Certificate Management for Avaya Aura® System Manager 7.1.x and 8.0.x

Release 7.1.x/8.0.x
Issue 4
September 2020

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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of 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.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN Avaya HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo under the link "Avaya Terms of Use for Hosted Services" or such successor site as designated by Avaya, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" or such successor site as designated by Avaya, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN

AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in Section M(i)1 or 2 as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "**Software**" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "**Designated Processor**" means a single stand-alone computing device. "**Server**" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "**Instance**" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("**VM**") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open

source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya

Support website: http://support.avaya.com, or
such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are

handled per the Avaya Product Security Support Flow

(https://support.avaya.com/css/P8/documents/100161515) .

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of
their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

Overview

This document covers the certificate management functionality for System Manager 7.1.x and 8.0.x releases. This functionality includes the ability to:

- View installed Trusted and Identity Certificates on the System Manager server.
- Add or remove Trusted Certificates on the System Manager server.
- Replace or renew Identity Certificates on the System Manager server signed by System Manager CA.
- Replace Identity Certificates on the System Manager server signed by a third-party CA.

Before attempting to make Certificate changes in System Manager, it is highly recommended to get a solution level view to understand which network elements will be affected. This will require planning and network audits before deploying new certificates.

System Manager uses five Identity Certificates for TLS connections: Management Container TLS Service, SAL Agent, DataStore Service, Postgres Access, and WebLM. Any changes to these certificates can cause major service interruptions. Be very careful when changing these certificates. Each side presents its Identity Certificate during a TLS handshake before the communication starts. If one side does not trust the signer of the Identity Certificate of the other side, the connection fails. For an entity to trust another certificate, the entity must possess the root CA certificate from the CA that issued the Identity Certificate. The root CA certificate must be stored in the entity's trusted list, also known as a Trust Store.

In case the certificate for a given service is to be replaced with a certificate signed by a 3rd party CA. The Trust Store of all the entities that interact with the given service should be updated before the identity certificate is replaced.

High level procedure to replace Identity Certificates

This section describes the high-level steps and prerequisites to replace Identity Certificates on System Manager. Subsequent sections provide the details of each step.

1. In case the System is part of a Geo-R pair disable replication:
    a. Login to **Primary** System Manager UI
    b. Browse to Services Geographic Redundancy
    c. Click on the **Disable Replication** Button.
2. Take a snapshot of the System Manager VM. In case of a Geo-R setup take a snapshot of both Primary and Secondary System Manager.
3. Add the external CA certificate including all the intermediate/Sub CA certificates and the root CA certificate to All System Manager trusted stores except USER_CERT_BASED_LOGIN_TLS store.
4. Add the external CA certificate including all the intermediate/Sub CA certificates and the root CA certificate to all elements/devices that interact with System Manager using TLS. E.g. Session Manager, Avaya Breeze, Geo-R System Manager peer etc.

Note: Any delay/failure in adding the trusted certificate might result in communication failure and disruptions. Make sure that all the elements are updated with the trusted certificates appropriately and service restarts (if any required) is complete before continuing to the next step.

5. Optional step, to be carried out if CRL/BOTH is set as the Revocation Type at Services → Security → Configuration → Security Configuration on System Manager Web Console: Schedule a CRL download job from the external CA CRL distribution point. Refer section *Configuring CRL download from external Distribution Point* for instructions.
6. Replace the identity certificates using one of the two options, as in section: *Replacing an Identify Certificate by a third party CA issued certificate*. For a standby System Manager these steps need to be carried out on the active peer System Manager.

   Important:

   a. The externally signed certificate must have the appropriate attributes for a given service as mentioned in *Identity Certificate attributes*.

   b. In case the identity certificate is being replaced for multiple services it is recommended to replace the **Management Container TLS Service** last as replacing this certificate would require an immediate restart of services for proper functionality.
7. Restart the following services by logging on to the System Manager CLI for which certificates have been replaced.
   a. Jboss service

      $> sudo service jboss restart
   b. Spirit Agent

      $> sudo service spiritAgent restart
   c. System Monitor

      $> sudo service systemMonitor restart

   It would take 12-15 minutes for the System Manager GUI to come up fully. Once the GUI is up, proceed with further steps, if required.

