

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

Issue 1.3

November 2017

"THE INFORMATION PROVIDED IN HEREIN IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. This document is intended to provide general information, and is not made part of any agreement you may have with Avaya related to your purchasing and/or licensing of Avaya products or services and related warranty, maintenance and support."

© 2017 Avaya Inc. All rights reserved.

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 | .4 |
|---|----|
| SCOPE | .4 |
| PROCEDURE TO IMPORT THIRD PARTY CERTIFICATES INTO SYSTEM MANAGER | .4 |
| Pre-requisite: | .4 |
| IDENTITY CERTIFICATE ATTRIBUTES | .5 |
| Management Container TLS Service | .5 |
| Section 1: For Primary System Manager or Standalone System Manager | .6 |
| Section 2: For Secondary System Manager | .9 |
| Section 3: For Managed Elements | 12 |
| Appendix 1 - PROCEDURE TO DISABLE A CERTIFICATE PROMPT IN INTERNET EXPLORER | 16 |
| STEP 1: Install Trusted Certificates | 16 |
| Appendix 2 - PROCEDURE TO DISABLE A CERTIFICATE PROMPT IN FIREFOX | 17 |
| STEP 1: Install Trusted Certificates | 17 |
| Appendix 3 – USEFUL COMMANDS | 17 |

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 thirdparty 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.

| 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 | DNS:{system-manager-vfqdn} | required ³ |
| Name | DNS:{system-manager-fqdn} | required |
| Authority Information Access | <pre>OCSP - URI:http://{ocsp-server}{:ocsp- port}{/ocsp-path}</pre> | optional ⁴ |
| CRL Distribution Points | URI:http://{crl-server}{:crl-port}{/crl-path} URI:ldap://{crl-server}{:crl-port}{/crl-dn} | optional ⁴ optional ⁴ |

Management Container TLS Service

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.

