



Avaya Solution & Interoperability Test Lab

Configuring Avaya Aura® System Platform R6.3 with Third-Party Security Certificates for Secure Socket Layer and Transport Layer Security - Issue 1.0

Abstract

These Application Notes describe the steps to configure Avaya Aura® System Platform R6.3 to use third-party security certificates for access to the web console.

Information in these Application Notes has been obtained through Solution Integration compliance testing and additional technical discussions. Testing was conducted at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of Avaya Aura® System Platform for third-party signed security certificates. The certificate management feature is used to replace the default Avaya Aura® System Platform Web Console certificate and private key. This certificate is also used if enterprise Lightweight Directory Access Protocol (LDAP) is enabled with Transport Layer Security (TLS).

Avaya Aura® System Platform is a software platform running CentOS plus Xen open source hypervisor for virtual machine monitoring and management. It hosts one or more Avaya products, each running on its own virtual server (virtual machine), and all running on a single physical server platform. Avaya Aura® System Platform provides a set of utilities commonly required for Avaya products, including installation, upgrade, backup/restore, licensing server, hardware monitoring and alarming, and remote access.

Avaya Aura® System Platform interacts with the following virtual machines:

- System domain (dom0) virtual machine
- Console domain (cdom) virtual machine
- Services domain (services_vm) virtual machine
- Template virtual machines

The Avaya Aura® System Platform Web interface is called System Platform Web Console and can be accessed through an Internet browser such as Microsoft Internet Explorer or Mozilla Firefox. System Platform Web Console can be used to view details of Avaya Aura® System Platform virtual machines (namely, System Domain (Dom-0) and Console Domain), install the required solution template, and perform various administrative activities by accessing options from the navigation pane. In the navigation pane, there are three categories of administrative options: Virtual Machine Management, Server Management, and User Administration.

A solution template is a set of one or more Avaya applications that are pre-integrated for easy installation on Avaya Aura® System Platform. Refer to [3] and [4] in **Section 9** for details on configuring Avaya Aura® System Manager and Avaya Aura® Communication Manager solution templates for third-party certificates. All communication outbound from the customer environment uses encapsulated Hypertext Transfer Protocol Secure (HTTPS).

In the context of Avaya Aura® System Platform, the certificate that is used to assert its identity is called a product certificate or an identity certificate. The issuer or Certificate Authority (CA) certificate used to verify and validate the identity of the far end is referred to as the trusted certificate or root CA certificate. TLS sessions use a client-server model. Clients (i.e., Internet browsers) contact a server (i.e., Avaya Aura® System Platform) and are offered an identity certificate as proof of the server's integrity. Clients verify the offered certificate by testing authenticity with a common trusted root CA certificate. The Internet browser will display a certificate error if this trusted root CA certificate is not installed in its repository of trusted

certificates. The administrator has the option to install the Avaya Aura® System Platform security certificate into a certificate store on the client PC or ignore the error. If successfully authenticated; the client and server commence negotiations on an encryption scheme, and if successful, transmission is secured from that point on.

2. Interoperability Testing

These Application Notes describe the configuration on System Platform to use third-party security certificates for HTTPS and secure LDAP connections. Microsoft Windows Server 2008 with Certificate Services is used as a third-party Certificate Authority (CA).

2.1. Test Description and Coverage

The following test areas were covered.

- Administration of Avaya Aura® System Platform.
- Generation of a Certificate Signing Request (CSR).
- Signing certificate using third-party CA.
- Installation of signed certificate.
- Accessing System Platform Web Console using both Microsoft Internet Explorer and Mozilla Firefox.
- Ensure installed third-party certificates are used following System Platform reboot.

Enterprise LDAP was not tested as part of these Application Notes.

Secure Access Link (SAL) was not tested as part of these Application Notes.

2.2. Test Results and Observations

All test cases were successful with the following observations.