8. In case the System is part of a Geo-R pair enable replication
   a. Login to **Primary** System Manager UI
   b. Browse to Services → Geographic Redundancy
   c. Click on the **Enable Replication** Button.
9. After making sure that all certificates and relevant truststores of System Manager and interacting elements are updated and confirmed to be working as expected the snapshots taken in step #2 can be removed.

Trusted Certificates

Overview

System Manager supports adding, removing, viewing and exporting trusted certificates using System Manager Web console. All these actions can be carried out for Primary active and Secondary System Manager (in case of a Geo-R setup) from the Web console of Primary System Manager.

Multiple Trust Stores exist on System Manager. Each Trust Store contains a set of CA certificates that are trusted by a given service. The following table describes them

Store type	Purpose	Protocol	Note
TM_INBOUND_TLS	Used for validating client certificates during inbound connections to System Manager application server.	HTTPS, JMX, RMI	
TM_OUTBOUND_TLS	Used for validating identity certificates during all outbound connections from System Manager application server	SIP	
TM_INBOUND_TLS_PEM	Used as trusted store for all geo replication(postgres streaming replication) and datastore services(postgres and OpenLDAP) in System Manager	LDAPS, Postgres,csync2	
USER_CERT_BASED_LOGIN_TLS	Used for validating client certificates during certificate based login to System Manager	HTTPS	Only certificates of CAs which issue client certificate for CAC/ smart card devices to be used for System Manager web UI authentication should be added to this store.

Viewing trusted CA certificates

Procedure

1. On the home page of the Primary System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance.
3. Click **More Actions > Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the certificate and the store type it resides and click **View**.

The View Trust Certificate page displays the details of the selected certificate.

Adding trusted CA certificates

About this task

You can import a trusted certificate:

- From a file.
- By copying the contents of a PEM file.
- From a list of an existing certificates.
- From a remote location using a TLS connection (available only on systems with regular hardening).

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance.
3. Click **More Actions > Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. Select the Store Type to add trusted certificate. Use All to add to all truststores
6. Depending on the certificate file format/certificate retrieval method use one of the below steps:

➢ To import a certificate from a file:
- Click **Import from file**.
- Click **Browse** and locate the file.
- Click **Retrieve Certificate**.
- Click **Commit**.

➢ To import a certificate in the PEM format:
- Select **Import as PEM Certificate**.
- Locate the PEM certificate.
- Open the certificate using Notepad.
- Copy the entire contents of the file. You must include the start and end tags:
  - `-----BEGIN CERTIFICATE-----" and "----- END CERTIFICATE----`.
- Paste the contents of the file in the box provided at the bottom of the page.
- Click **Commit**.

➢ To import certificates from existing certificates:
- Click **Import from existing**.
- Select the certificate from the Global Trusted Certificate section.
- Click **Commit**.

➢ To import certificates using TLS (available only on systems with standard hardening):
- Click **Import using TLS**.
- Enter the IP Address of the location in the **IP Address** field.

- Enter the port of the location in the **Port** field.
- Click **Retrieve Certificate**.
- Click **Commit**.

Removing trusted CA certificates

Note: The System Manager CA certificate must not be removed from the trust store before ensuring that System Manager itself and all elements interacting with System Manager are using an external CA issued identity certificate.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance.
3. Click **More Actions > Configure Trusted Certificates**.
4. Select the certificates you want to remove, then click **Remove**.

The system removes the certificates from the list of trusted certificates on the System Manager.

Exporting a System Manager Certificate

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the appropriate certificate to export.
5. Click **Export**.

Identity Certificates

Overview

System Manager Identity Certificates can be viewed, renewed and replaced from System Manager Web console. All these actions can be carried out for Primary active and Secondary System Manager (in case of a Geo-R setup) from the Web console of Primary System Manager.