| | avaya.com/SINSI/ | | | 👚 🐨 C" 🚺 • image search | 户 俞 | |
|--|---|--|---|--|--|--|
| AYA | Ava | aya Aura® System I | Manager 6.3 | Help : Ab | conclusion of the base of the start is a start is the start is the start is the start of the start is the sta | |
| | Manual Elements (Isourita | er í Manane Flemente | | | Inventory Bone | |
| ventory Hanage Clements Collected Inventory | Identity Certificates | Y / remark crements | | | Help Done | |
| Install and Upgrade Yanagement | | | | | | |
| Manage Serviceability Agents | Identity Certificates | | | | | |
| Inventory Yanagement | Replace Expert Renew | | | Filters 6 | | |
| | | | | | | |
| Synchronization | Service Name | Common Name | Valid To | Espired | Service Description | |
| ynchronization 5 1888 and CallPilot | Service Name | Common Name | Valid Te Sat Nov 29 14:55:00 15T 2014 | Expired | Service Description | |
| ynchronization 5 1888 and CallPilot ynchronization | Service Name IAM SAML Signing JONS | Common Name Lam_stand_stipping joing | Valid Te Sat New 29 14:55:00 15T 2014 Pri New 28 15:52:34 15T 2014 | Expired No No | Service Description IAM SAML Seguine Service JONS Service | |
| ynchronization 5 1888 and Califilot ynchronization | Service Name IAM SAML Signing JONS IAM Dutubase | Common Name Lam_Land_signing joing Lam_db | Valid Te Sat Nov 29 14:55:09 15T 2014 Fm Nov 28 15:52:34 15T 2014 Fm Nov 28 15:52:33 15T 2014 | Engined Pio Pio Pio | Service Descriptio IAM GAML Seguin Service JONS Service IAM Database Service | |
| ynchronication 5 1889 and CallPilot ynchronication | Service Name IAM SAML Signing JONS IAM Dutabase Apache Load Balancer | Common Name Ism_saml_stipping jong Ism_db spathe_load_balancer | Valid To: Sat Nov 29 14:55:00 IST 2014 Pri Hov 20 15:52:34 IST 2014 Pri Hov 20 15:52:33 IST 2014 Pri Hov 20 15:52:34 IST 2014 | Expired No No No | Service Description IAM SANL, Signin Service JONS Service IAM Database Service Apathe Land Apathe Land | |
| ynchronication 5 1889 and CallPilot ynchronication | Service Name IAM SAML Signing JONS IAM Dutabase Apsche Load Balancer IAM LDAP | Common Name Ian_saml_sipping jons Ian_db apache_load_balancer Ian_dbp | Valid To Sat Nov 29 14:55:09 157 2014 Pri: Nov 20 15:52:34 157 2014 Pri: Nov 20 15:52:33 157 2014 Pri: Nov 20 15:52:24 157 2014 Pri: Nov 20 15:52:52 157 2014 | Taylord No No No No | Service Decorption IAM SAML Supan Service JONS Service IAM Database Service Apathe Said Balancer Service IAM LOAP Service | |
| ynchronization 5 1980 and CallPilot ynchronization | Service Name JAM SAML Signing JONS JAM Database Apache Load Balancer JAM LDAP WEELM Legacy | Common Hame iam_saml_signing jone iam_dh apache_load_balancar iam_ldap whim_lapacy | Valid To: Sat New 29 14:55:09 IST 2014 Fin New 29 15:52:14 IST 2014 Fin New 20 15:52:13 IST 2014 Fin New 20 15:52:03 IST 2014 | Expired Dia Dia Dia Dia Dia Dia Dia | Service Decorption IAM SAML Supan Service JONS Service IAM Database Service Apache Load Balancer Service IAM LOAD Servic WEBLM Leptop Service | |
