Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.3.x and 7.0.x

Issue 1.3

November 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation Disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operation instructions and performance specifications that Avaya generally makes available to users of its products.

Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Contents

INTRODUCTION

This document is for the System Manager 6.3.x and 7.0.x releases. The document lists the steps required for supporting third-party certificates in System Manager.

SCOPE

The scope of this document is limited to the configuration of Container TLS service certificate of System Manager with third-party certificate.

PROCEDURE TO IMPORT THIRD PARTY CERTIFICATES INTO SYSTEM MANAGER

Pre-requisite:

- A certificate needs to be generated with the hostname as the CN, Subject Alternative Name as the FQDN and VFQDN (Refer section for getting VFQDN value) of that machine, as DNS name, and signed by the third-party certificate authority (CA). Refer Identity Certificate Attributes section for more details about certificate attributes in certificate.
  Note - FQDN and VFQDN must be different and unique must match FQDN and VFQDN values provided during System Manager installation. VFQDN must be same for primary and secondary System Manager if Geographic Redundancy is enabled.
  Note– Refer Section 4 for getting VFQDN of System Manager.
- In the Geographic Redundancy environment, secondary System Manager certificate needs to be generated with the hostname as the CN, Subject Alternative Name as VFQDN and FQDN of secondary System Manager, as DNS name.
- The enhanced key usage of the certificate must have Server Authentication and client Authentication values.
- The PKCS#12 format file must include the private key and the associated third party identity certificate and the chain of all Sub CA/intermediate CA and root CA in its issuing hierarchy.
- The third-party CA certificate is required including all Sub CA/intermediate CA and root CA in the issuing hierarchy of the identity certificate.
- Recommended certificate signature algorithm is SHA-256 With RSA.
- Create a backup of System Manager. Avaya recommends storing the backup on an external device. For more information on creating a backup of the installed System Manager data, see the System Manager Release Notes of the respective release on the Avaya Support site.
- Before starting with following steps, disable the Geographic Redundancy replication.

- **Section 1** contains steps for replacing Container TLS service certificate of system manager with third-party certificate.

- **Section 2** contains steps for replacing Container TLS service certificate of secondary system manager with third-party certificate in case of Geographic redundancy environment.

- **Section 3** contains steps for supporting third-party certificate in different elements like Session Manager, Branch Nodes and more.

IDENTITY CERTIFICATE ATTRIBUTES

The certificate attributes for the identity certificates of Container TLS service in System Manager is mentioned in the table below. While replacing the certificate with System Manager CA or External CA signed certificate strictly ensure that the new identity certificate has the mentioned attributes. This is required for correct functionality of System Manager and other related elements.

Management Container TLS Service

Attribute	Value	Required?
Subject	`CN={system-manager-fqdn}`	required
Validity	*validity period*	required
Authority Key Identifier	*Hash*	required [1]
Subject Key Identifier	*Hash*	recommended

Key Usage	`digitalSignature`
	`nonrepudiation`
	`keyEncipherment`
		required
		optional
		required

Extended Key Usage	`id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1` `id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2`	required required [2]
Subject Alternative Name	`DNS:{system-manager-vfqdn}` `DNS:{system-manager-fqdn}`	required[3] required
Authority Information Access	`OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}`	optional[4]
CRL Distribution Points	`URI:http://{crl-server}{:crl-port}{/crl-path}` `URI:ldap://{crl-server}{:crl-port}{/crl-dn}` [6]	optional[4] optional[4]

1. Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
2. Required as this Identity Certificate is used when the server is acting as a client (TLS mutual authentication)
3. System Manager VFQDN is required for communication with geo-R aware elements like Session Manager. VFQDN is required even for standalone System Manager deployment.

