Product Support Notice

PSN #	PSN020586u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 24-Jan-23. This is Issue #05, published date: 27-Feb-23.

Severity/risk level	High	Urgency	Immediately

Name of problem PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023

Products affected

Avaya Aura® AVP Utilities - 8.x
Avaya Aura® Application Enablement Services - 8.1.2, 10.1
Avaya Aura® Communication Manager - 8.1, 10.1
Avaya Aura® Media Server 10.1, 8.0.2
Avaya Aura® Session Manager 8.1, 10.1
Avaya Aura® System Manager 8.1, 10.1
Avaya Aura® WebLM 8.1
Avaya Breeze® 3.8.1.1

Problem description

This PSN will be updated as new information is available.
Make sure you are signed up for E-Notifications, *available on support.avaya.com* under *Alerts & Reports → Set E-Notifications*

February 27, 2023 Update: Added Avaya Breeze®, finalized Aura 8.1 OVA posting date.

February 10, 2023 Update: Added Avaya Aura® Media Server.

February 1, 2023 Update: *To facilitate deployment of 10.1 OVAs prior to the launch of Aura® 10.1.2, Avaya is reactivating the original 10.1 OVAs for Session Manager, System Manager and Communication Manager. This will allow deployment of the original 10.1 OVAs using the current 10.1.x.x SMGR SDM or SDM Client.*
*New PLDS IDs have been created for the short period until Aura 10.1.2 is GA. These will be deprecated upon launch of Aura® 10.1.2. See the **Workaround or alternative remediation** section of this PSN for details.*

January 27, 2023 Update: *To deploy the newly re-signed 10.1 OVAs using SDM Client or SMGR SDM, you must use SDM Client 10.1.2 and SMGR 10.1.2 or later. Target GA for Aura 10.1.2 is mid-February, 2023. Other deployment methods with the newly re-signed 10.1 OVAs will work.*

On February 20th, 2023, the Avaya signing certificate used for signing the Avaya Aura® OVAs listed in the "Products affected" section of this PSN will expire. This may result in a warning indicating the certificate is expired when the original Avaya Aura® 8.1 and 10.1 OVAs are deployed through Avaya Aura® System Manager Solution Deployment Manager (SDM), the SDM Client, vCenter, or the embedded VMware Host Client.

The warning message simply indicates that the certificate used by Avaya to sign and validate the OVA has now expired, but this does not impact the functionality of the deployed application in any way.
This warning will only be visible when deploying an OVA.

This is not service impacting. The original OVAs will still deploy and work correctly and remain fully supported by Avaya. If a virtual machine has already been deployed using the original OVAs, no action is required as there is no functional impact.

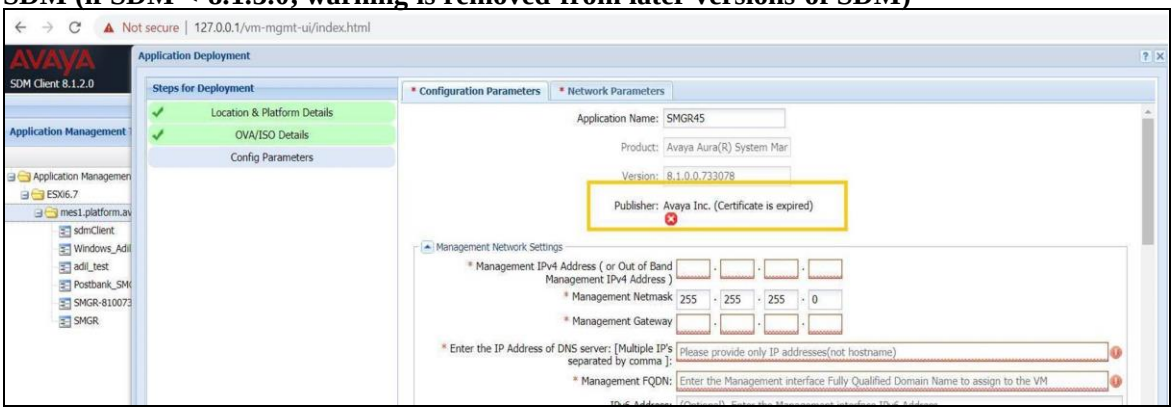
As noted in the **Resolution** section of this PSN, Avaya is in the process of re-signing the OVAs with a new certificate that will resolve this issue. This is an iterative process. Aura® 10.1 OVAs will be re-signed and reissued on January 24, 2023, followed by the Aura® 8.1 OVAs. Reference the table in the **Resolution** section of this PSN for Aura® 8.1 target dates.