Below is a table containing details about different System Manager Identity certificates and their usages:

Service name	To/from	Protocol	Port	Support 2048 key length and SHA2 signature	Note
SPIRIT	Connection between the Serviceability Agent and System Manager HTTPS port.	HTTPS	Ephemeral port connecting to System Manager port 443	Yes	This certificate is used for internal, within System Manager, connections
Management Container TLS Service	System Manager Web UI access. Connection between elements and System Manager for management	HTTPS, JMX, RMI	Port 443 Port 3873 Port 9000 Port 1391 Port 10636 Ephemeral port connecting to elements and 3rd party devices for management	Yes	The Certificate is used by System Manager application server for all inbound TLS ports(except WebLM port 52233) and all outbound connections
DataStore Service	For all geo replication (postgres streaming replication) and datastore services(postgres and OpenLDAP) in System Manager From CS1k for openLDAP.	LDAPS	Port 5432 Port 636 Port 30865 Ephemeral ports connecting to peer System Manager ports for geo replication.	Yes	
Postgres Access	For super user access to postgres database during maintenance activities	TLS	Ephemeral ports connecting to port 5432 for Database access	Yes	This certificate is used for internal, within System Manager, connections
WebLM	Connections to WebLM port for Licensing.	HTTPS	Port 52233	Yes	In case the System Manager has been upgraded from an earlier release (7.0.x and before) this port has a demo certificate.

Identity Certificate attributes

The certificate attributes for the identity certificates of various services in System Manager is mentioned in the tables 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}`[6]	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}`[6] `DNS:{system-manager-fqdn}`[6]	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}`	optional[4] optional[4]

DataStore Service

Attribute	Value	Required?
Subject	`CN={system-manager-fqdn}`[6]	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}[6] DNS:{system-manager-ip}	required[3] optional[5]
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]

WebLM

Attribute	Value	Required?
Subject	CN={system-manager-fqdn}[6]	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-fqdn}[6]	optional
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]

SPIRIT

Attribute	Value	Required?
Subject	`CN={system-manager-fqdn}`[6]	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-clientAuth = 1.3.6.1.5.5.7.3.3.2`	required
Subject Alternative Name	`DNS: {system-manager-fqdn}`[6]	optional
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]

Postgres Access

Attribute	Value	Required?
Subject	`CN=MGMTDB`[7]	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-clientAuth = 1.3.6.1.5.5.7.3.3.2	required
Subject Alternative Name		Not 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.avaya.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. Authority Information Access or CRL distribution point might be required based on the certificate revocation checking behavior of System Manager itself and other elements interacting over TLS. For viewing/changing System Manager Revocation checking behavior browse to **Services → Security → Configuration → Security Configuration** on System Manager Web UI.

5. CS1k devices connect to System Manager LDAPS port using the IP address. So, in case System Manager is being used to manage CS1k the IP address must be added in the SAN field.

6. {system-manager-fqdn} and {system-manager-vfqdn} should be case-sensitive and should have the exact same case as the FQDN and VFQDN value of the system respectively.

7. MGMTDB is a fixed/constant value in all upper-case.

Viewing Identity Certificates

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance.
3. Click **More Actions** > **Configure Identity Certificates**.

4. Select the specific service to view the certificate.

Replacing an Identify Certificate by a third-party CA issued certificate

Use one of the below procedures to replace an Identity Certificate of a System Manager by one signed by a third-party CA. A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise -run CA that is maintained by the IT department.

Important:

- Add the third-party CA certificate including all the intermediate/Sub CA certificates and the root CA certificate on all devices/elements that interact with System Manager before carrying out the below steps. Failure to do so would result in loss of communication with the devices and service outages.

Using a PKCS#12 format store (available only in standard hardening mode)

Before you begin

Make sure you have the following:

- An identity certificate in a PKCS#12 format store.
- The attributes in the certificate must be in accordance with the section: *Identity Certificate attributes*
- **The certificate keystore file must have only one entry, that of type PrivateKeyEntry that has the private key and the identity certificate with all the intermediate/Sub CA and root CA certificate in the chain of trust.**

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the Identity Certificates page, select the specific service
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Import third party certificate**.
7. Select the Certificate File Format as **PKCS#12**
8. Click on the **Choose File** button to browse and select the PKCS#12 store file.
9. Enter the password in the **Password** field.
10. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
11. Click **Commit**.

