



Product Support Notice

© 2025 Avaya LLC All Rights Reserved.

PSN # PSN006359u

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

Original publication date: 14-March-2025. This is Issue 01, published date: 14-March-2025.

Severity/risk level

Critical

Urgency

Immediately

Name of problem

Avaya Push Notification Provider server certificate update: Transition from Entrust CA to Sectigo CA.

Products affected

The following Avaya applications configured with the push notification provider address pnp.avaya.com are affected:

- Avaya Aura Session Manager 8.1.3 with patch 84125 and higher, 10.x
- Avaya Aura Web Gateway 3.9 and higher, 10.x
- Avaya IP office 11.x and higher (Note – A separate PSN will be published for IP Office to address the certificate installation instructions)

Avaya applications using pnp.avaya.com as the push notification provider address are NOT impacted, as the server pnp.avaya.com continues to use AvayaITserverCA2 as the Certification Authority. Therefore, the CA update is NOT required for these applications:

- Avaya Presence Service on Avaya Breeze
- Avaya Multimedia Messaging 3.x
- Avaya Aura Web Gateway 3.8.x and lower

Problem description

The Certification Authority (CA) for the Avaya Push Notification Provider pnp.avaya.com is changing. The existing server certificate for pnp.avaya.com, issued by Entrust CA, is set to expire on **April 1, 2025**. Due to transition of Entrust's Public Certificate business to Sectigo, Entrust will cease issuing public TLS certificates from the Entrust root CA. Consequently, Avaya has decided to switch to Sectigo as the new Certificate Authority (CA). The new server certificate issued by Sectigo CA for pnp.avaya.com will be updated on Push Notification Provider (PNP) server. To ensure a smooth transition and avoid push notification delivery failures, all customers using the push notification service on the Avaya Workplace client must update the above-mentioned Avaya application's Trust Store to include the new Sectigo CA certificates before **March 30, 2025 (8.30AM UTC)**.

Adding the new Sectigo CA certificates to the trust store of Avaya Aura Session Manager and Avaya Aura Web Gateway.

Step by Step procedure:

1. Avaya Aura Session Manager

To allow Session Managers to trust the Avaya Push Notification provider server and provide Apple Push Notification service for iOS and Android endpoints, the below process can be followed:

1. Log into the System Manager web interface.
2. Navigate to the **Services > Inventory > Manage Elements** screen.
3. For each Session Manager that will be sending push notifications to the APN provider, the following steps must be followed:
 - a. Select the checkbox by Session Manager server to modify, click on the "More Actions" pull down menu, and select "Manage Trusted Certificates".
 - b. Click on the "Add" button at the top of the table of trusted certificates.
 - c. In the Add Trusted Certificate window, select "WebSphere" from the Store Type, click on "Import as PEM certificate", and copy/paste the text below into the text window for the PEM certificate as shown below:

© 2025 Avaya LLC All Rights Reserved.

```

oBEKIz6W8Qfs4q8p74Klf9AwplQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQF
MAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2Nybc5jb21vZG9jYS5jb20v
QUFBQ2VydGlmaWNhdGVtZXJ2aWNlcy5jcmwwNqA0oDKGMGh0dHA6Ly9jcmwuY29t
b2RvLm5ldC9BQUFDZXJ0aWZpY2F0ZVNlcnZpY2VzLmNybdANBgkqhkiG9w0BAQUF
AAOCAQEACFb8AvCb6P+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1Q
GE8mTgHj5rCl7r+8dFRBv/38ErjHT1r0iWAFf2C3BURz9vHCv8S5dla2LX1rzNLz
Rt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BsWO/8tqtlbgT2
G9w84FoVxp7Z8VIIMCFIA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsi
l2D4kf501KKaU73yqWjgom7C12yxow+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3
smPi9WlsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----

```

d. After the form is filled out as shown above, click on the Commit button to save the Sectigo certificate chain to the SM trust store. The resulting certificate should look something like this on the SM trusted certificate page:

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains navigation links: Home, Inventory, Manage Elements, Create Profiles and Disc..., Element Type Access, Subnet Configuration, Manage Serviceability..., Synchronization, and Connection Pooling. The main content area is titled 'Manage Trusted Certificates' and includes a 'Done' button. Below the title is a table with 9 items. The table has columns for 'Store Description', 'Store Type', and 'Subject Name'. One item is highlighted with a red box: 'WEBSphere' with 'Subject Name' 'CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB'.