Note: Application AWS, KVM and ISO images all have a different validation process and are not impacted by this issue.

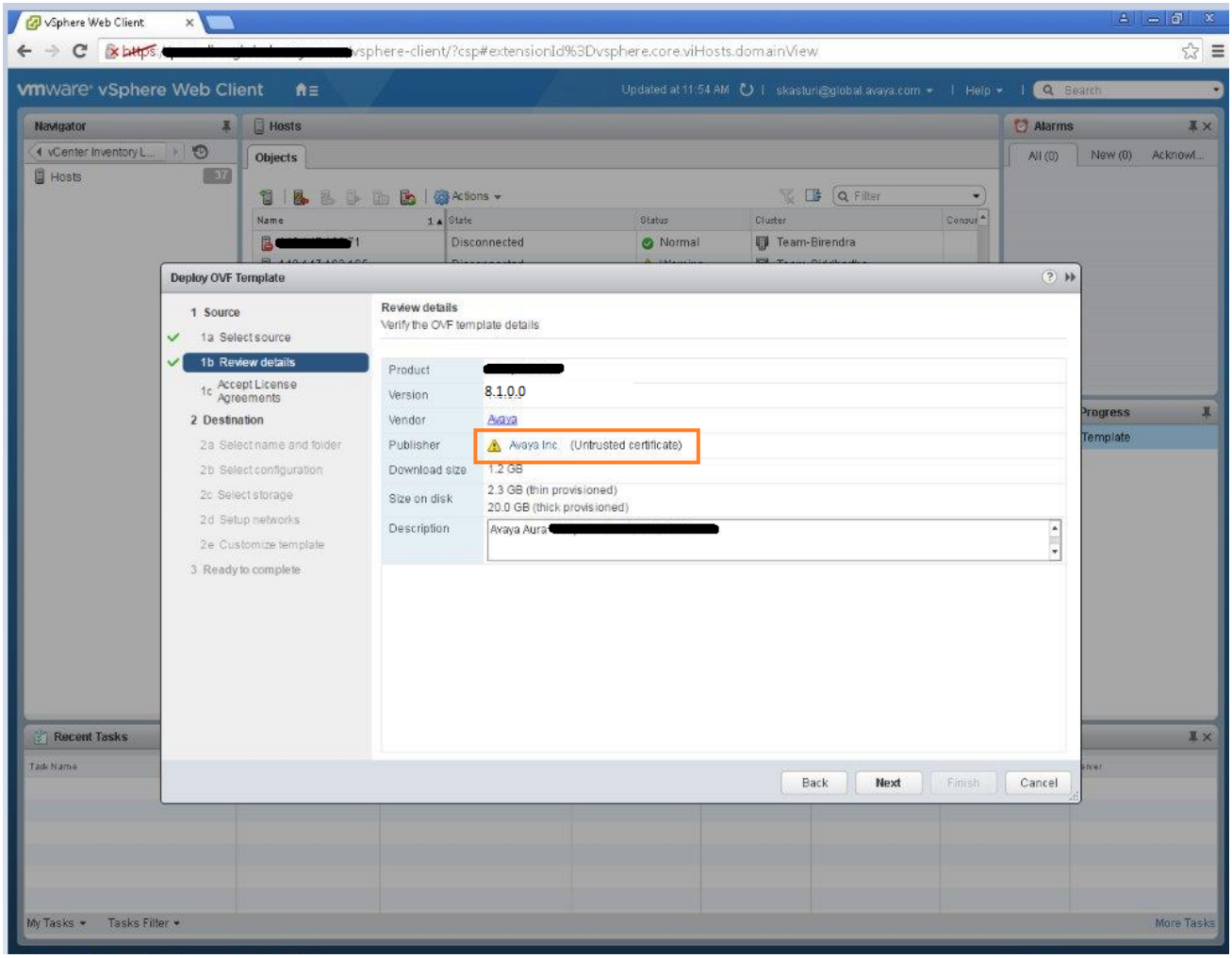
IMPORTANT NOTE – it is critical to read and follow the Special Instructions referenced below.
VMware introduced additional verification of OVF signing certificates in vCenter 7.0 U2. Therefore, there are additional steps required prior to deploying the re-signed OVAs in a vCenter enviornment. These steps are documented in the **Resolution** section of this PSN under "**Special instructions when utilizing vCenter 7.0 U2 or later**".