   VFQDN can be found using one of the below methods:
   - Using the curl command access the following url like:
     $ **curl --connect-timeout 1 -k -silent https://{system-manager-fqdn}/ws/grservice/getgrstate/test**
     Refer tag <virtualFQDN> grsmgr.smgrdev.avaya.com </virtualFQDN> for the value. Here grsmgr.smgrdev.avaya.com is the VFQDN

   - Access the url : **https://{system-manager-fqdn}/ws/grservice/getgrstate/test** on the browser. An output like the following is received:
     STANDALONE 148.147.162.203 pdev26vm3.smgrdev.avaya.com STANDALONE 127.0.0.1 grsmgr.smgrdev.av aya.com 7.1.11.710006664 2017-05-08T09:52:16.330Z
     Here grsmgr.smgrdev.avaya.com is the VFQDN, the value before the release number text

   - On System Manager CLI view the read the following file like:
     $ **cat $MGMT_HOME/infra/conf/smgr-properties.properties**
     Look for the value of property virtualFQDN

4. Optionally required: System Manager and other Aura elements do not carry out revocation checking, but if other devices in the network require revocation checking information may be required.

Section 1: For Primary System Manager or Standalone System Manager

STEP 1: Replace the System Manager Web Server identity certificate with the third party certificate by using System Manager Console.

Replace an identity certificate

1. On the System Manager console, under **Elements**, click **Inventory.**
2. Click **Manage Elements** in the left navigation pane.
3. On the Manage Elements page, select **System Manager** and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificate page, select **Container TLS Service.**
5. On the Identity Certificate page, click **Replace**.
6. On the Replace Identity Certificate page, perform following step:
    - Click **Import third party PCKS # 12** file and do the following:
        - Enter the file name in the **Please select a file** field.
        - Enter the password in the **Password** field.
        - Click **Retrieve Certificate**. The Certificate Details section displays the details of the certificate.
        - Click **Commit** to replace the certificate with the imported third-party certificate.

