

PSN # PSN005588u

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

Original publication date: 28-Mar-20. This is Issue #01, published date: 28-Mar-20.

Severity/risk level High Urgency Immediately

Name of problem Avaya IP Office OVA Certificate Expiry

Products affected

Avaya IP Office 10.1.0.7

Avaya IP Office 11.0.4.2

Powered by Avaya IP Office (Virtualized) 3.0.4

Problem description

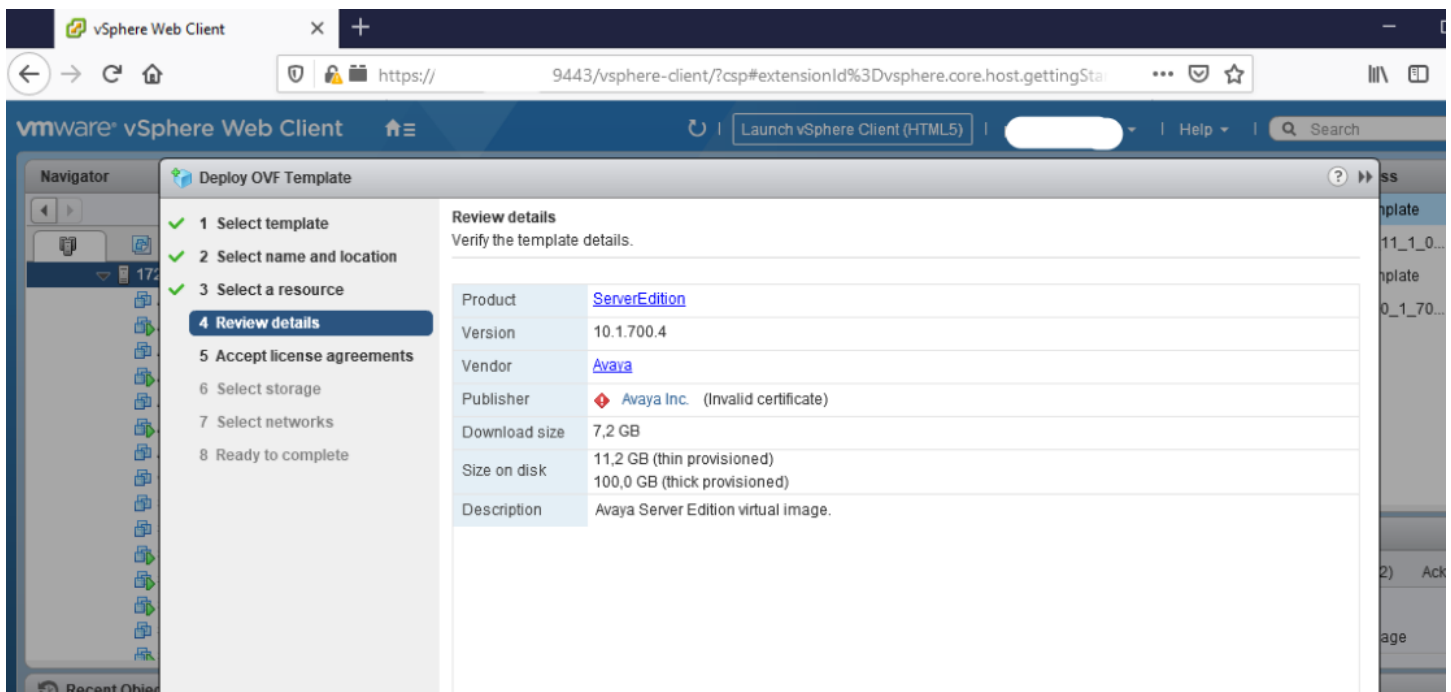
This PSN will be updated as new information is available.

Make sure you are signed up for E-Notifications, available on support.avaya.com under Alerts & Reports → Set E-Notifications

Note: This issue affects IP Office OVA deployments only.

On March 23rd, 2020, the Avaya signing certificate used for the IP Office OVAs listed in the “Products affected” section of this PSN expired. This will result in issues when those OVAs are being deployed.

The following is an example of what might be seen when deploying an OVA with an expired Avaya signing certificate.



Resolution

Avaya is in the process of re-signing the OVAs with a new certificate that will resolve this issue. These new OVAs shall be posted to Avaya Support Portal once Solution Validation is completed. This PSN will be updated at that time.

Current tentative target ETA for availability of new OVA versions of IP Office 10.1.0.7 and 11.0.4.2 as well as Powered by Avaya IP Office (Virtualized) 3.0.4 is week of 6th April.

No changes to software or functionality will occur in these new OVAs. The only change is that the certificate and the signature file will be renewed. The OVA file name will change to reflect a new version number.

Workaround or alternative remediation

n/a

Remarks

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](#).

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.