Product Support Notice

PSN #	PSN005042u

Original publication date: 2-Aug-2017. This is Issue #02, published date: 7-Nov-2017	Severity/risk level*	Medium	Urgency*	When convenient

Name of problem*

IP Office 500v2 systems with self-signed certificates have started in some cases to generate a warning about expiry in Manager and the display of 96x1 telephones

Products affected*

IP Office 500v2

Problem description*

IP Office 500v2 systems that don't have a time reference at first boot from the warehouse adopt a default time and date format of Midnight, 1st Jan 2011. Further as a part of the start-up sequence, they check for the presence of an Identity Certificate. If it is not there, like in the case for a new system, it will create a default self-signed certificate.

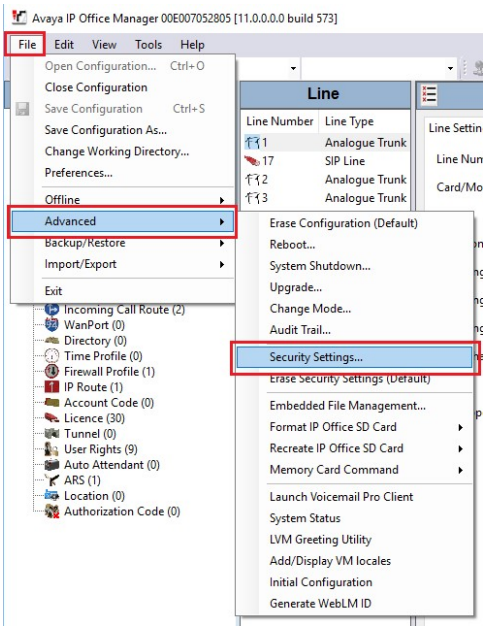
The life of this default self-signed certificate is 7 years. So any system that did not have a time reference and has not had an externally generated certificate loaded to it, or had its Security Settings reset which will regenerate the certificate, will expire at the end of 2017.

Regardless of the type of certificate, IP Office manager provides an advanced warning (180 days by default) of the IP Office identity certificate expiry so that the Administrator or Maintainer can take appropriate action.

Best practice for a new installation is to make sure that there is a time server available when powering up the unit initially, or to regenerate the certificate (explicitly or reset the security settings) after setting the time and date.

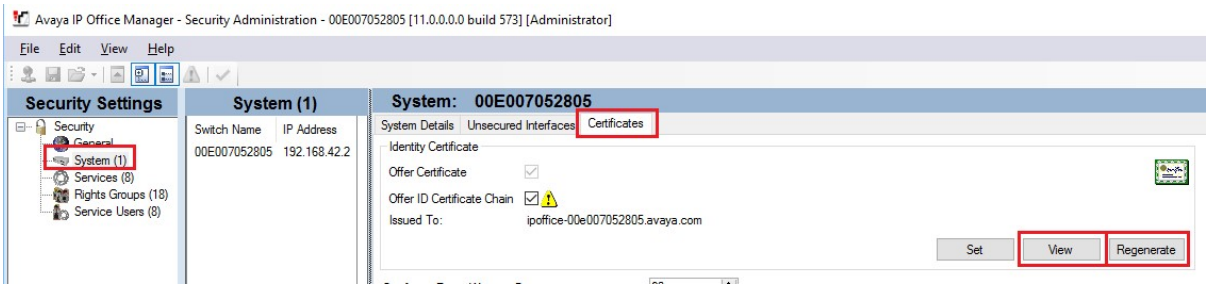
Resolution*

For the Self Signed certificate, the simplest action is to delete/regenerate it through the Security settings in IP Office Manager under **File** > **Advanced** > **Security Settings…**

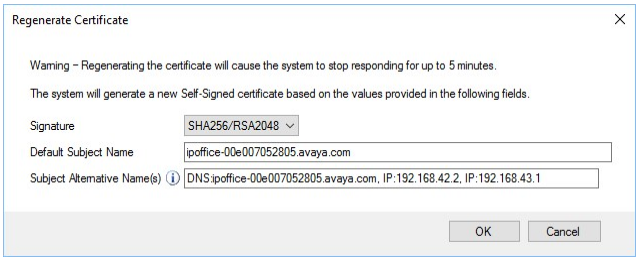


Note: This action should be performed outside normal operating hours as certificate generation is computationally intensive and may impact the functionality of IP Office.

1. The options are under **System** and in the **Certificates** tab. There are options to **View** the current certificate and **Regenerate** it. In older Manager releases, that button is labelled as **Delete**.