- One-way TLS negotiation is used to allow access from any web browser

3. Reference Configuration

Avaya Aura® System Platform is used to host Avaya Aura® System Manager in the example configuration as shown in **Figure 1**. This is to support administration of Avaya Aura® Session Managers, Avaya Aura® Communication Manager and User Management. All references are in **Section 9**. Avaya Aura® System Platform is also used to host Avaya Aura® Communication Manager. As the process to configure third-party certificates is the same for all System Platform hosts, these Application Notes will only focus on configuration of System Platform hosting System Manager.

The following restrictions apply to third-party certificates generated for System Platform:

- The only acceptable extension of a new certificate file is **.crt**.
- The only acceptable extension of a new private key file is **.key**.
- The option to select and upload the key is only for the System Platform Web Console certificate.
- An uploaded certificate is valid if its start date is not set to a date later than the current date and its end date is not set to a date earlier than the current date. An uploaded private key is valid if it matches the uploaded certificate.

All certificates generated in the example use 2048 bit key length and SHA-1 hash algorithm. Refer to [2] for details on how to generate a self-signed security certificate.

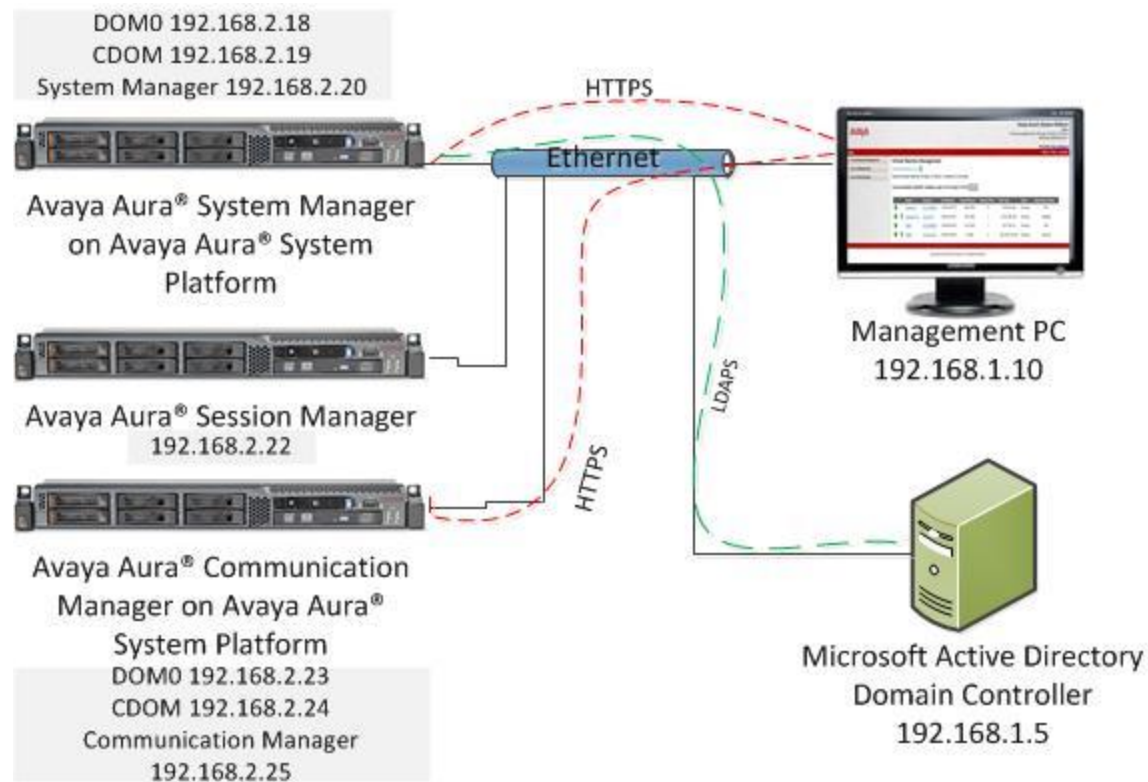


Figure 1: Avaya Aura® System Platform with Third-Party Security Certificates

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager template on Avaya Aura® System Platform running on Avaya S8800 Server	System Platform Release 6.2 FP2 System Platform Version: 6.3.1.08002 System Manager Release 6.2 FP2 System Manager Version: 6.3.6.6.2103
Avaya Aura® Communication Manager template on Avaya Aura® System Platform running on Avaya S8800 Server	System Platform Release 6.2 FP2 System Platform Version: 6.3.1.08002 Communication Manager Release 6.2 FP2 Communication Manager Version: 6.3.3.0.124
Avaya Aura® Session Manager on Avaya S8800 Server	Release 6.2 FP2 (6.3.2) Build 6.3.2.0.632023
Hewlett Packard Compaq 6000 Pro Microtower PC	Microsoft Windows Server 2008 R2 Enterprise SP1 x64 <ul style="list-style-type: none">Active Directory Certificate Services Role
Hewlett Packard Compaq 6000 Pro Microtower PC	Microsoft Windows 7 Enterprise SP1 (x32)

5. Configure Certificates for Avaya Aura® System Platform

The steps required to administer third-party certificates on System Platform are;

- Download a third-party trusted root CA certificate.
- Create a Certificate Signing Request (CSR) and Private Key for Avaya Aura® System Platform.
- Process the Certificate Signing Request.