| ynchronization 5 1889 and CallPilot ynchronization | Service Name IAM SAML Signing JONS IAM Database Apsche Lead Balancer IAM LDAP WEBLM Legecy JONA | Common Hame ian_sami_signing jons ian_db apache_lead_belancer ian_ldap webin_leasey yens | Value To: Sat Nov. 29.14:55:00.157.2014 Pin Hov. 20.15:52:24.187.2014 Pin Hov. 20.15:52:33.187.2014 Pin Hov. 20.15:52:34.167.2014 Pin Hov. 20.15:52:34.167.2014 Pin Hov. 20.15:52:35.187.2014 Pin Hov. 20.15:52:31.187.2014 Pin Hov. 20.15:52:31.187.2013 Pin Hov. 20.15:52:31.24.107.2013 | Taylord Pic Pic Pic Pic Pic Pic Pic | Service Description IAM SANA Septim Service JOHS Service IAM Database Service Service IAM DAP Service IAM LDAP Service WELLM Logect Service JOHA Service | |
| ynchronization 5 1889 and CallPilot ynchronization | Service Name IAM SAML Signing JONS JONS And Dutabase Apsche Lood Balancer JAM LUAAP WEBLM Loper; JONS DOSE DIE | Common Human iam_saml_signing jone iam_dh apache_load_balancar iam_ldap webim_lapacy jone dra | Valid To Sat Nov 29 14:55:08 IST 2014 Pri Hov 20 15:52:24 IST 2014 Pri Hov 20 15:52:34 IST 2014 Pri Hov 20 15:52:34 IST 2014 Pri Hov 20 15:52:32 IST 2014 The Hov 20 15:52:41 IST 2014 Pri Hov 20 15:52:41 IST 2014 | Tapired No No No No No No No No | Service Decorption IAnt Status Service JOHS Benice IAN Database Aparthe Lind Balance Service IAN LDAP Service VEDLU Legecy Service JOHA Barvice Used for DSE | |
| ynchronization 5 1889 and CallPilot ynchronization | Service Name IAM SAML Signing JOHS AM Database Apsche Lasd Balancer IAM LDAP WEBLM Legecy DOHA DOHE Management | Common Hame iam_saml_signing jons iam_db apacha_laad_balancer iam_ldap webim_lagecy jons das mgmt | Value To: Sat Nov 29 14:55:00 15T 2014 Pri Nov 20 15:52:10 15T 2014 Pri Nov 20 15:52:23 15T 2014 Pri Nov 20 15:52:24 10T 2014 Pri Nov 20 15:52:21 10T 2014 Pri Nov 20 15:52:21 10T 2014 Pri Nov 20 15:52:21 10T 2014 | Tapaired Pio Pio Pio Pio Pio Pio Pio Pio Pio Pio | Service Decorption IAM SAMIN Samice JOHS Service IAM Database Samice IAM LOAP Service IAM LOAP Service JOHA Service JOHA Service Used for DSE Management Service | |
| ynchronization 5 1809 and Calibiot ynchronization | Service Name IAM SAML Signing JONS IAM Database Apsche Load Balancer IAM LDAP WEBLM Legety JONA DISE Mexeponent IAM SAML | Common Name ian_iand_signing jone ian_db apacha_losd_belancer ian_idap weblm_iapacy jone dra mpont ian_sand_brops | Value To: Sat Nov. 29 14:55:00 IST 2014 Fin Hov. 20 15:52:14 IST 2014 Fin Hov. 20 15:52:13 IST 2014 Fin Hov. 20 15:52:23 IST 2014 | Taylord Pic Pic Pic Pic Pic Pic Pic Pic Pic Pic | Service Description IAM Software Service JONES Service IAM Database Sarvice Sarvice IAM LDAP Service USAN LDAP Service JONA Service Usan für DBE Management Service IAM SARL Service | |
| iyechronization 5 1800 and Califolat iyechronization | Servic Name IAM SAM, Signing JONS IAM Database Apsche Load Balancer IAM DAtabase MERLINAP WEBLM Legery JORA DISE Management SPERT | Common Hame ian_sami_siquing jone ian_db apache_bed_belancer ian_ldap webin_legacy gens dra transmither apack apach | Value To: Sat Nov. 29 14:55:00 187 2014 Fin Hov. 20 15:52:24 187 2014 Fin Hov. 20 15:52:24 187 2014 Fin Hov. 20 15:52:23 187 2014 Fin Hov. 20 15:52:23 187 2014 Thus Hov. 20 15:52:23 187 2014 Thus Hov. 20 15:52:23 187 2013 Fin Hov. 20 15:52:23 187 2014 Fin Hov. 20 15:52:23 1187 2014 | Tapaired Pic Pic Pic Pic Pic Pic Pic Pic Pic Pic | Service Decopter IAM SAMI, Septing Service JONS Service IAM Detabase Apache Sanice Ravice Ravice Value Service Used for DBE Donaf Service Used for DBE Mangement Service IAM SAMI, Service SAMI, Service | |