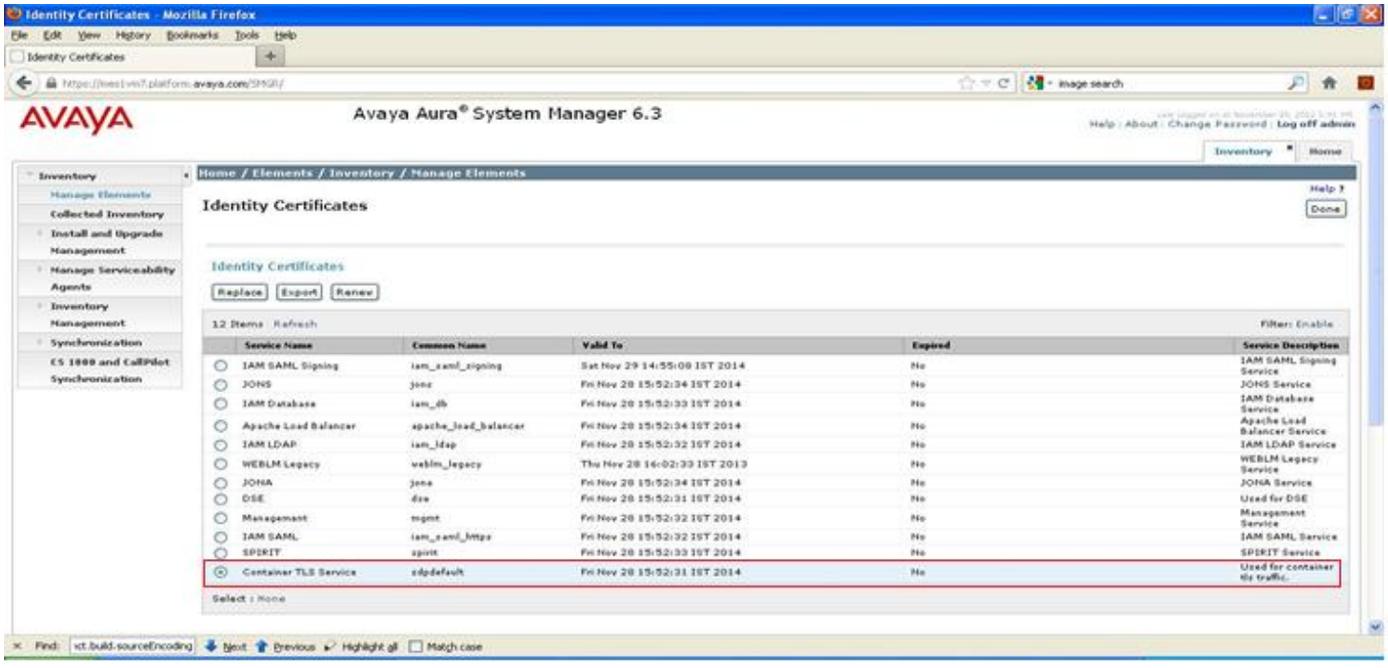


Figure 1: System Manager Identity Certificates

STEP 2: Add the third party CA certificate to Primary System Manager or standalone System Manager Trusted certificate Stores.

Add certificate to System Manager trusted certificate store using System Manager Console

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Inventory** in the left navigation pane.
3. On the Manage Elements page, select **System Manager** and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add**
5. On Add Trusted Certificate page, select **Store Type to add trusted certificate** as **All**.
6. On Add Trusted Certificate page, select **Import from file**.
7. On Add Trusted Certificate page, browse third party Root CA certificate for **Please select a file**.
8. On Add Trusted Certificate page, click **Retrieve Certificate**.
9. On Add Trusted Certificate page, click **Commit**.

Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

.

Note: Do not delete any certificate from System Manager trusted certificate store.