Refer to **Section 9, Reference [3]** for details on how to configure Microsoft Windows Server 2008 Certificate Authority and templates.

5.1. Download Third-Party Certificate Authority Trusted Root Certificate

Obtain the trusted root CA certificate from the CA administrator. For a Microsoft Windows 2008 Server CA, obtain the trusted root certificate by browsing to the CA certificate services webpage <http://<CAserver IPaddress>/certsrv>, logging in with Active Directory domain administrator-level account and clicking on **Download a CA certificate, certificate chain, or CRL** link.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Select the current **CA certificate** and **Base 64** encoding method. Click **Download CA certificate**.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [TRIGGERCA1(2)]
Previous [TRIGGERCA1(1)]
Previous [TRIGGERCA1]

Encoding method:

☐ DER

☒ Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

Enter a file name (e.g., rootCAcert.pem) and save the file to the local PC.

5.2. Create a Certificate Signing Request for Avaya Aura® System Platform

To create a Certificate Signing Request for System Platform; open a Secure Shell (SSH) session to System Platform Console Domain (CDom) IP Address. Enter the following command;

```
openssl req -out smgrCDom.csr -new -newkey rsa:2048 -nodes -keyout smgrCDom.key
```

where;

- **smgrCDom.csr** is the name of the Certificate Signing Request output file.
- **smgrCDom.key** is the name of the private key.

Enter the appropriate response to the country, address, etc., as prompted. See the example below. Enter a password for the private key, when prompted.

```
[admin@smgrSPCDom ~]$ openssl req -out smgrCDom.csr -new -newkey rsa:2048 -nodes -keyout smgrCDom.key
```

Generating a 2048 bit RSA private key

.....+++

.....+++

writing new private key to 'smgrCDom.key'

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:**US**

State or Province Name (full name) [Berkshire]:**Colorado**

Locality Name (eg, city) [Newbury]:**Denver**

Organization Name (eg, company) [My Company Ltd]:**Avaya**

Organizational Unit Name (eg, section) []:**SIL**

Common Name (eg, your name or your server's hostname)

[:**smgrSPCDom.silstack.com**

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

Download the resulting CSR and private key to the local PC using an SFTP client (e.g., WinSCP or Filezilla).

Note: SHA-1 is used by the default openssl configuration file. To use SHA-2 (SHA-256 or SHA-512) it is necessary to edit the openssl configuration file to use SHA-256. See **Reference [3]** for details on how to use openssl to create a private key and certificate signing request for SHA256/2048bit keys.