Using a Certificate Signing Request

Notes

- Part 1 of this procedure generates a new and unique CSR and corresponding private key every time it is carried out. Only the certificate generated from the latest generated CSR could be used to carry out the second part of this procedure.
- The generated private key is stored in a secure manner on the product and it can't be exported.
- As of today SMGR only supports the CN (Common Name) attribute in the CSR it generates. System Manager for its functionality only requires the CN attribute in its identity certificates (and it should have a value as per the "Identity Certificate attributes") . Rest of the DN attributes are optional. If someone wants to specify additional attributes in the DN it should be added while signing the CSR

Procedure part 1: Generating a Certificate Signing Request (CSR)

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the Identity Certificates page, select the specific service
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Generate Certificate Signing Request (CSR) for third party certificate**.
7. Select the **Common Name (CN)** check box and enter the value if a change is required. System pre-populates the value from the existing certificate CN value. Choose this value in accordance with the value in section: *Identity Certificate attributes* for the specific service.
8. Select **RSA** for the **Key Algorithm**.
9. Select **2048** as the **Key Size**.
10. For **Subject Alternative Name,** select the **DNS Name** or **IP Address** or **URI** or **id-on-xmppAddr** check box to add/edit a value. Otherwise, the system pre-populates the value from the existing certificate. Choose these values in accordance with the value in section: *Identity Certificate attributes* for the specific service
11. Click **Generate CSR**.
12. Using the CSR generate an identity certificate from the external certificate authority. Make sure that the Subject Alternate names field as present in the CSR is not over-written while generating the certificate.

Procedure part 2: Importing external CA signed certificate

Before you begin

Make sure you have the following:

- An identity certificate signed by an external CA using the CSR generated in the earlier step. The option to import a certificate file in PEM format, as in step #7 below, is only available once a CSR has been generated.
- The attributes in the certificate must be in accordance with the section: *Identity Certificate attributes*
- **The certificate file must have the identity certificate and all the intermediate/Sub CA and root CA certificate in the chain of trust**.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select either Primary or Secondary System Manager Instance from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the Identity Certificates page, select the specific service
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Import third party certificate**.
7. Select the Certificate File Format as **PEM.**
8. Click on the **Choose File** button to browse and select the certificate file.
9. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
10. Click **Commit**.

Replacing an Identify Certificate by a System Manager CA issued certificate

Use this procedure to replace an Identity Certificate of System Manager by one signed by the System Manager CA

Important:

In case the WebLM demo certificate is being replaced with a System Manager CA signed certificate, before doing the below steps add the System Manager CA certificate (the whole chain of CA certificates in case System Manager is a Sub CA to another CA) to the truststore of all elements/devices connecting to System Manager for licensing. Failure to do so would result in the loss of communication with the devices and service outages.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory > Manage Elements**.
2. Select the System Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the Identity Certificates page, select the specific service
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Replace this Certificate with Internal CA Signed Certificate**.
7. Select the **Common Name (CN)** check box and enter the value if a change is required. System pre-populates the value from the existing certificate CN value. Choose this value in accordance with the value in section: *Identity Certificate attributes* for the specific service
8. Select **RSA** for the **Key Algorithm**.
9. Select **2048** as the **Key Size**.
10. For **Subject Alternative Name,** select the **DNS Name** or **IP Address** or **URI** or **id-on-xmppAddr** check box to add/edit a value. Otherwise, the system pre-populates the value from the existing certificate. Choose these values in accordance with the value in section: *Identity Certificate attributes* for the specific service.
11. Click **Commit**.

Demo certificates

System Manager WebLM port used for licensing can have a demo certificate if the System has been upgraded from release 7.0.x and earlier. Demo certificates are non-unique identity certificates issued by the Avaya SIP Product Certificate Authority. Demo certificates are very insecure and do not meet current NIST standards (SHA256 and 2048-bit keys). It is recommended to not use demo certificates in the deployment.

Check for Demo Certificate

Determine if you are using a demo identity certificate.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select either Primary or Secondary System Manager Instances.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select WebLM.
5. Check the **Issuer Name**.

If the **Issuer Name** field contains **CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US**, you have a demo identity certificate.

