username in the Search end entity with username field to search for the end entity that was just created.
 - b. Note: Repeat step a) steps 1-10 for each AADS/AMM/AAWG node

II. Click **Public Web**.

- a. Click **Create Keystore**.
- b. Enter the username and enrollment code for the end entity created from step I-3
- c. Click **Certificate Chain** to download the trust chain in DER format (certdist.cer)
- d. Select a key length of 2048-bits
 - For the tmdefaultca, this must be 2048-bits
- e. Click **Enroll**.

A p12 keystore will be downloaded named <username>.p12, where the <username> is the username you chose when adding the end entity. The p12 keystore will be password protected using the same password entered for the end entity from step I-3

o Convert the trust chain to PEM format:

- From a Linux command prompt on the AADS/AMM/AAWG:
\$> openssl x509 -in ./certdist.cer -inform der -out smgrchain.pem

o Create a combined PEM trust chain as follows (cert-chain.pem). Concatenate the following PEM files into a single file:

- From a Linux command prompt on the AADS/AMM/AAWG:
\$> cat intermediate.pem root.pem smgrchain.pem > cert-chain.pem
 - intermediate.pem is the 3rdparty intermediate CA
 - root.pem is the 3rdparty root CA
 - smgrchain.pem is the trust chain for the SMGR CA

2. Launch the AADS/AMM/AAWG installer.
3. Click **Front-End Host**, System Manager and Certificate configuration
4. Specify 'N' when asked whether to use System Manager for certificates
5. Use the downloaded <username>.p12 file to fill in the REST, OAM and NODE interface certificate configuration for AADS/AMM and AAWG.
6. For AMM and AAWG, also use it for the SIP interface.
7. Click **Signing authority certificate configuration**.
 - a. Specify "N" when asked if the certificate is in PKCS12 format
 - b. Add the cert-chain.pem file as the Signing authority PEM certificate file

Fill in the rest of the details on this screen and then click the **Apply** button.

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Please follow the instructions in the installation manual.

Download

n/a

Patch install instructions

Service-interrupting?

n/a

No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

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

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).

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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.