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.

| https://westvict.platfor | m.avaya.com/SHGR/ | | 🖙 🐨 C 🚺 🛃 - inage search | ₽ 會 |
|---|---|---|---|--|
| AVAYA | Avaya Aura ^e System Mana | ger 6.3 | Help / About - Change Pas | resed : Log off ade |
| | None / Flements / Investory / Non-on Flements | | Inve | entory * Home |
| Manage Demente Collected Inventory | Trusted Certificates | | | Help Done |
| Hanagement | Trusted Certificates | | | |
| Agents Inventory | (View Add Expan) (Rammer) | | | |
| Agents † Inventory Management | (Ves Add Esper) (Rumme) 15 Dame Refresh | | | filter: Enable |
| Agents i Inventory Management i Synchronization | (Ves Add Esper) (Rumme) 15 Demo Refresh | Store Type | Subject Name | Filteri Enable |
| Agents Deventory Nanagement Synchronization Synchronization | Stars Refresh Used for validating TLB cleant identity certificates Used for validating TLB cleant identity certificates | Stars Type TM_DH-GUHD_TLS TM_DH8-GUHD_TLS | Subject Name Crimédiauls, OLI=MONT, O+AVAVA OLI=MONT, Crimes I um 7,plations, avapa.com, C=CA, L=BVH O+AVAVA | Filteri Enable |
| Agents Inventory Hanagement Synchronization C5100 and CalPilot Synchronization | Media Expansition 15 Berne 35 Berne State Bescription Used for validating TLB cleant identity contificates Used for validating TLB cleant identity contificates Used for validating TLB cleant identity contificates Used for validating TLB cleant identity contificates Used for validating TLB cleant identity contificates Used for validating TLB cleant identity contificates | Store Type TM_DH&OUND_TLS TM_DH&OUND_TLS TM_DH&OUND_TLS TM_DH&OUND_TLS TM_DH&OUND_TLS | Solipeit Name Chridefault, OUHROMT, OHAVAYA OUHROMT, Chrimes I um 7 gleffinn, svays com, CHCA, LHEVH OHAVAYA OHAVAYA, OUHROMT, Chridefault ChHEISOP CA, OUHRAYso Global Brovices, OUHClass 2 Mana Solicities CA, OUHRAYso do Sela Directory, Christian Solicities CA, OUHRAYSO DO Constant, Carl | Filter: Enable ST+OR, ped PKI Individual pe (c)06; |
| Agents Inventory Hanagement Synchronization CS 1999 and CaBPilot Synchronization | User Expansity Frances 15 Diama Rafresh 5 Stare Description | Sterr Type TM_DR&OURD_TLS TM_DR&OURD_TLS TM_DR&OURD_TLS TM_DR&OURD_TLS TM_DR&OURD_TLS TM_OUTBOURD_TLS TM_OUTBOURD_TLS TM_OUTBOURD_TLS | Sobject Name CH-default, OU-MOMT, O+AVAVA OU-MOMT, Chimess I vin T, platform, svays.com, C=CA, L=BVH O+AVAVA O=AVAVA, OU-MOMT, CH-default Chief EDP CA, OU-MOMT, CH-default Chief EDP CA, OU-MOMT, O+Avays, TeC, CHIS Chief Subscriber CA, OC-globalt, DC=vavys, DC=com Chief fault, OU-MOMT, O+AVAVA OU-MOMT, CHimess I vin T, platform, svays, com, C=CA, L=BVH OU-MOMT, CHimess I vin T, platform, svays, com, C=CA, L=BVH | Filter: Enable . ST=OR. ped PKI Induidual pe (c)06. . ST=OR. |
| Agents Agents Agents Supervised Synchronization C5 1000 and Califyiot Synchronization | Used Example 15 Dama Rafnesh 15 States Decodynamic 10 Used for validationy TLB client identity certificates 11 Used for validationy TLB client identity certificates 12 Used for validationy TLB client identity certificates 13 Used for validationy TLB client identity certificates 14 Used for validationy TLB client identity certificates 15 Used for validationy TLB client identity certificates 15 Used for validationy TLB client identity certificates 15 Used for validationy TLB client identity certificates 16 Used for validationy TLB client identity certificates 17 Used for validationy TLB client identity certificates 16 Used for validationy TLB server identity certificates 17 Used for validationy TLB server identity certificates 17 Used for validationy TLB server identity certificates | Sters Type TM_DHOUND_TLS TM_DHOUND_TLS TM_DHOUND_TLS TM_DHOUND_TLS TM_DHOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS TM_OUTBOUND_TLS | Soldjant Name Chindefault, OUHMONT, OHAVAVA OUHMONT, Chimasa I van Jalatferm, avaya.com, CHCA, LHEVH OHAVAVA OHAVAVA, OUHMONT, Chindefault Chindefault, SoldHarms of use at https://www.ventigh.dem/ OUHMAVAYATCLERCA, DC-glabab, DC-avaya, IAC, CHS ChindevayaTtclearCA, DC-glabab, DC-avaya, IAC, CHS ChindevayaTtclearCA, DC-glabab, DC-avaya, DC-cean Chindefault, Collearos I van Jalatferm, avaya.com, CHCA, LHEVH OHAVAVA, OUHMONT, Chindefault OHAVAVA, OUHMONT, Chindefault | Filter: Enable ST+OH, ged DKI Individual ps (c)06, ST=OH, |
| Agents Agents Agents Accounts | Used for validating TLS client identity certificates Used for validating TLS every identity certificates | Sten Type TM_DRECURD_TLS TM_DRECURD_TLS TM_DRECURD_TLS TM_DRECURD_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS TM_OUTEOUND_TLS | Subject Name Chi-default, OU-MOMT, OHAVAVA OU-MOMT, Chimas I van Zelafism, svaga.com, CHCA, LHEVIH OHAVAVA OHAVAVA OHAVAVA OHAVAVA, OU-MOMT, Chindefault Chielsop CA, OU-Mayaya dolah Bervitasi, OU-Class 2 Mana- Subarchar CA, OU-Moms I van Zelafishi, DCHavaya, Icen, CHI OHAVAVA, OU-MOMT, OHAVAVA OU-MOMT, Chimas I van Zelafishi, DCHavaya, Com, CHCA, LHEVIH OHAVAVA, OU-MOMT, OHAVAVA OHAVAVA, OU-MOMT, OHAVAVA OHAVAVA, OU-MOMT, Chindefault OHAVAVA, OU-MOMT, Chindefault OHAVAVA, OU-MOMT, Chindefault OHAVAVA, OU-MOMT, Chindefault OHAVAVA, OU-MOMT, Chindefault Chielsop CA, OU-Mayas dolah Servicas, OU-Class 2 Mana- Isbaschar CA, OU-Mars di sa arthtpa//www.veriagin.com/ OU-Varisity Therash, OH | Filter: Enable ST+OH, ged DKI Endividual ge (c)06, ST+OH, ged PKI Endividual ge (c)06, |