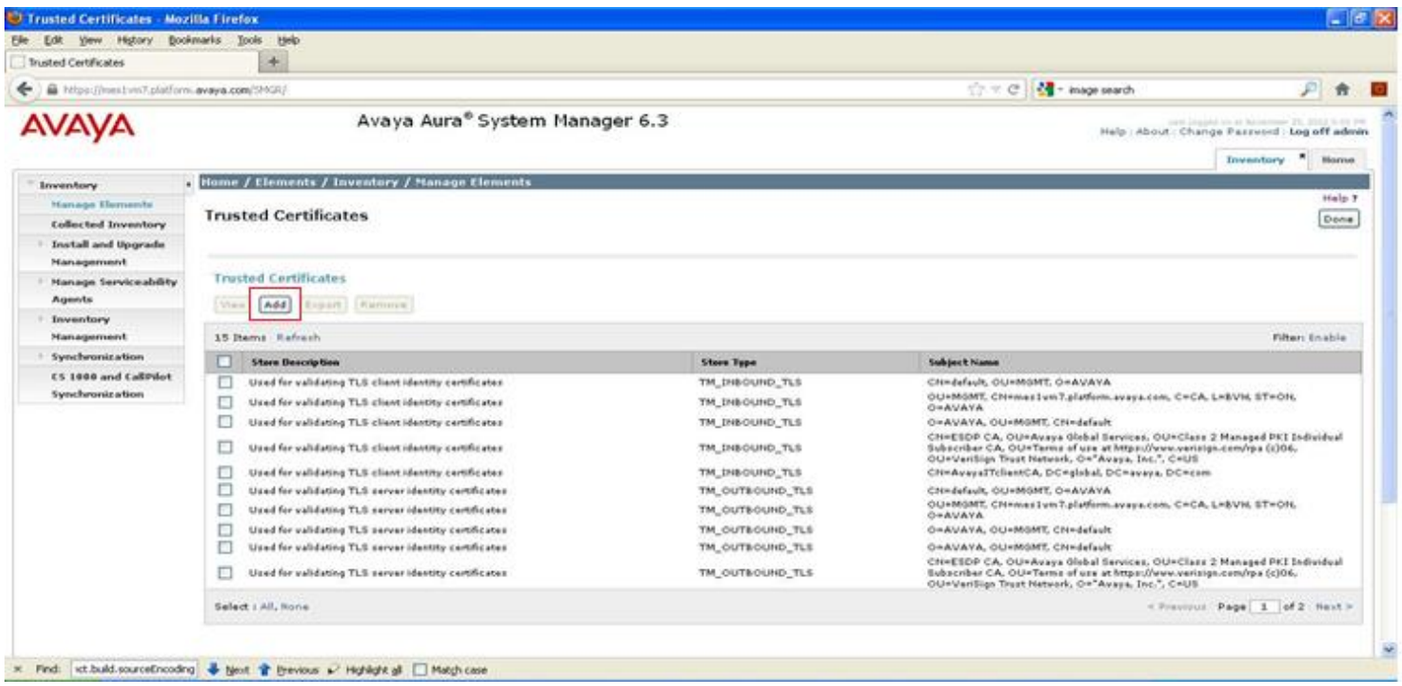


Figure 2: System Manager Trusted Certificates

Add third party Root CA certificate to System Manager Spirit Agent service's trusted certificate store

1. From System Manager C L I , execute the below as a **root user**
   # sh $SPIRIT_HOME/scripts/configureSpiritSecurity.sh

If the system is already configured in Geographic Redundancy environment with Session Manager and EDP configured with System Manager, then do the steps mentioned in section 'For Session Manager, Branch Session Manager, and Personal Profile Manager Nodes' under Section 3 and then proceed with next steps.

STEP 3: Restart JBoss at System Manager.

Restart JBoss

1. From System Manager C L I , execute the below as a **root user**
   #**service jboss restart**

STEP 4: Restart SystemMonitor service on System Manager.

Restart SystemMonitor

1. From System Manager C L I , execute the below as a **root user**
   #**service systemMonitor restart**

Note: Once Jboss service is restarted, access System Manager web console after 15 minutes. Validate the third party certificate by accessing it from the Primary System Manager web console in browser and matching with the 3rd party certificate thumbprint.

Section 2: For Secondary System Manager

Perform the following steps if the System Manager is deployed in Geographic Redundancy environment. Follow the steps in **Section 2.A** and **Section 2.B** according to following points.

- If the primary System Manager is already configured with the third-party certificate and if you want to configure the System Manager in Geographic Redundancy environment, then perform steps in **Section 2.A** on Secondary System Manager before configuring Geographic Redundancy.
- If the system is already configured in Geographic Redundancy environment and steps in Section 1 have been already performed and have to configure secondary System Manager with third-party certificate, then perform steps in **Section 2.B**.

Section 2.A: If the primary System Manager is already configured with third-party certificate and wants to configure System Manager in Geographic Redundancy environment.

Add CA certificate to Secondary System Manager trusted certificate store using Secondary System Manager UI

1. On the Secondary System Manager console, under **Elements**, click **Inventory**.
2. Click **Inventory** in the left navigation pane.
3. On the Manage Elements page, select **System Manager** and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add**
5. On Add Trusted Certificate page, select **Store Type to add trusted certificate** as **All**.
6. On Add Trusted Certificate page, select **Import from file**.
7. On Add Trusted Certificate page, browse third party Root CA certificate for **Please select a file**.
8. On Add Trusted Certificate page, click **Retrieve Certificate**.
9. On Add Trusted Certificate page, click **Commit**.

Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

Note: Do not delete any certificate from Secondary System Manager trusted certificate store.

Add third-party Root CA certificate to Secondary System Manager Spirit Agent service's trusted certificate store

10. From Secondary System Manager C L I , execute the below as a **root user**
    # sh $SPIRIT_HOME/scripts/configureSpiritSecurity.sh

Restart JBoss

11. From Secondary System Manager C L I , execute the below as a **root user**
    #**service jboss restart**

Restart SystemMonitor

12. From Secondary System Manager C L I , execute the below as a **root user**
    #**service systemMonitor restart**

Note: Now you can configure Geographic Redundancy and enable replication. If you want to replace secondary system manager with third-party certificate, follow steps Step no. 1, 3 and 4 in Section 2.B

Section 2.B: In case system is already configured in Geo environment and steps in Section 1 have been already performed and have to configure secondary System Manager with 3rd party certificate.