The following are ***examples*** of what might be seen when deploying the original Avaya Aura® OVAs after the February 20, 2023 signing certificate expiration date.

SDM (if SDM < 8.1.3.0; warning is removed from later versions of SDM)

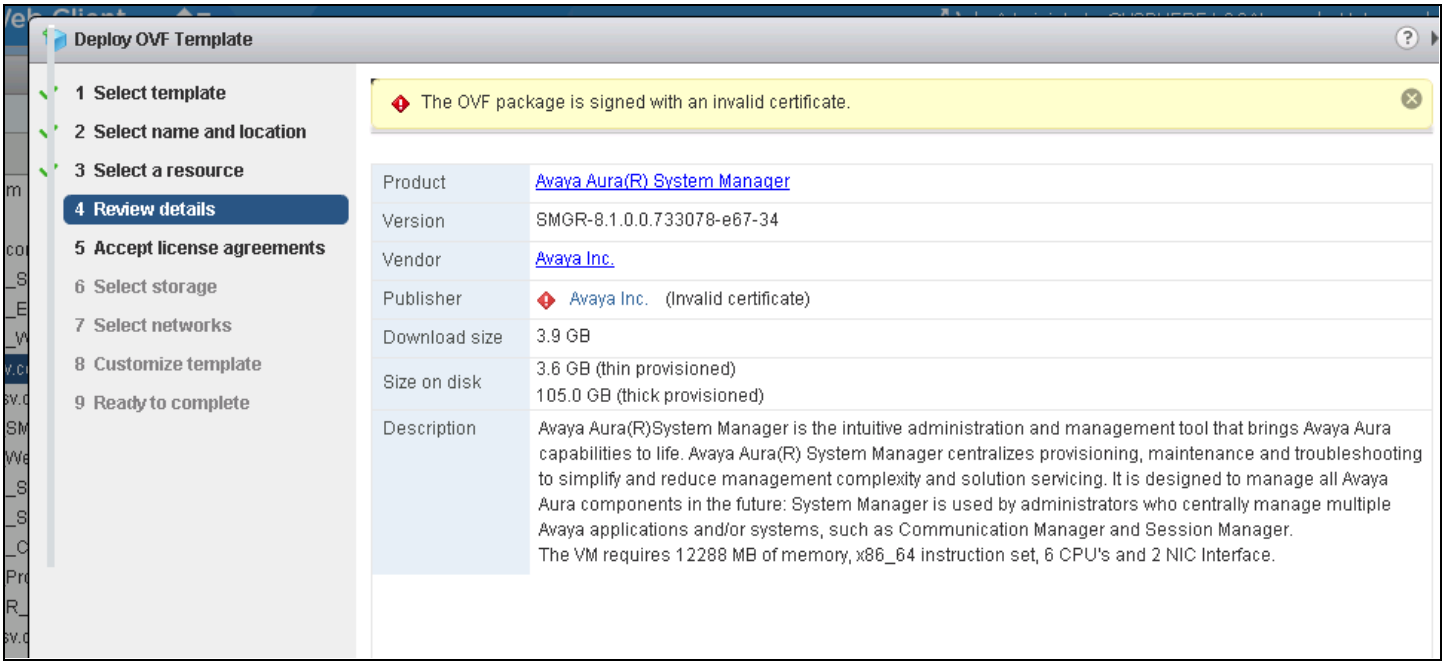


VMware Host Client



vCenter (except for 6.5)

vCenter 6.5 OVA DEPLOYMENT IS BLOCKED – ***use SDM or SDM Client to deploy OVA***
(only applicable for Aura® 8.1 since vCenter/ESXi 6.5 is not supported for Aura® 10.1)



Resolution

Avaya is in the process of re-signing the Aura® 8.1 and 10.1 OVAs with a new certificate that will address the February 20, 2023 certificate expiry issue. These shall be posted to PLDS once System Verification is completed. This PSN and the corresponding application PCNs will be updated at that time.
This will be an iterative process, starting with 10.1 OVAs first,
The dates will be tracked in the table below.
Note: *To deploy the newly re-signed 10.1 OVAs using SDM Client or SMGR SDM, requires SDM Client 10.1.2 and SMGR 10.1.2 or later.*

Always reference the required order of upgrade for Avaya components.

Updated Aura OVA	Application	PCN Reference	Posted on PLDS
10.1 PLDS Ids will remain the same for all but AAMS. OVAs will use SHA256 checksum in the manifest file. No changes to software or functionality except AES 10.1 AES 10.1 OVA will now support Fault Tolerance. The certificate and the signature file will be renewed. OVA file name will change to reflect a new version number.	Application Enablement Services Communication Manager Session Manager System Manager AAMS	PCN2139S PCN2133S PCN2135S PCN2137S PCN2148S	Jan 24, 2023 Jan 24, 2023 Jan 24, 2023 Jan 24, 2023 Feb 13, 2023