5.3. Process the Certificate Signing Request

The CSR from **Section 5.2** is sent to the CA to be signed. In this example a Microsoft Windows 2008 Server Enterprise CA is used. Using Internet Explorer, browse to Microsoft Active Directory Certificate Services on the CA server. See **Reference [3]** for details on configuring Microsoft Windows 2008 Server as a certificate authority.

http://<IPaddressOfCAserver>/certsrv/

where <IPaddressOfCAserver> is the IP address or FQDN of the Microsoft Windows 2008 CA. Click on **Request a certificate**.

Microsoft Active Directory Certificate Services — TRIGGERCA1 Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Click on **Advanced Certificate Request** (Not shown). Click on **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**. (Not shown). Paste the contents of the CSR into the **Base-64-encoded certificate request box**. Use a suitable **Certificate Template** e.g., **WebServer-Enterprise**, and click **Submit**. See **Reference [3]** for details on creating certificate templates.

Microsoft Active Directory Certificate Services — ENTERPRISECA1

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 or PKCS #7 file into the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
h0S4TCJUktIL5oWxe6FLxYwMHXbnVhO64IkZzZ9T
Qa4pmpvKJrjJIGz4cZiRaR1dL51Lwovmh4bQTEDn
L0bxMTpRQwwc3Ca1EgcG4ogtv1edfTxQI85hpbMu
ACsaXpHPpmsc6ecmSPPKbFOjIwdVzbSwdPBqX9Q
UZpc5IgIO68=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

WebServer-Enterprise

Additional Attributes:

Attributes:

Submit >

Select **Base64 encoded** radio button and click **Download certificate** to save file to the local PC.



Save the signed identity certificate file with **.pem** extension and a descriptive name, e.g., **smgrCDomsigned.pem**

Note: An alternative method (to using Active Directory Certificate Services webpage) of signing the CSR utilises **certutil** command-line tool on the Windows Server 2008 CA. This method is required when a template, with a minimum support for Windows Server 2008 CA, is used. A template of this type is used when a hash algorithm of SHA-2 (SHA-256 or SHA-512) is required. An example of the command-line argument is shown below.

```
C:\Users\administrator.SILSTACK>certreq -submit -config "CA1.SILStack.com\CA1" -  
attrib "CertificateTemplate:Web-SHA256" c:/smgrSPCDom.csr
```

Where;

- **CA1.SILStack.com\CA1** is the name of the CA server configuration string, found by entering the command **certutil -getconfig**.
- **Web-SHA256** is the name of a template configured with sha256 hash algorithm, 2048 bit encryption, and client and server authentication.
- **c:/smgrSPCDom.csr** is the file path to CSR.

6. Configure Avaya Aura® System Platform to use Third-Party Signed Security Certificates and Private Key

The default System Platform Web Console certificate and private key can be replaced by selecting and uploading a new certificate file and a new private key from the local machine. Open a compatible web browser (Microsoft Internet Explorer or Mozilla Firefox) and enter the Fully Qualified Domain Name (FQDN) or IP address of System Platform CDom into the address bar using HTTPS. Log into System Platform by entering a valid user ID and password.

A login form with a title "Login". It contains two input fields: "User Id" with the value "admin" and "Password" with masked characters "*****". Below the fields are two buttons: "Reset" and "Log On".

Browse to **Server Management** → **Certificate Management**. The default **System Platform Certificate** is displayed.

The image shows the main interface of the Avaya Aura® System Platform Web Console. The top header is the same as the previous image. Below it is a red navigation bar with "Home" and "HA status: Not configured" (with "About", "Help", and "Log Out" links). A left sidebar contains a tree view with categories: "Virtual Machine Management", "Server Management" (highlighted with a red box), and "User Administration". Under "Server Management", "Certificate Management" is also highlighted with a red box. The main content area is titled "Server Management" and "Certificate Management". It displays the "System Platform Certificate" details in a table-like format with fields for Type, Version, Start Date, Expiry Date, Issuer, Subject, Serial Number, and SHA-1 Thumbprint. Below this are sections for "Change Certificate Alarm Parameters" (with a "Save" button) and "Provide New Certificate" (with steps for uploading a new certificate file and a new private key file).