Please make sure to replace the secondary system manager web server identity certificate with correct third party certificate i.e. 3rd party certificate with correct secondary system manager parameters.

STEP 1: Replace the Secondary System Manager Web Server identity certificate with the third party certificate using Primary System Manager Console.

Replace an identity certificate

1. On the Primary System Manager console, under **Elements**, click **Inventory.**
2. Click **Manage Elements** in the left navigation pane.
3. On the Manage Elements page, select **Secondary System Manager** and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificate page, select **Container TLS Service.**
5. On the Identity Certificate page, click **Replace**.
6. On the Replace Identity Certificate page, perform following step:
    - Click **Import third party PCKS # 12** file and do the following:
        - Enter the file name in the **Please select a file** field.
        - Enter the password in the **Password** field.
        - Click **Retrieve Certificate**. The Certificate Details section displays the details of the certificate.
        - Click **Commit** to replace the certificate with the imported third-party certificate.

STEP 2: Add the third party CA certificate to Secondary System Manager Trusted certificate Stores.

Add certificate to Secondary System Manager trusted certificate store using Primary System Manager Console

1. On the Primary System Manager console, under **Elements**, click **Inventory**.
2. Click **Inventory** in the left navigation pane.
3. On the Manage Elements page, select **Secondary System Manager** and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add**
5. On Add Trusted Certificate page, select **Select Store Type to add trusted certificate** as **All**.
6. On Add Trusted Certificate page, select **Import from file**.
7. On Add Trusted Certificate page, browse third party Root CA certificate for **Please select a file**.
8. On Add Trusted Certificate page, click **Retrieve Certificate**.
9. On Add Trusted Certificate page, click **Commit**.

Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

Note: Do not delete any certificate from Secondary System Manager trusted certificate store.

Add third party Root CA certificate to Secondary System Manager Spirit Agent service's trusted certificate store

2. From Secondary System Manager C L I , execute the below as a **root user**
   # sh $SPIRIT_HOME/scripts/configureSpiritSecurity.sh

STEP 3: Restart JBoss at Secondary System Manager Node via SSH using root user.

Restart JBoss

2. From Secondary System Manager C L I , execute the below as a **root user**
   #**service jboss restart**

STEP 4: Restart SystemMonitor service at Secondary System Manager Node via SSH using root user.

Restart SystemMonitor

1. From Secondary System Manager C L I , execute the below as a **root user**
   #**service systemMonitor restart**

Note: Validate the third party certificate by accessing it from the Secondary System Manager web console in browser and matching with 3rd party certificate thumbprint.

If you have other elements then follow the steps in Section 3 or else you are done with configuring 3rd party certificate and can enable Geographic Redundancy replication.

Note: These steps need to be carried out after the steps in Section 1 and Section 2.

Section 3: For Managed Elements

The steps in this section need to be carried out based on the deployment environment. Execute specific steps on deployed boxes if deployed environment has Session Manager Nodes, Branch Session Manager Nodes. Also, separate steps needs to be executed in case of Presence nodes or Conferencing nodes.

For Session Manager, Branch Session Manager, and Personal Profile Manager Nodes

STEP 1: Add the third party CA Certificate to Session Manager trusted certificate store using System Manager Console.

Add certificate to Session Manager trusted certificate store

1. On the System Manager console, under **Elements**, click **Inventory**.
2. Click **Manage Elements** in the left navigation pane.
3. On the Manage Elements page, select Session Manager Entity and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add.**
5. On Add Trusted Certificate page, select **Select Store Type to add trusted certificate** as **All**.
6. On Add Trusted Certificate page, select **Import from file**.
7. On Add Trusted Certificate page, browse third party Root CA certificate for **Please select a file**.
8. On Add Trusted Certificate page, click **Retrieve Certificate**.
9. On Add Trusted Certificate page, click **Commit**.