8.1 * PLDS Ids will remain the same for all but AAMS 8.0.2. No changes to software or functionality Certificate and the signature file will be renewed. OVA file name will change to reflect a new version number.	Avaya Aura AVP Utility Services (AVPU) Application Enablement Services 8.1.2 Communication Manager 8.1, 8.1E Session Manager 8.1, 8.1E System Manager 8.1, 8.1E Standalone WebLM 8.1 ** AAMS 8.0.2	PCN2098S *** PCN2102S PCN2095S PCN2099S PCN2100S PCN2101S PCN2092S	Feb 21, 2023, for ALL

** There is one day where the original cert will have expired prior to the re-signed OVA being available. Recommendation would be to plan any new 8.1.x deployments for Feb 21, 2023 or later. In the event of a critical outage that requires a server rebuild/remaster, the original 8.1 OVAs can be deployed by accepting the warning and moving forward with deployment.*
*** Standalone WebLM 8.1 does not currently offer an OVA that supports data encryption.*
**** Aura® 8.1 PCNs will be updated when the re-signed OVAs are posted on PLDS.*

Updated Avaya Breeze® OVA	OVA	PCN Reference	Posted on PLDS
3.8.1.1	Avaya Breeze® 3.8.1.1 OVA Avaya Breeze® 3.8.1.1 AWS ONLY OVA	PCN2125S	Feb 27, 2023

Special instructions when utilizing vCenter 7.0 U2 or later

As noted in https://kb.vmware.com/s/article/84240, *prior to vCenter 7.0 U2, there was minimal certificate verification done on OVA/OVF packages.*
Starting 7.0 U2, the OVF signing certificates are verified for their expiry, validity and checked if the signing certificate is trusted. This means that the entire chain of the signing certificate should be trusted against the VECS store.