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 CLI, 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 CLI, execute the below as a **root user** #service jboss restart

Restart SystemMonitor

12. From Secondary System Manager CLI, 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:
 - o 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

 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 CLI, 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

 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/spirittrust.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

 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/spirittrust.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.

| Certificates | | | ? 🔀 |
|---|--|---|--|
| Intended purpose: | <all></all> | | ~ |
| Intermediate Certifical | tion Authorities Trusted Root Ce | ertification Auth | norities Trusted Publ < > |
| Issued To | Issued By | Expiratio | Friendly Name 🛛 🔼 |
| AAA Certificate : ABA.ECOM Root AddTrust Extern America Online F Autoridad Certifi Autoridad Certifi Avaya Trusted A Baltimore EZ by I | Ser AAA Certificate Services CA ABA.ECOM Root CA Ial AddTrust External CA too America Online Root ca Autoridad Certificador ca Autoridad Certificador vava Trusted Authe AvayaITrootCA DST Baltimore EZ by DST | 1/1/2029 7/9/2009 5/30/2020 11/20/2037 6/29/2009 6/30/2009 10/4/2016 7/22/2039 7/4/2009 | COMODO DST (ABA.ECOM USERTrust America Online R Autoridad Certifi Autoridad Certifi <none> <none> DST (Baltimore E</none></none> |
| | ort <u>R</u> emove | | Advanced |
| Certificate intended p | urposes | | View |
| | | | |

- 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**.

| Certificate purpo | se | |
|--|--|---------|
| Select one or mo Purposes. | ore purposes to be listed under Advanced | |
| Certificate purpo | oses: | |
| Server Aut | hentication | |
| Clerk Auth | entication | |
| Code Signi | ng | Sec. 3. |
| Secure Em | al | |
| V Time Starro | ina | |
| Mirrosoft T | nust List Sinning | |
| Export format Select the defau certificate to a fr | it drag and drop export format when drag le folder. | ging a |
| Export format: | DER Encoded Sinary X.509 (*.cer) | ~ |
| | | |

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