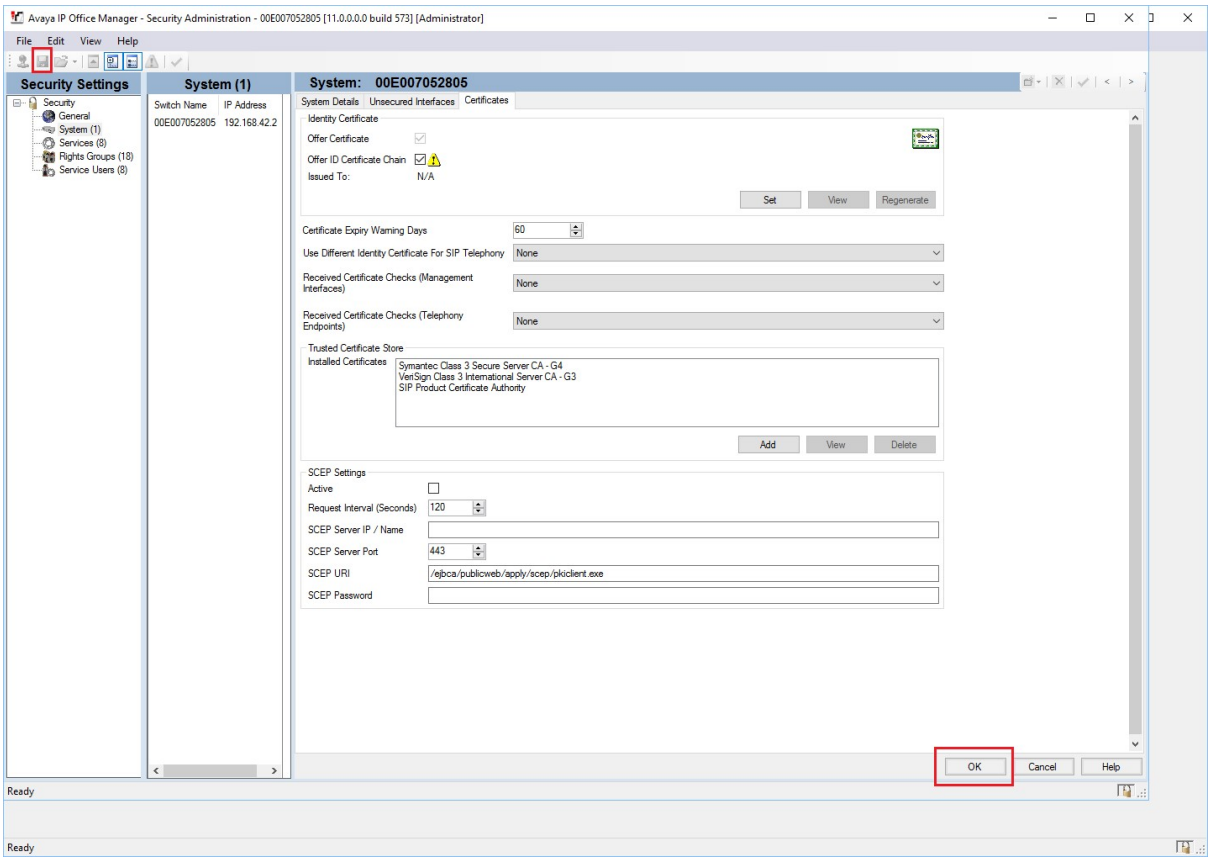
2. On clicking the **Regenerate** (or **Delete**) Button, a window appears that displays the settings to be used to create the new certificate (as shown in the screenshot below):



3. For the default self-signed certificate, the default parameters can be accepted by clicking OK. For non-default certificates, follow the procedure that was used while generating it initially or use the documentation for guidance for extra information that may be required.

WARNING: The next step will trigger the regeneration of the IP Office Identity Certificate and this action should be performed outside normal operating hours as certificate generation is computationally intensive and may impact the functionality of the IP Office.

4. Click OK at the bottom of the form and then save the security settings.
   The re-creation will start.



More information on these options is available in the online manual:
http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/manager/Certificate.html

For an external certificate, a new certificate should be obtained and uploaded.
The new certificate may need to be distributed to client applications to ensure continued service.

Distributing New Certificate

When an external certificate is updated, you should check the requirements to distribute the authorized certificate to clients. For example, if you are using a certificate from a well-known public issuer, their certificate will likely be there in your PC's/Smart Phone's CA cache.
For a self-signed certificate, the new certificate should be distributed to any application or client that uses it and this must be coordinated with loading it to the IP Office, else certificate checks will fail. For most applications, this is in the installation manual.

Updating Certificate on Remote H323 Extensions

This process shows how to remove the current license from the phone, so that the phone will not be able to perform certificate checks. The IP Office certificate can then be renewed and downloaded to the phones like it was done in initial deployment.