When utilizing vCenter 7.0 U2 or later, the following instructions are necessary to add the signing certificate to the VMware Endpoint Certificate Store (VECS) prior to deploying the re-signed Avaya Aura® OVA. If this is not done, then you will see an error similar to the following when deploying the OVA.

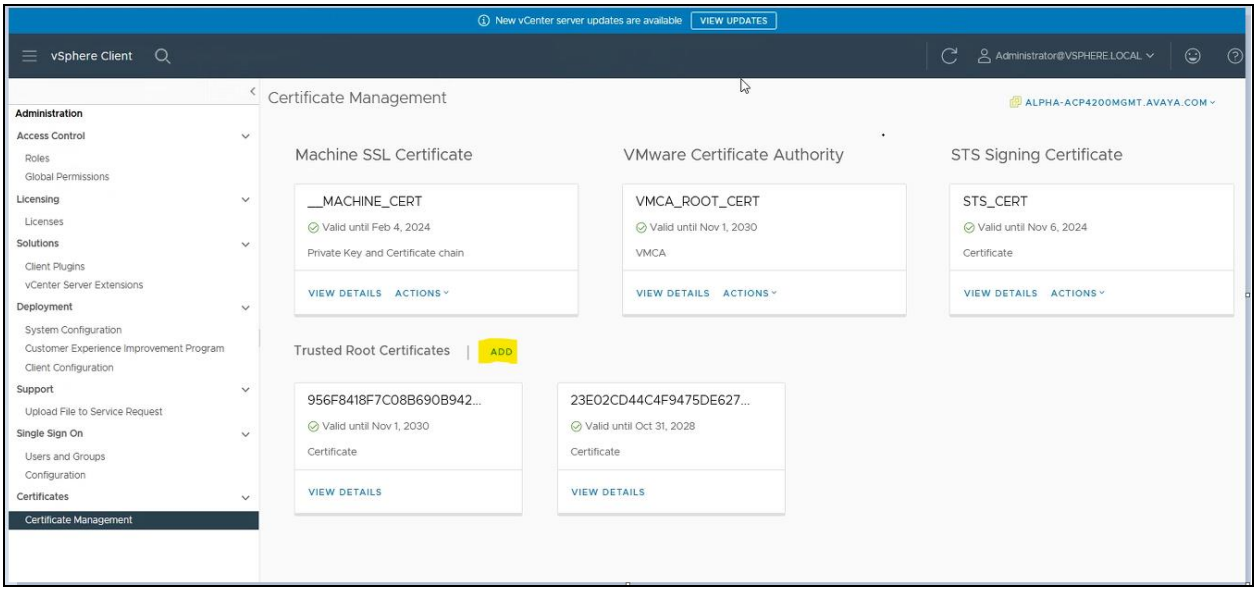
```
Error: "The Certificate is not trusted".
```

Note: If deploying multiple Aura® OVAs (same application or different applications) on the same vCenter, these steps only need be performed once.

1) The signing certificate's chain (root CA and intermediate certificates) must be added to VECS. Avaya has created a file that contains the Root and 2 intermediate certs (total three certs) "**AvayaAura-2023-OVA-ReSpin-CertChain.pem**".
2) This file is available for download from **PLDS ID: AURAOVARESPIN01**
3) Once the **AvayaAura-2023-OVA-ReSpin-CertChain.pem** file is downloaded, verify the checksum. This can be performed on Windows with the following utility from the "cmd" window.