Store Description	Store Type	Subject Name
☐ Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	POSTGRES	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	WEBSphere	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
☐ Used for validating TLS client identity certificates	WEBSphere	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	WEBSphere	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB
☐ Used for validating TLS server identity certificates	SYSLOG	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=System Manager CA
☐ Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=System Manager CA

- e. Click the Done button on this page to return to the list of managed elements.
- f. Repeat the steps above for the rest of the Session Manager instances that will be sending push notifications.

4. Refer to the Administering Avaya Aura Session Manager guide for details on how to configure Apple Push Notification for Session Manager and how to run maintenance tests to confirm connectivity between the Session Manager and the APN provider is functioning properly. (Test is run by clicking the “Verify Settings” button on the Elements > Session Manager > Network Configuration > Push Notification > Notification Application screen.)

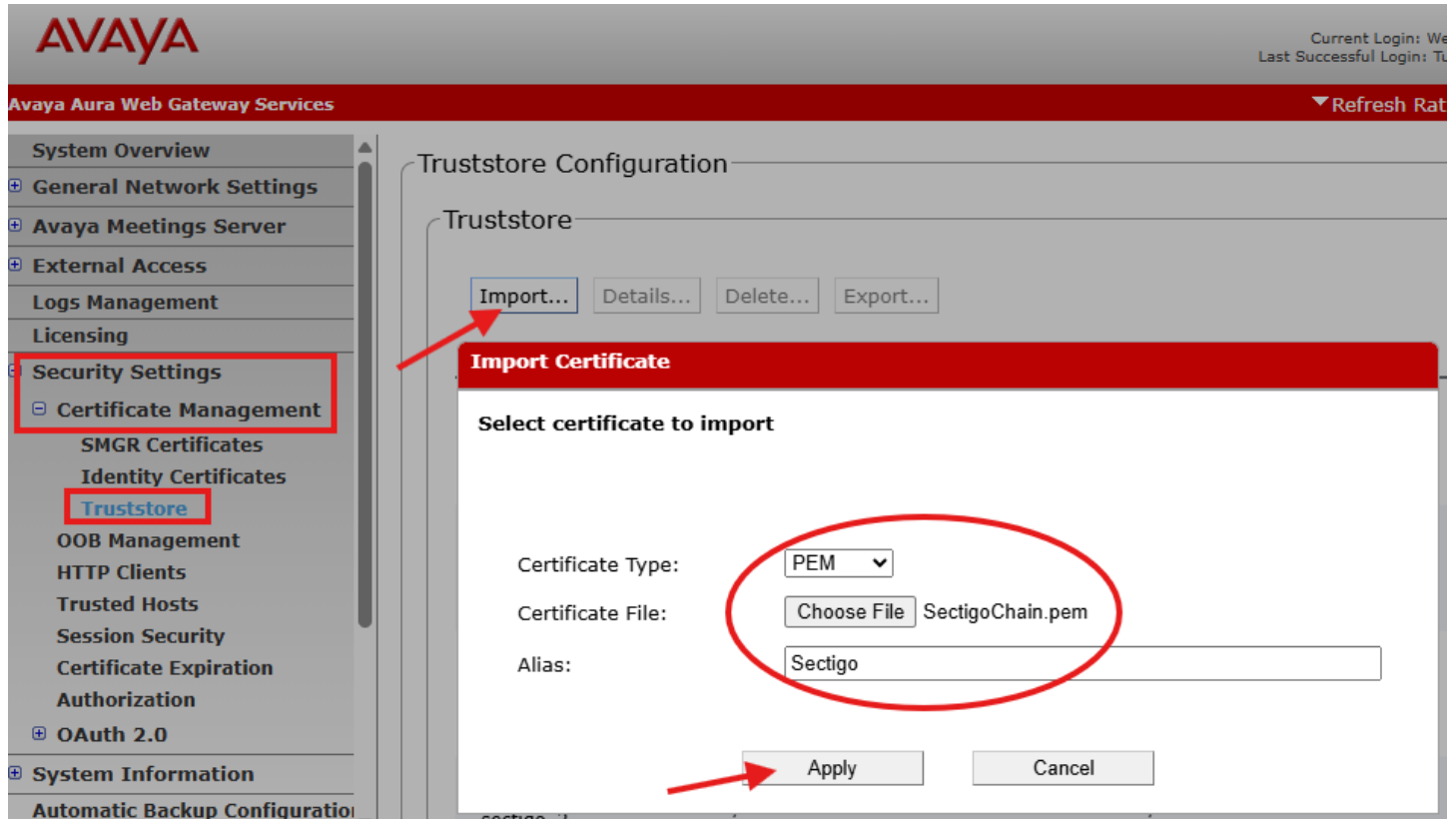
Note: Restart of Session Manager is not required, so this is not service impacting.