6.1. Install third-party Security Certificate and Private Key on Avaya Aura® System Platform

Click on **Provide New Certificate** to expand the options for adding new certificates and private key. Under the heading **Upload new Certificate File (Required)**, click on **Select New Certificate File** and browse to the signed third-party certificate created in **Section 5.3**. Click **Open** (Not Shown) to select the file. Click **Upload**.



Provide New Certificate

1 -> Upload new Certificate File (Required)

Select New Certificate File Upload

C:\Users\emmetlee\Documents\SIL\Trigger Proj Cancel

Click on **Upload new Private Key** and **Select Private Key File**. Browse to the private key file generated in **Section 5.2**, click **Open**(Not shown) and **Upload**.

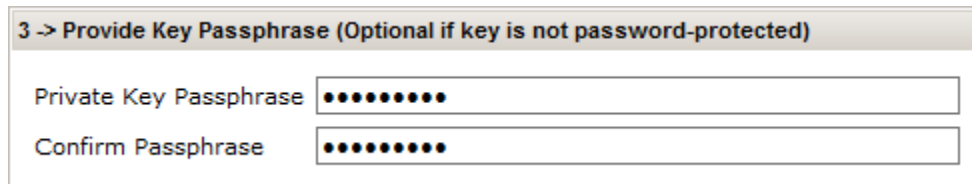


2 -> Upload new Private Key File (Required)

Select Private Key File Upload

C:\Users\emmetlee\Documents\SIL\ Cancel

Enter the password for the private key, created in **Section 5.2**.



3 -> Provide Key Passphrase (Optional if key is not password-protected)

Private Key Passphrase

Confirm Passphrase

Click on **Upload Chain Certificate** and **Provide New Certificate**. Browse to the third-party CA certificate downloaded from the CA in **Section 5.1**, click **Open**(Not shown) and **Upload**.



4 -> Upload Chain Certificate File (Optional if certificate is self-signed)

Provide New Certificate Upload

C:\Users\emmetlee\Documents\SIL\ Cancel

Click **Save** (Not Shown). System Platform will restart and the new third-party or customer defined certificates will be used thereafter, when accessing the server over HTTPS.

6.2. Certificate Alarm Parameters

Avaya recommends configuration of the certificate alarm parameters to notify an administrator of impending expiration of a security certificate. To configure the number of days prior to console domain certificate expiration date, browse to **Server Management** → **Certificate Management**. Enter the number of days under the **Change Certificate Alarm Parameters** section and click **Save**.

Home

Virtual Machine Management

Server Management

- System Information
- Patch Management**
- Platform Upgrade
- Log Viewer
- Date / Time Configuration
- Logging Configuration
- System Configuration
- Network Configuration
- Static Route Configuration
- Ethernet Configuration
- Alarm Configuration
- Certificate Management**
- License Management
- SAL Gateway Management
- High Availability
- Performance Statistics
- Eject CD / DVD
- File Manager
- Security Configuration
- Backup / Restore**
- Server Reboot / Shutdown
- SNMP Trap Receiver Configuration

Server Management

Certificate Management ?

System Platform Certificate

Type:	X.509
Version:	3
Start Date:	Mon Feb 10 10:04:54 GMT 2014
Expiry Date:	Wed Feb 10 10:04:54 GMT 2016
Issuer:	CN=TRIGGERCA1, DC=SILStack, DC=com
Subject:	CN=smgrSPCDom.silstack.com, OU=SIL, O=Avaya, L=Galway, ST=Connecticut
Serial Number:	86171950705409418854780
SHA-1 Thumbprint:	16:5D:62:88:9F:8E:1F:1F:39:C0:4D:1B:EA:6A:8E:AD:35:B6:07:7C

Change Certificate Alarm Parameters

Issue a daily alarm days before the console domain certificate expiration date.

