Replace SMGR CA

System Manager : How to create a new root CA in SMGR 7.0

Abstract This process defines the steps necessary to replace the default System Manager CA with a new CA in release 7.0 of System Manager (SMGR). Please ensure you read the entire process before beginning.

NOTE: If you are using a Geographic Redundant (GR) pair of SMGR servers then you will need to first disable GR replication and convert the primary to standalone before proceeding. The steps to perform these tasks can be found in the Administering Avaya Aura System Manager document. Once the GR has been removed, you should apply the process below only to the intended primary SMGR and then once complete, reconfigure GR. The new CA will be pushed from the primary SMGR to the secondary SMGR automatically. Body NOTE: There is a known issue within System Manager 7 that causes trust to fail when there is more than one active CA. This is fixed in release 7.0.0.2 under ID SMGR-35243. The process below will remove the original CA to prevent this issue, but if you are already running 7.0.0.2 then you can skip that step and leave both original and new CAs in the system NOTE: As with any process such as this, we advise that a backup be taken prior to beginning First off, it is important to decide what information is needed when creating your new root CA.

There is a utility which is included in release SMGR 7.0 called createCA which allows you to create a root CA quickly and easily in a 1 step process. However, you are limited to only being able to provide a Common Name (CN) value for the new root CA.

If this is ok, then please refer to the Administering System Manager guide for details on how to run the createCA.bin script and ignore the following steps.

However, if you want to have more control over the values of your new root CA such as providing more information in the subject DN than just the CN or configuring the Signing Algorithm, etc then please follow the steps below to manually create your new root CA.

NOTE: As with any process such as this, we advise that a backup be taken prior to beginning First of all you need to define the new Crypto Token to be used by the new root CA. To do this, log into the SMGR web interface, navigate to Security→Certificates→Authority and click on the Crypto Tokens menu on the left

Click on the Create new… link

Enter a name for the new token such as newCACryptoToken.

Enter and confirm an Authentication Code which may be used when accessing the SMGR using this token at a later date.

Ensure the Auto-activation checkbox is ticked and then click on the Save button.

Next, you need to generate 2 separate key pairs.

To do this, click on the Generate new key pair button to generate the default privatesignkeyalias key pair

Then, overwrite the privatesignkeyalias entry with privatedeckeyalias and click on the Generate new key pair button again.

You should now have 2 unique key pairs called privatesignkeyalias and privatedeckeyalias

Click on the Back to Crypto Token overview link to return to the main Crypto Token page.

Click on the Certification Authorities menu on the left

Enter a temporary name for your new CA such as newCA and click on the Create button.

You will then see a screen where the components of the new CA can be configured.

Select your new Crypto Token from the drop down list in the Crypto Token section.

Then ensure you set the defaultKey, keyEncryptKey, hardTokenEncrypt, testKey entries to be the privatedeckeyalias key pair

Also, set the certSignKey to be the privatesignkeyalias key pair

Then, adjust the settings as necessary for example:

Signing Algorithm SHA256WithRSA Extended Services Key Specification (RSA key size) RSA 2048 Subject DN CN=Tonys SMGR CA,OU=ETSS,O=AVAYA,L=PONTYPRIDD,ST=CARDIFF,C=GB Validity 1825d

NOTE: Ensure that the Signed By field is set to Self Signed

When finished, click on the Create button

You will then see that there are 2 active CAs. The original (tmdefeaultca) and the new CA (newCA)

You should now proceed to rename the CAs.

To do this, select tmdefaultca from the list box and in the text box below, enter a new name such as originalCA. Click on the Rename button

Then select the new CA from the list box and in the text box, enter the value tmdefaultca and click on the Rename button again

You should now have the same 2 active CAs but the original tmdefaultca is called originalCA and your new CA is called tmdefaultca

Click on the Certificate Profiles menu on the left

Edit each of the following profiles in turn and ensure that the tmdefaultca CA is selected in the Available CAs list box and then click on the Save button:

ID_CLIENT ID_CLIENT_SERVER ID_SERVER

Next, click on the End Entity Profiles menu on the left

Edit each of the following profiles in turn and ensure that the tmdefaultca CA is selected in the Available CAs list box and also that the Default CA is set to tmdefaultca and then click on the Save button:

EXTERNAL_CSR_PROFILE INBOUND_OUTBOUND_TLS INBOUND_TLS OUTBOUND_TLS

Next, click on the Search End Entities menu on the left

Set the Search end entities with status field to All and click on the Search button

This will display a list of all End Entities:

Check the CA column and if it already shows tmdefaultca then you can skip that entity and move on to the next one.

If it doesn't show tmdefaultca then click on the Edit End Entity link on the right of the Entity and change the CA field to tmdefaultca and then click on the Save button followed by the Close button.

Once all of the Entities have been updated, click on the Search button again to refresh the list and now all Entities should show tmdefaultca in the CA column.

NOTE: You only need to perform the step below if you are not running release 7.0.0.2 or later due to a known product defect covered by ID SMGR-35243

Click on the Certification Authorities menu on the left

Select the originalCA and click on the Delete CA button.

You will be prompted to confirm deletion. Click on the OK button

You have now deleted the originalCA and will no longer be affected by the product defect. You should now continue with the rest of the process

NOTE: You only need to perform the step above if you are not running release 7.0.0.2 or later due to a known product defect covered by ID SMGR-35243

Next, navigate on the SMGR dashboard to Inventory→Manage Elements and select the System

Manager entry. Click on More Actions→Configure Identity Certificates

You should be presented with a list of certificates. Select the Management certificate and scroll down to make a note of the Issuer Name of that certificate. It should be the current CA (originalCA).

Now, we need to regenerate all of the certificates using the new CA. To do this, log into the SMGR CLI using SSH and run the following command as the root user:

NOTE: This is one single command that may be shown on multiple lines due to its length

Version 7: sh /opt/Avaya/Mgmt/7.0.9/trs/trust_initializer_install.sh -RMIPORT 1399 -HTTPSPORT 443 -TMCONFIGLOC /opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/tm/

Version: 7.1 sh /opt/Avaya/Mgmt/7.1.11/trs/trust_initializer_install.sh -RMIPORT 1399 -HTTPSPORT 443 -TMCONFIGLOC /opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/tm/

Version: 8.1 sh /opt/Avaya/Mgmt/8.1.7/trs/trust_initializer_install.sh -HTTPSPORT 443 -TMCONFIGLOC /opt/Avaya/JBoss/wildfly-10.1.0.Final/avmgmt/configuration/tm/

This command should take about a minute to run and once complete you should get a message indicating ‘TM Initialization success’

If you receive a failure response, please try the above command again and if it still fails then do not proceed any further and engage Avaya support for assistance.

If you receive a success response then you should restart the SMGR services to load the new certificates using the command below run as the root user:

```
service jboss restart
```

After about 15 minutes, the SMGR web interface should be available again. Log back in and navigate back to Inventory→Manage Elements and select the System Manager. Click on More Actions→Configure Identity Certificates and select the Management certificate again.

This time the Issuer Name should be your new CA. This will be the same for all of the certificates in the list except for the WebLM Legacy certificate. This is a special certificate that is not issued by the SMGRs CA.

NOTE: It is important to realize that as SMGR is now using certificates that have been issued by your new CA, communication will be broken between SMGR and certificate trusted products such as Session Manager, Presence or EDP. You should now reinitialize trust on those products so that they begin to trust the SMGR again and vice-versa.