2. Avaya Aura Web Gateway

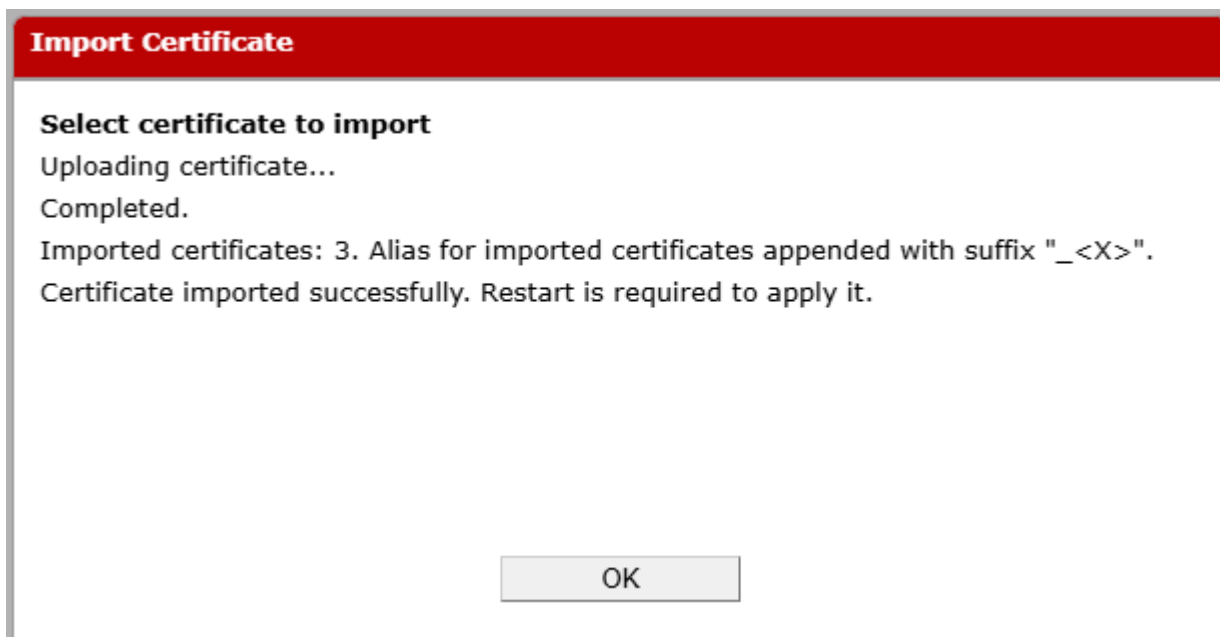
Note - Restart of AAWG is required, this is service impacting and needs to be done during scheduled down time.

To allow Avaya Aura Web Gateway to trust the Avaya Push Notification provider server and provide Apple Push Notification service for iOS and Android endpoints, the below process can be followed.