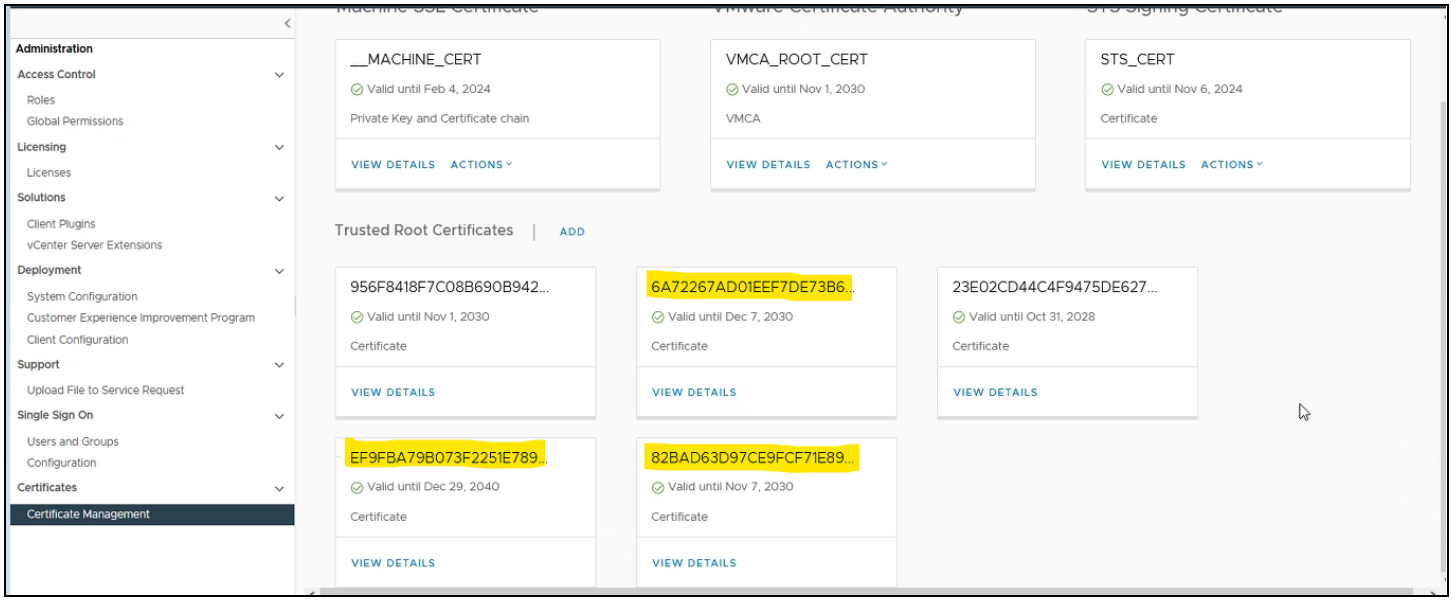
```
certUtil -hashfile [full path to file\AvayaAura-2023-OVA-ReSpin-CertChain.pem] MD5
MD5 hash of AvayaAura-2023-OVA-ReSpin-CertChain.pem:
46fc76d8b99b855ab79c293e4266af10
CertUtil: -hashfile command completed successfully.
```

4) After verifying the checksum, login to vCenter with Administrator privileges. From the drop down menu, select **Administration→Certificates→Certificate Management.**
5) In the **Certificate Management** page, select **ADD** certs to **Trusted Root Certificates**
   Note that there may already be existing Trusted Root Certificates in the store as shown in the example below.
   For ease of verification, capture any existing Trusted Root Certificates already present before adding the new certificates to the store. Once the certificate has been added, it cannot be removed via the UI.



6) Select the **AvayaAura-2023-OVA-ReSpin-CertChain.pem** file downloaded in Step 2 above and then select **ADD**.

7) Verify that the root and intermediate certs are now shown in **Trusted Root Certificates**.
   a. Click on **VIEW DETAILS** for each of the certificates below.



b. Below are the details of the certificates, in text format, present in the pem file that can be used for verification. The user will want to verify the keytool output certificate attributes with the "**VIEW DETAILS**" in vCenter. Compare the following attributes.