   Repeat the above steps for Intermediate CA certificates if Intermediate CA certificates present in Identity certificate chain.

STEP 2: Restart Service at Session Manager Node.

Restart Service

1. Access Session Manager SSH by using **CLI** credentials and execute
   # restart mgmt

Note: This would be required to be done for all Session Manager Nodes in the deployed environment.

For Conferencing nodes

STEP 1: Add the third party CA certificate to Conferencing node via SSH using root user.

Add certificate to Conferencing trusted certificate store

1. Access Conferencing server SSH, as a **root** user.
2. Add third party Root CA certificate to SAL Agent trust store at Conferencing node $SPIRIT_HOME/security/spirit-trust.jks

   Execute keytool command to add certificate
   *Keytool **-import** {-alias alias} {-file cert_file} [-keypass keypass] {-noprompt} {-trustcacerts} {-storetype storetype} {-keystore keystore} [-storepass storepass] [-provider provider_class_name] {-v} {-Jjavaoption}*

   #keytool -import -file ca-crt.pem -keypass password -keystore $SPIRIT_HOME/security/spirit-trust.jks -storepass samplepassord

   The keystore password is stored at $SPIRIT_HOME/security/securityConfig.properties.

   The property ***com.avaya.spirit.security.keyStorePasswordKey*** holds the keystore password.

   Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

3. Restart SPIRIT Service

For Presence nodes

STEP 1: Add the third party CA certificate to Presence node via SSH using root user.

Add certificate to Presence trusted certificate store

1. Access Presence SSH, as a **root** user.
2. Add third party Root CA certificate to trust store $JABBER_HOME/certs/generic.keystore.jks
3. Execute command to add certificate

   # sh $PRES_HOME/presence/bin/prescert addTrusted pem <pem-file-path> [alias <alias-name>] - add a trusted certificate to the JKS keystore and trust PEM file
4. Add third party Root CA certificate to SAL Agent trust store at Presence node $SPIRIT_HOME/ security/spirit-trust.jks

   Execute keytool command to add certificate

   *Keytool **-import** {-alias alias} {-file cert_file} [-keypass keypass] {-noprompt} {-trustcacerts} {-storetype storetype} {-keystore keystore} [-storepass storepass] [-provider provider_class_name] {-v} {-Jjavaoption}*

   #keytool -import -file ca-crt.pem -keypass password -keystore $SPIRIT_HOME/security/spirit-trust.jks -storepass samplepassword

   The keystore password is stored at $SPIRIT_HOME/security/securityConfig.properties.

   The property ***com.avaya.spirit.security.keyStorePasswordKey*** holds the keystore password.

   Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

5. Restart Service
   #sh $PRES_HOME/presence/bin/stop.sh
   #sh $PRES_HOME/presence/bin/start.sh

For CS1K nodes

STEP 1: Add the third party CA certificate to CS1K node via System Manager Console.

Note: For CS1K members registered to the System Manager, the CA certificate needs to be pushed out to CS1K members as well. Update the trust list for each member by choosing the members (Certificate endpoints) and follow the steps mentioned above.

Add certificate to CS1K nodes using System Manager Console

1. On the System Manager console, under Elements, click Inventory.
2. Click Manage Elements in the left navigation pane.
3. On the Manage Elements page, select CS1K entity and click More Actions > Configure Trusted Certificates.
4. On the Trusted Certificate page, click Add.
5. On Add Trusted Certificate page, select Select Store Type to add trusted certificate as All.
6. On Add Trusted Certificate page, select Import from file.
7. On Add Trusted Certificate page, browse third party Root CA certificate for Please select a file.
8. On Add Trusted Certificate page, click Retrieve Certificate.
9. On Add Trusted Certificate page, click Commit.

Repeat the above steps for all Intermediate/Sub CA certificates in the Identity certificate chain.

