

PSN # PSN005994u

Original publication date: 17-Jan-2022. This is Issue #02, published date: 31-Jan-2022. Severity/risk level Medium Urgency Optional

### Name of problem

IP Office Container Telephony Certificate expiry

### Products affected

IP Office Powered by Container all releases

### Description

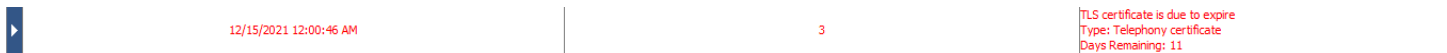
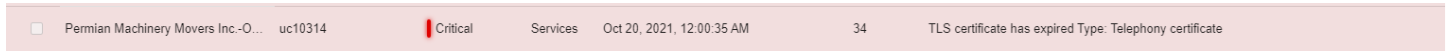
This issue affects sites that do not have Auto Cert Management enabled (see the Resolution section of this document for details of how to check this auto-renewal functionality is enabled).

The IP Office Container self-signed telephony certificate is approaching its expiry date and without Auto Cert Management enabled will incur endpoint disconnects once the certificate expires.

The IP Office will initiate an alert 13 days before the telephony certificate expiry date which will be visible in COM and SSA under the critical alarm category.

If the certificate is left to expire telephony endpoints will become disconnected from the IP Office and will need to be manually reconfigured to reconnect.

### COM Screenshot of alert:



**Note: a similar alert will be seen in SSA**

### Limitations:

### Resolution

At least 36 hours before the telephony certificate expires the following procedure should be followed to enable Automatic Certificate Management and to obtain and apply a new telephony certificate to the system and its registered endpoints.

- Upgrade IP Office to 11.0.5300.81 or later build through COM.
- Wait for 15 minutes and make sure all hard phones and Workplace IX clients register with IP Office
- Launch IP Office Administrator interface (port 8443) and login as "BusinessPartner"
- Navigate to Security --> Certificate screen
- Enable "Use Deployment Root CA" and "Automatic Phone Provisioning"

Security Settings | uc10547

- General
- System
- Services
- Rights Groups
- Service Users
- Certificates

GlobalSign	GlobalSign	2006-12-15 08:00:00	2021-12-15 08:00:00	↓	🗑️	ℹ️
GlobalSign	GlobalSign	2006-12-15 08:00:00	2021-12-15 08:00:00	↓	🗑️	ℹ️
GTS Root R1	GTS Root R1	2016-06-22 00:00:00	2036-06-22 00:00:00	↓	🗑️	ℹ️
GTS Root R2	GTS Root R2	2016-06-22 00:00:00	2036-06-22 00:00:00	↓	🗑️	ℹ️
Entrust Root Certification Auth...	Entrust Certification Authority ...	2015-10-05 19:13:56	2030-12-05 19:43:56	↓	🗑️	ℹ️

Use different certificate for telephony

Offer Certificate  YES

Offer ID Certificate Chain  YES

Private Key

Issued To:

Use Deployment Root CA  YES

Automatic Phone Provisioning  YES

- Wait for all hard phones and Workplace IX clients to register with IP Office
- Login again to IP Office Administrator interface (port 8443) and login as "BusinessPartner" (Logout if already login)
- Navigate to Security --> Certificate screen and click on the "View" button

Security Settings | uc10547

- General
- System
- Services
- Rights Groups
- Service Users
- Certificates

GlobalSign	GlobalSign	2006-12-15 08:00:00	2021-12-15 08:00:00	↓	🗑️	ℹ️
GlobalSign	GlobalSign	2006-12-15 08:00:00	2021-12-15 08:00:00	↓	🗑️	ℹ️
GTS Root R1	GTS Root R1	2016-06-22 00:00:00	2036-06-22 00:00:00	↓	🗑️	ℹ️
GTS Root R2	GTS Root R2	2016-06-22 00:00:00	2036-06-22 00:00:00	↓	🗑️	ℹ️
Entrust Root Certification Auth...	Entrust Certification Authority ...	2015-10-05 19:13:56	2030-12-05 19:43:56	↓	🗑️	ℹ️

Use different certificate for telephony

Offer Certificate  YES

Offer ID Certificate Chain  YES

Private Key

Issued To:

Use Deployment Root CA  YES

Automatic Phone Provisioning  YES

- The IP Office telephony certificate should renew and should show the new telephony certificate expiry date

Note: The above procedure needs to be administered before the IP Office telephony certificate expires.  
If the telephony certificate has already expired then follow the above procedure and at the end, all hard phones need to be factory reset and reconfigured to register with the IP Office.  
The Avaya Workplace IX client may also need to be reconfigured for registering with IP Office.

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

n/a

Verification

n/a

Failure

n/a

Patch uninstall instructions

Service-interrupting?

## 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](https://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.