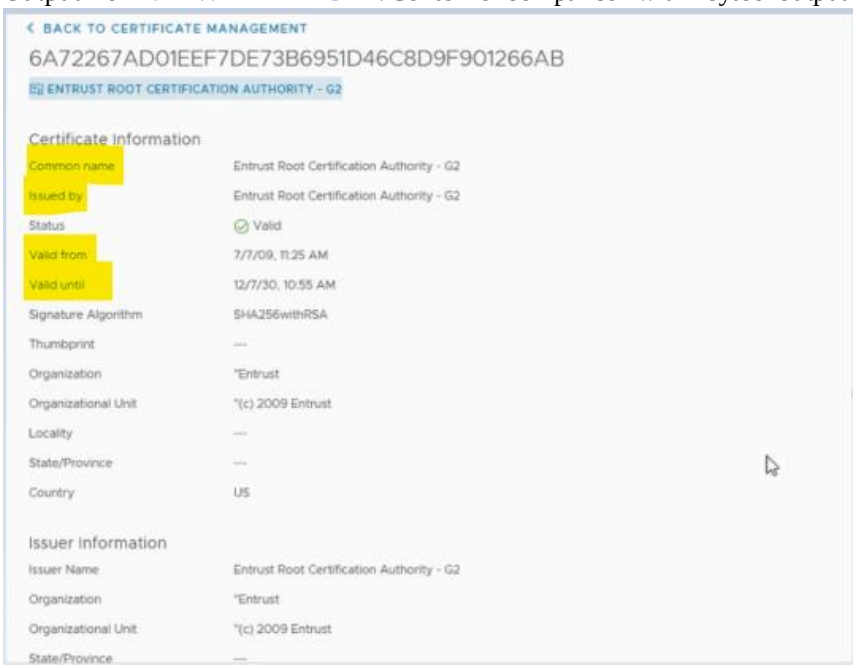
vCenter VIEW DETAILS	Keytool output
Common Name	Owner
Issued by	Issuer
Valid From /Valid Until	Valid from…..until