Replace Demo Certificate

Replace the demo certificate with a System Manager CA or 3rd party CA issued Identity certificate

Procedure

1. Import the CA certificate, and any other root CA/Intermediate CA certificates in the chain of trust to the trust stores of all devices/elements connecting to System Manager Port 52233 for licensing. Refer the element/device documentation to find exact steps to do this.

   Note: Any delay/failure in adding the trusted certificate might result in communication failure and disruptions. Make sure that all the elements are updated with the trusted certificates appropriately and service restarts (in any required) is complete before continuing to the next step.

2. Refer *Replacing an Identify Certificate by a third party CA issued certificate* or *Replacing an Identify Certificate by a System Manager CA issued certificate* as required to replace the certificate for service **WebLM**.
3. Restart the Jboss service for changes to take effect. On System Manager CLI execute the command:
   $> sudo service jboss restart

Installing Demo Certificate

This procedure reinstalls demo certificates to quickly restore a previously working environment.

About this task

Important:

Avaya does not recommend installing demo certificates. Demo certificates are not secure. Use the System Manager CA or 3rd party CA issued certificate.

Procedure

1. Log in to the System Manager server using the customer login.
2. Enter the command `toggleWeblmOldcert` to install the demo certificates for WebLM port 52233.
3. Restart the Jboss service for changes to take effect. On System Manager CLI execute the following command:

   $> sudo service jboss restart

Identity Certificates lifecycle

Validity

System Manager CA, by default, issues identity certificates that are valid for 39 months from the time of creation.

For an external CA signed certificate, the validity would depend upon the configuration on the Certificate authority signing the given certificate.

Raising alarms when certificates reach expiration date

Alarms are raised daily in case a System Manager Identity certificate is about to expire within a given threshold number of days. The default threshold value is 60 days. For viewing/modifying this value browse to **Services** → **Configurations** → **Settings** → **SMGR** → **Trust Management** on System Manager Web console.

Auto-renewal of certificates

In case a System Manager Identity certificate signed by the default System Manager CA is about to expire within a given threshold number of days it is automatically renewed with a new certificate valid of 39 months. All the certificate attributes are retained. The default threshold value is 30 days. For viewing/modifying this value browse to **Services** → **Configurations** → **Settings** → **SMGR** → **Trust Management** on System Manager Web console.

Note: External CA signed certificates won't get auto-renewed in case the remaining validity is less than the threshold value. System Manager Administrator must make sure to check the alarms generated in case the certificates near expiry and manually replace them with new certificates with extended validity.

Certificate Revocation Management

Configuring revocation checking behavior

System Manager carries out certificate revocation checking based on the System Configuration. For viewing/changing System Manager Revocation checking behavior refer to the **Revocation Configuration** section by browsing to the **Global** tab on **Services** → **Security** → **Configuration** → **Security Configuration** on System Manager Web UI.

Any configuration change on this page requires a System Manager Application server restart. A System Manager Application server restart is automatically triggered on committing any change to this configuration.

Revocation Configuration field descriptions

Certificate Revocation Validation

BEST_EFFORT: Revocation checking is done but if due to some network limitation/failures/glitch the validation can't be completed the connection is allowed.

MANDATORY: Revocation checking is done and if due to some network limitation/failures/glitch the validation can't be completed the connection is aborted.

NONE: Certificates are not checked for revocation. If NONE is chosen all other configurations are disabled.

Revocation Type

OCSP: Use Online Certificate Status Protocol (OCSP) as the method of revocation checking.

CRL: Certificate revocation list (CRL) as the method for revocation checking

BOTH: Use both OCSP and CRL for validation checking.

Revocation Type Preference

Only of significance if Revocation Type is set to BOTH

CRL: Prefer CRL for getting revocation information. Fallback to OCSP, only if CRL can't be obtained

OCSP: Prefer OCSP for getting revocation information. Fallback to CRL, only if revocation information isn't obtained using OCSP.

Check method

ONLY_END_ENTITY: Check only the end entity certificate for revocation.

CERT_CHAIN: Check the end entity certificate and all the intermediate CA certificates in the chain for revocation.