The CS1K Server needs to be restarted. The changes will take effect only after the server restarts.

Section 4: Getting VFQDN value of System Manager.

Step 1: Login to System Manager through CLI, as admin user.
Step 2: Run following command:

```
cat $MGMT_HOME/infra/conf/smgr-properties.properties
```

In the output of above command virtualFQDN attribute value is VFQDN.

APPENDIXES

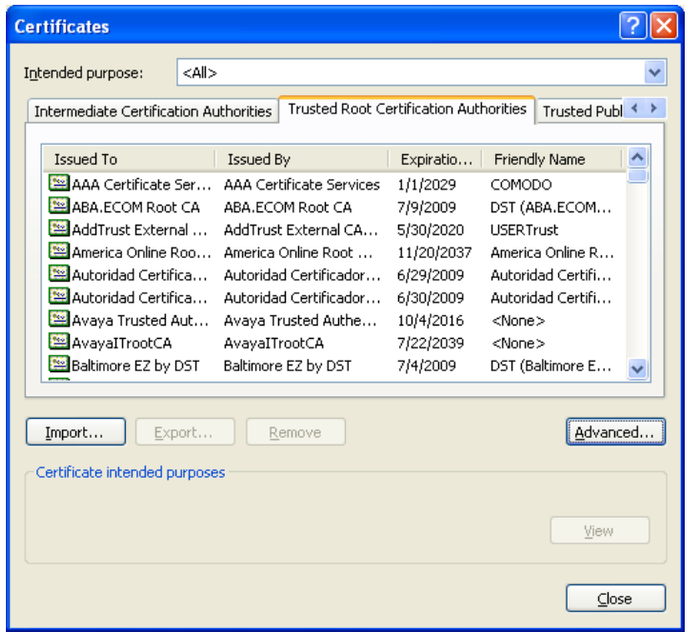
Appendix 1 - PROCEDURE TO DISABLE A CERTIFICATE PROMPT IN INTERNET EXPLORER

IE Version 8.0
Use the following steps to complete the task.

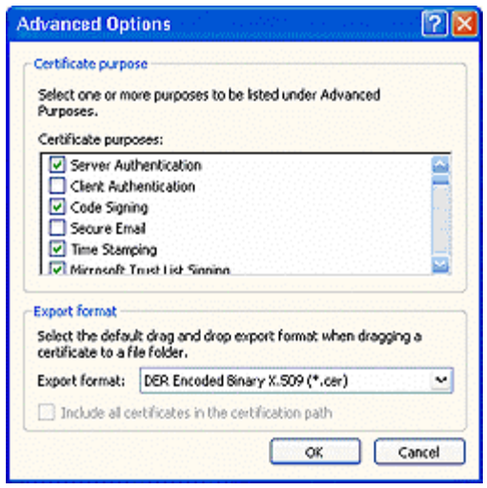
STEP 1: Install Trusted Certificates

To install CAs certificate in the list of trusted certificates:

1. On the **Tools** menu, click **Internet Options**, and then click the **Content** tab.
2. Click **Certificates**.
3. Click following tabbed category for the type of certificates you want to install:
   Trusted Root Certification Authorities. This category includes only self-signed certificates in the root store. When a CA's root certificate is listed in this category, you are trusting content from sites, people, and publishers with credentials issued by the CA.



4. To add other certificates to the list, click **Import**.
   The Certificate Manager Import Wizard takes you through the process of adding a certificate
5. To configure the **Intended Purpose** box, select the filter for the types of certificates to be displayed in the list. Click **Advanced**.



Appendix 2 - PROCEDURE TO DISABLE A CERTIFICATE PROMPT IN FIREFOX

Firefox Version: 3.5
Use the following steps to complete the task.

STEP 1: Install Trusted Certificates

1. Open a Firefox browser.
2. Choose **Options** from the **Tool** menu.
3. Click the **Advanced** button.
4. Select the **Encryption** pane.
5. Click **View Certificates**.
6. Click the **Authorities** tab, at the bottom of the screen, click **Import**.
7. Navigate to the CA certificate and import it.