The Valid From/Until dates these will be dependent on the timezone of the vCenter. But will be within 24 hours of these dates.
Certificate 3 below has both the keytool output and **VIEW DETAILS** output as an example.

```
$>keytool -printcert -file  AvayaAura-2023-OVA-ReSpin-CertChain.pem
Certificate[1]:
Owner: CN=Entrust Code Signing CA - OVCS2, O="Entrust, Inc.", C=US
Issuer: CN=Entrust Code Signing Root Certification Authority - CSBR1, O="Entrust, Inc.", C=US
Serial number: 71ef5574af3554c35a2c69f66f4b6bcd
Valid from: Fri May 07 19:20:45 GMT 2021 until: Sat Dec 29 23:59:00 GMT 2040
Certificate fingerprints:
         SHA1: A6:1D:C5:D9:0A:06:00:3E:B4:DD:35:99:B7:A0:52:FC:3F:70:D7:CC
         SHA256:
95:F8:43:04:6B:AC:03:55:72:A3:BA:1B:82:1D:F8:B7:59:46:7F:5B:51:2D:DF:A8:A7:2F:07:99:44:7D:63:68
Signature algorithm name: SHA512WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3



Certificate[2]:
Owner: CN=Entrust Code Signing Root Certification Authority - CSBR1, O="Entrust, Inc.", C=US
Issuer: 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
Serial number: 4e40e43754ede68c0000000051d3947f
Valid from: Fri May 07 15:43:45 GMT 2021 until: Thu Nov 07 16:13:45 GMT 2030
Certificate fingerprints:
         SHA1: B3:37:B8:FD:B5:6E:CB:58:BF:5D:BC:F8:C2:2C:32:01:07:53:5A:02
         SHA256:
18:DD:9A:46:70:54:C7:4A:5A:E4:61:82:84:3A:6F:4E:C4:6D:5E:33:8D:91:AD:F4:E5:98:0B:50:19:3F:B9:4B
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3



Certificate[3]:
Owner: 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
Issuer: 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
Serial number: 4a538c28
Valid from: Tue Jul 07 17:25:54 GMT 2009 until: Sat Dec 07 17:55:54 GMT 2030
Certificate fingerprints:
```

```
        SHA1: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4
        SHA256:
43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:39
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

Output from **VIEW DETAILS** in vCenter for comparison with keytool output for certificate 3 above.



8) Once verification is complete, deploy Avaya Aura® OVAs.

Workaround or alternative remediation

Original Aura® 10.1 OVAs reactivated on PLDS to facilate deployment of 10.1 prior to Aura® 10.1.2 availablity.
The new 10.1 OVAs can currently only be deployed via vCenter or the ESXi embedded host client. Deployment via SMGR SDM or SDM Client is necessary if root access needs to be enabled. SDM 10.1.2 is required to deploy the new 10.1 OVAs. Since that will not be available until Aura® 10.1.2 launches mid-February, for customers who require root access, Avaya is reactivating the original 10.1 OVAs with new PLDS IDs.
These PLDS IDs for the original 10.1 OVAs will be deprecated when Aura® 10.1.2 launches mid-February.
Note: The new 10.1 OVAs were provided to address the expiration (February 20, 2023) of the Avaya signing certificate used for Avaya Aura OVAs. The updated OVAs also provide support for SHA256. Existing 10.1 deployments require no action. Only new installations beginning February 20, 2023 will require the updated OVA due to the certificate expiration.

Original 10.1 OVA	File	PLDS ID	MD5 Checksum
Original Avaya Aura System Manager 10.1 Profile 2 OVA	SMGR-10.1.0.0.537353-e70-21E.ova	SMGR101OLDOVA1	6deee1669c71814249826cf45f1f8391
Original Avaya Aura System Manager 10.1 Profile 3 OVA	SMGR-PROFILE3-10.1.0.0.537353-e70-21E.ova	SMGR101OLDOVA2	b4f330b92d9278292172aeb67bf0565f
Original Avaya Aura System Manager 10.1 Profile 4 OVA	SMGR-PROFILE4-10.1.0.0.537353-e70-21E.ova	SMGR101OLDOVA3	ae5986a5509c475066bb307ddf9c03ab
Original Avaya Aura Session Manager 10.1 OVA	SM-10.1.0.0.1010009-e70-01.ova	SM000000255	c305ec472cd81c872b212ee7fdb2d0c5
Original Avaya Aura Branch Session Manager 10.1 OVA	BSM-10.1.0.0.1010009-e70-01.ova	SM000000254	3da94a8a5752ffb95371a3371c63b2aa
Original Avaya Aura Communication Manager 10.1 Simplex OVA	CM-Simplex-010.1.0.0.974-e70-0.ova	CM000002017	1212CDB6A2DD06536E440CF8AD0DC3A0
Original Avaya Aura Communication Manager 10.1 Duplex OVA	CM-Duplex-010.1.0.0.974-e70-0.ova	CM000002018	5096E355411F8712C891F0E239BB3F1C

For 8.1 OVAs only.
If blocked when deploying an original 8.1 OVA with vCenter 6.5, utilize Solution Deployment Manager (SDM).

If that is not possible, the following workaround utilizing this VMware KB article has been utilized.
https://kb.vmware.com/s/article/51123

This requires the OVA to be unzipped and then only install the ovf and vmdk files.

Remarks
Issue 1 – January 24, 2023
Issue 2 – January 27, 2023: Updated to clarify deployment of re-signed OVAs via SDM requires SMGR/SDM 10.1.2.
Issue 3 – February 1, 2023: Updated to provide original 10.1 OVAs until launch of 10.1.2.
Issue 4 – February 10, 2023: Updated to include AAMS.
Issue 5 – February 27, 2023: Updated to include Breeze and specify Aura 8.1 OVAs were posted Feb 21.

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?**
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
n/a
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.

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.