Product Support Notice

PSN # PSN006201u

Original publication date: 30-June-2023. This is Issue #01, published date: 30-June-2023.	Severity/risk level	High	Urgency	Immediately

Name of problem

During deployment of Avaya IP Office OVA on VMWare vCenter, a warning may appear indicating publisher certificate is invalid/untrusted.

Products affected

Avaya IP Office OVA 11.1.2.4.0
Avaya IP Office OVA 11.0.4.8.0
Avaya IP Office OVA 11.1.3.0.0 (and later)

Problem description

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.

With the above known issue on VMWare vCenter, during deployment IP Office OVA on VMWare vCenter a warning may appear indicating publisher is certificate invalid if Entrust root CA and intermediate certificates are not present on vCenter setup (VECS store).

This warning will only be visible when deploying an OVA.

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

Solutions

Below steps need be performed only once on vCenter to add Entrust intermediate and root CA certificates to VECS store.

1) Entrust root CA and intermedia certificates are available for download from PLDS ID: **IPO00009485**
2) Download the '**AvayaIPOffice-2023-OVA-CertChain.crt**' file. (This certificate file contains certificates - Entrust Code Signing CA - OVCS2, Entrust Code Signing Root Certification Authority - CSBR1 and Entrust Root Certification Authority - G2)
3) Login to vCenter with Administrator privileges. From the drop-down menu, select **Administration→ Certificates→ Certificate Management**.
4) In the Certificate Management page, select ADD certificae to Trusted Root Certificates
5) Select the '**AvayaIPOffice-2023-OVA-CertChain.crt**' certificate and click ADD.
6) Verify that the root and intermediate certificates are now shown in Trusted Root Certificates. Click on 'VIEW DETAILS' for each certificate.

Note- There may already be existing Trusted Root Certificates in the VECS store. 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.

Remarks

None

Software Update Notes

The information in this section concerns a new software package, recommended in the Resolution above.

Backup before applying the software package

n/a

Download

n/a

Software install instructions

n/a

Verification

n/a

Failure

n/a

Software uninstall instructions

n/a

Service-interrupting?

No

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.