Appendix 3 – USEFUL COMMANDS

Commands to convert certificate to PKCS12 format using OpenSSL tool:-

If there only one CA certificate present in certificate chain –

openssl pkcs12 -export –out outputPKCS12.pfx -inkey privateKey.key -in identityCertificate.pem -certfile caCert.pem

identityCertificate.pem - Certificate which is signed by third party CA.

privateKey.key – Private key file.

caCert.pem – CA Certificate chain file.

outputPKCS12.pfx – Output PKCS12 store file.

For example - openssl pkcs12 -export -out outputFile.pfx -inkey pk.pem -in cert.pem -certfile CA.pem

```
root >keytool -keystore outputFile.pfx -list -v -storetype PKCS12 -storepass 12345

Keystore type: PKCS12
Keystore provider: BCFIPS

Your keystore contains 1 entry

Alias name: 14907cd4e9835569ca876ba17c5c9a3cad69e341
Creation date: Apr 13, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 3
Certificate[1]:
Owner: C=US, O=AVAYA, CN=TEST CERT
Issuer: CN=Intermediate CA
Serial number: 6fa4eec33cf5b091
Valid from: Thu Apr 13 16:08:08 IST 2017 until: Mon May 14 16:16:16 IST 2018
Certificate fingerprints:
         MD5:  D0:66:E2:A1:C7:FA:22:48:60:5D:37:B9:D6:77:F0:AF
         SHA1: 14:90:7C:D4:E9:83:55:69:CA:87:6B:A1:7C:5C:9A:3C:AD:69:E3:41
         SHA256: 58:4C:08:74:30:50:B3:84:45:8F:F6:17:14:20:03:18:36:52:31:02:FF:B1:8D:28:42:75:14:48:E4:30:4D:CB
         Signature algorithm name: SHA256WITHRSA
         Version: 3
Certificate[2]:
Owner: CN=Intermediate CA
Issuer: O=AVAYA, OU=MGMT, CN=System Manager CA
Serial number: 7f5f1692126024f4
Valid from: Thu Apr 13 16:16:16 IST 2017 until: Mon May 14 16:16:16 IST 2018
Certificate fingerprints:
         MD5:  63:9C:B5:00:A4:DB:EE:A2:CF:B4:26:15:5E:0B:48:53
         SHA1: B7:44:42:D4:FE:B3:36:A2:2C:75:11:4D:4C:A6:8C:B7:AD:C3:9A:BD
         SHA256: 26:09:66:9D:EF:4C:B5:5C:6C:16:BB:09:C3:6D:97:86:43:9F:35:6F:09:DA:32:6A:0A:49:8C:CB:2D:67:C1:2F
         Signature algorithm name: SHA256WITHRSA
         Version: 3
Certificate[3]:
Owner: O=AVAYA, OU=MGMT, CN=System Manager CA
Issuer: O=AVAYA, OU=MGMT, CN=System Manager CA
Serial number: 15bb6f7b3dcddcd6
Valid from: Thu Mar 23 12:38:39 IST 2017 until: Sun Mar 21 12:38:39 IST 2027
Certificate fingerprints:
         MD5:  2A:8D:A7:6F:92:19:31:92:BA:DE:32:59:FC:38:4A:9A
         SHA1: 96:A2:35:F8:E9:61:06:0D:A3:3D:25:22:54:50:38:AE:31:CB:D8:99
         SHA256: B2:DF:D3:16:AF:BE:4C:32:19:F7:89:B2:8C:FC:82:99:7E:C0:A6:4B:C5:33:02:90:FC:67:E0:8C:DA:0C:C9:32
         Signature algorithm name: SHA256WITHRSA
         Version: 3


*******************************************
*******************************************
```

Certificate chain of Identity certificate and CA certificates.