External links to read about revocation checking

https://en.wikipedia.org/wiki/Certificate_revocation_list

https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

Configuring CRL download from external Distribution Point

When a system is configured to use CRL or Both (CRL and OCSP) as the revocation checking mechanism; CRL download jobs can be configured to periodically download CRLs from external Distribution points. It is recommended to configure periodic download jobs at frequency equal to CRL publishing frequency at the distribution point or once per day, whichever is lesser for all the CAs in the ecosystem. This would include CRL distribution points for all certificates that Aura elements interact with. This helps reduce additional communication over the network while establishing a TLS session.

Procedure

1. On System Manager Web Console browse to
   Home / Services / Security / Configuration / CRL Download

2. Click on the **Add** button
3. Provide a **Job Name** and set the **Job Frequency**
4. Provide the **CRL distribution Point** like: `http://{crl-server}{:crl-port}{/crl-path}`
5. To download multiple CRLs in the same job click on **Add** button to provide another **CRL distribution Point**
6. Click on **Commit** button to schedule the job**.**

IP/FQDN change on System with 3rd party Identity Certificate

System Manager uses certificate subject CN field, which is equal to the FQDN value, for identity validation. Also, the DataStore service certificate might have the IP address (required if System Manager is managing CS1k) of the System in the SAN field. So, in case a system has 3rd party certificates installed, IP/FQDN change is not allowed till new certificates, with the future IP/FQDN value, are installed. As. this would cause connectivity issues and service outages.

Follow one of the below two set of steps to change the IP/FQDN of a system which has 3rd party certificates installed. Only one of the below two set of steps should be used:

Note: Make sure that once you start on the procedure all the suggested steps are completed. Do not stop/leave in the middle; this may result in service outages.

By replacing current certificates with System Manager CA issued certificates

Note: Follow these steps only if System Manager CA certificate is already installed in all the trust stores of System Manager. Otherwise follow the set of steps in the next section. Refer the FAQ section for steps to check if System Manager CA certificate is already installed.

1. Take a snapshot of the System Manager VM.
2. Replace certificates for services which have 3rd party certificates installed and contain the FQDN and/or IP (whichever is being changed) in the Subject CN and/or Subject Alternate Name field with System Manager CA issued certificate. The replaced certificate should have the existing (current system) IP/FQDN in the Subject CN or Subject Alternate Name field.

   Refer section: Replacing an Identify Certificate by a System Manager CA issued certificate for replacing the certificates.

   While replacing, refer section: Identity Certificate attributes for knowing the certificate attributes for the certificates used by System Manager
3. Run IP/FQDN change script. Refer section “Changing the IP address or FQDN in System Manager” of System Manager Admin guide.
4. Install 3rd Party CA issued certificates for System Manager Services for which certificates were replaced in step #2. Once the system is up and the web console is accessible using the new FQDN.

   Refer section: Steps to replace an Identity Certificate issued by a third-party CA
5. Update System Manager IP/FQDN on all elements interacting with System Manager.
6. Once the system is up and confirmed to be working as expected the snapshot taken in step #1 can be removed.

By replacing current certificates with new 3rd party CA issued certificates

1. Take a snapshot of the System Manager VM.
2. Optional step, only required if FQDN is being changed and *management container tls service* and/or *datastore service* has 3rd party certificate installed.

   Login to System Manager CLI using your customer CLI account and execute the script as shown below:

   $>sudo $MGMT_HOME/infra/bin/update-postgres-conf-ipfqdn.sh add

   <new_FQDN> Where <new_FQDN> is the FQDN you are changing to

3. Replace certificates for services which have 3rd party certificates installed and contain the FQDN and/or IP (whichever is being changed) in the Subject CN and/or Subject Alternate Name field with new 3rd party CA issued certificates with the new (to be changed)IP and FQDN value .

   Refer section Identity Certificate attributes for knowing the certificate attributes for the certificates used by System Manager.

   Refer section: Steps to replace an Identity Certificate issued by a third-party CA to replace the certificates.
4. Run IP/FQDN change script. Refer section "Changing the IP address or FQDN in System Manager" of System Manager Admin guide.
5. Update System Manager IP/FQDN on all elements interacting with System Manager.
6. Once the system is up and confirmed to be working as expected the snapshot taken in step #1 can be removed.