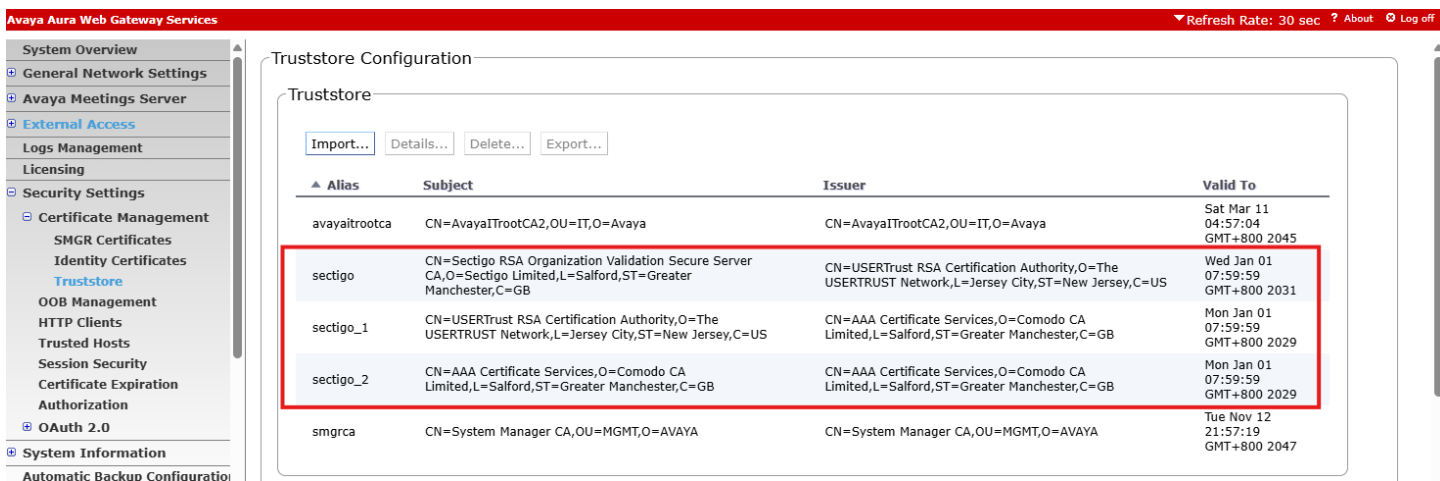
1. Copy/paste the above text (under the Session manager section) including the BEGIN and END Certificate lines in the notepad, save the file with pem extension, e.g. SectigoChain.pem.
2. Log into Avaya Aura Web Gateway Web GUI with URL https://<AAWG_IP>:8445/admin.
3. Navigate to **Security Settings > Certificate Management > Trust Store**, click import, Choose Certificate Type as PEM, select the Certificate File SectigoChain.pem, name an Alias there. Click Apply.



3. Click OK to restart the service.



4. Verify the Sectigo CA certificates in the trust store after service restart.



5. Navigate to **Advanced > Push Notification Settings > Provider Settings > Click “Test” button**, make sure the connection test is successful.

System Overview
General Network Settings
Avaya Meetings Server
External Access
Logs Management
Licensing
Security Settings
System Information
Automatic Backup Configuration
Spaces Configuration
Advanced
CORS Configuration
Application Management
Media Settings
Push Notification Settings
Provider Settings
Mobile Application Settings

Push Notification Provider Settings

Push Notification Provider: APN Production

Add

Edit

Remove

Enter Company Domain:

XXXXXXXXXX

Generate Key

Push Notification Provider Name: APN Production

Push Notification Provider Address: pnp.avaya.com

Push Notification Provider Port: 443

System Id: c1eac845-ba14-48bd-b412-...

Public Key:-----BEGIN PUBLIC KEY-----MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE6V/co4BwgZqvpfI7rFN8c6RdAloUWEt1/tmNQ+ij+zOR+5q8nlicbaP4r+ILTSsr0Ftuaneo0Nqkmgq2AkN4A==-----END PUBLIC KEY-----

Test

Export...

Save

Cancel

Provider Connectivity Test

Connectivity test succeeded.

OK

NOTE: At some point if this CA certificate is replaced or needs to be updated, an update to this PSN will be published.

Workaround or alternative remediation

n/a

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

N/A

Download

N/A

Patch install instructions	Service-interrupting?Y
----------------------------	------------------------

N/A

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
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 LLC, 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 LLC.
All other trademarks are the property of their respective owners.