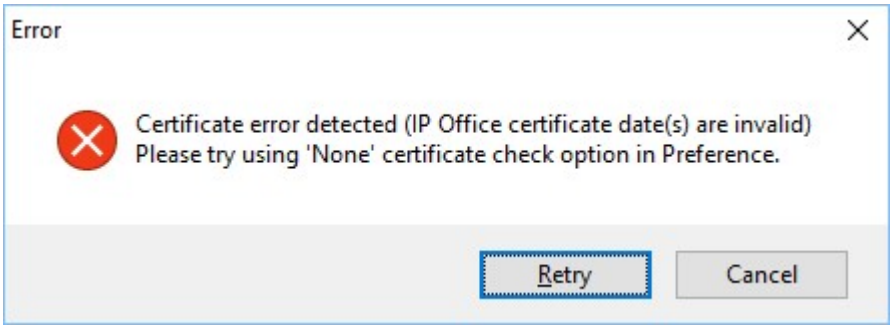
1. Download the `46xxsettings.txt` file from the IP Office. This can be done by simply entering `http://192.168.42.1/46xxsettings.txt` in a browser. This URL is case-sensitive. However, you can modify IP Address as required. Copy the above link and paste it in a text editor like Notepad.
2. Edit the line with the certificate: `SET TRUSTCERTS "Root-CA-01234ABC.pem"` (filename will be different)
   To remove the certificate filename: `SET TRUSTCERTS ""`.
3. Save the file to the PC.
4. If there is already an explicit `46xxsettings.txt` on the SD card, temporarily rename it (For example: `46xxsettings.bak`).
5. Paste the edited file to the SD card.
6. Restart all the remote phones, using SSA for example. Watch SysMon to ensure that all phones obtain the new settings file.
   At this stage, the telephones will delete the stored certificate(s).
7. Refresh the certificate on the IP Office.
8. Delete the `46xxsettings.txt` file. Where there was a file on the card previously, it needs to be updated with the new certificate filename. Obtain that by the above process and edit the `46xxsettings.bak` to include the new filename, and then save it back with the `.txt` extension.
9. Restart the phones again. They will then download the new certificate and normal functionality will be restored.

If this process fails, then the phones can be reset to remove the old certificate using the CLEAR procedure, then re-configuring them after the IP Office certificate has been regenerated.

Impact of Allowing Certificate to Expire

The IP Office identity certificate should be renewed before it expires.
If the certificate expires, several IP Office features and clients will fail or require user interaction to continue.

1. **Manager**



This can be solved by changing certificate checking preference.

2. **Web Based Applications**
   Most browsers will give a warning that the supplied certificate has expired. Most will allow the user to acknowledge the warning and continue working. Future versions may block access.
   This applies to;
   - Web Manager and related applications (Web Control Panel)
     The following use the Server Edition/Apps Server Certificate. So they are not applicable for the IP500v2 certificate expiry, but will apply if the Server certificate expires.
     - WebRTC clients - not applicable to the IP500v2 certificate. The Server Edition/Apps Server Certificate is offered
     - Web Collaboration
     - One-X Portal for IP Office
     - Integrated Contact Recorder
3. **Avaya Feature Phones**
   The 96x1 family phones (9608, 9611, 9621, and 9641) are served with the IP Office certificate in the auto created provisioning file. When the phones are used with the default TCP connection, it displays a warning that the user can ignore. Once the certificate is refreshed, re-boot the phone to download the new one.
   96x1 H323 and SIP, plus other Avaya SIP phones (like the J129) using TLS and HTTPS, any HTTPS connection will fail and the TLS will not re-connect after a TLS link fails or re-keying, leaving the user with no service. To recover, the phone must be cleared using the CLEAR service procedure and re-commissioned.

For 96x1 H323, it is possible to manage the process for getting the new certificate to the phones without clearing and re-commissioning. But it must be performed prior to the expiry. See section:
Distributing New Certificate.

4. **IP Office Line, Web Socket, High Security**
   An IP Office line using Web Sockets and set to High security will fail to connect/re-connect after certificate expiry.
5. **SIP or MS Trunks using TLS**
   There are many permutations but most likely the trunk will fail, on rekeying or at re-connect.
6. **one-X Mobile Applications**
   They will present an error message relating to the certificate expiry. Information on ignoring the error is given.
7. **Avaya Communicator for iPad**
   This will not connect. A new certificate is required.
8. **IP Office Contact Center (IPOCC) and Avaya Contact Center Select (ACCS)**
   It will fail to connect to the IP Office and must be provisioned with a new certificate.

Links:
For certificate summary in Manager manual/help:
http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/manager/Certificate.html

For more information on Certificates in the IP Office security Guidelines:
http://marketingtools.avaya.com/knowledgebase/businesspartner/ipoffice/mergedProjects/security/chapter_6_certificates_and_trust.htm

Workaround or alternative remediation*

For new installations, ensure that there is a time server available when 1st powering up the unit, or to regenerate the certificate (explicitly or reset the security settings) after setting the time/date.

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?
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

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.