Peer Certificate Validation

All the System Manager TLS services support validation of peer Identity Certificates that have a SHA256 signature and have a public key length of 2048bits.

System Manager verifies that the peer identity certificate could be traced all the way to a trusted root CA certificate. The root CA cert must reside on the service Trust Store.

For the TLS connections from/to System Manager the identity certificate is validated using standard path validation algorithm which complies with the RFC5280 section "Certificate Path Validation".

Certificate Revocation checking is carried out as per the configuration at **Services** → **Security** → **Configuration** → **Security Configuration** on System Manager Web Console.

Certificate validation for HTTPS connections

There can be two modes of certificate validation behavior. The mode can be configured from System Manager Web Console by browsing to **SMGR** tab of **Services** → **Security** → **Configuration** → **Security Configuration.**

Cert based authentication is unchecked for **System Manager User Interface** (default configuration):

System Manager requests a client certificate (via TLS *Certificate Request* message):

- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate for the connection to get stablished.
- If the client does not provide a certificate, the connection is allowed.

Cert based authentication is checked for **System Manager User Interface**:

System Manager requests a client certificate (via TLS *Certificate Request* message):

- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate for the connection to get stablished.
- If the client does not provide a certificate, the connection is aborted.

TLS ports with mandatory mutual authentication

System Manager ports 1391(JMX,) 2009(DRS JMX), 3873(EJB-RMI), 636(LDAPS), 30865(csync2), 5432(postgres replication), 8193(JMS) have mandatory mutual authentication. For TLS connections to these ports:

System Manager requests a client certificate (via TLS *Certificate Request* message):

- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate for the connection to get stablished.
- If the client does not provide a certificate, the connection is aborted.

TLS ports with configurable mutual authentication

For System Manager Ports 52233(Licensing over HTTPS), port 9000(notify sync), port 10636(LDAPS used by IDE) mutual authentication can be configured from System Manager Web Console by browsing to **SMGR** tab of **Home → Services → Security → Configuration → Security Configuration.**

Cert based authentication is unchecked for **Other TLS Ports** (default configuration):

System Manager requests a client certificate (via TLS *Certificate Request* message):

- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate for the connection to get stablished.
- If the client does not provide a certificate, the connection is allowed.

Cert based authentication is checked for **Other TLS Ports**:

System Manager requests a client certificate (via TLS *Certificate Request* message):

- If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate for the connection to get stablished.
- If the client does not provide a certificate, the connection is aborted.

Troubleshooting Certificate issues

Login to System Manager CLI interface and execute the command as below:

$> collectLogs

Appendix

Steps to generate PKCS12 format store using openSSL

In case someone wants to import a private key and a corresponding certificate, system Manager web interface supports the use of PKCS#12 format stores for that. Refer the following steps in case a private key and certificate have already been generated and are present in separate files in PEM format.

Copy these files to the current working directory of your machine

privateKey.key: The key file that was created while generating the CSR/RSA key pair

cacert.pem: The certificate of the CA which signed the certificate. In case a chain of intermediate CAs exists, the file must contain the trusted certificate for all the intermediate CAs and the Root CA.

certificate.pem: The certificate, signed by the external CA.

Run the following command:

$>openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.pem -certfile cacert.pem

It will ask for Export password value- Provide it and remember it for use while importing certificate on System Manager.

certificate.pfx can be used to import certificates to System Manager.

FAQs

I already have external CA signed certificates from one Certificate Authority installed on System Manager, how can I replace it by certificates signed by another Certificate Authority?

>> Follow the steps as per section High level procedure to replace Identity Certificates for the new identity and trusted certificates.

How to find if a System Manager CA certificate is present in a given trust store?

>> For a given Store Type on page Services → Inventory → Manage Elements → More Actions → Manage Trusted Certificates, verify if the Subject Details and Serial Number field for any of the certificates matches the CERTSERIALNUMBER and SUBJECTDN fields respectively of the certificate found at Services → Security → Certificates → Authority → CA Structure & CRLs → View Certificate for the CA: tmdefaultca.