Provide New Certificate

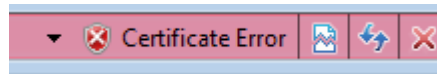
6.3. Enterprise Lightweight Directory Access Protocol Authentication

System Platform web console user authentication can be implemented against an enterprise Lightweight Directory Access Protocol (LDAP) Authentication database. If the user login details do not match a local System Platform LDAP account, then an external enterprise LDAP server can be accessed for authentication. See **Reference [2]** for details on configuring enterprise LDAP for System Platform. If TLS is used for secure enterprise LDAP communication, the third-party security certificate installed in **Section 6.1** will be used during the TLS negotiation with the directory server, e.g., Microsoft Active Directory.

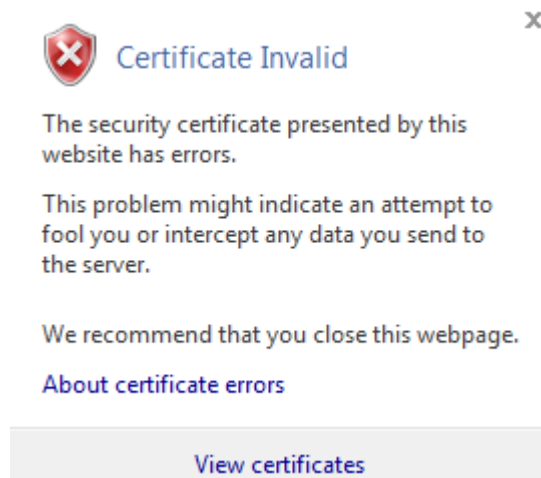
7. Verification Steps

This section includes instructions to verify System Platform deployment is successfully using third-party TLS certificates for System Platform Web console.

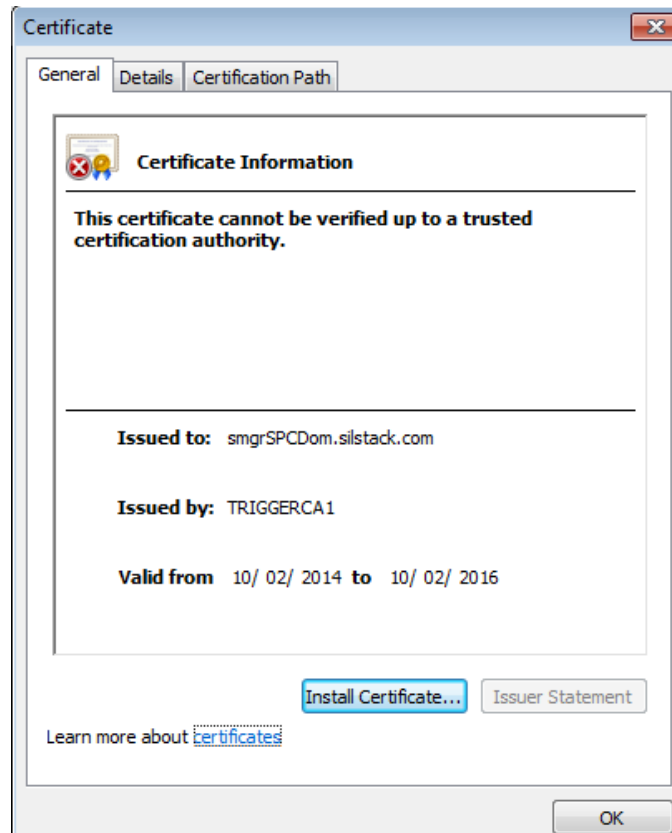
When logging into System Platform click on the **Certificate Error** on the browser bar, when using Microsoft Internet Explorer.



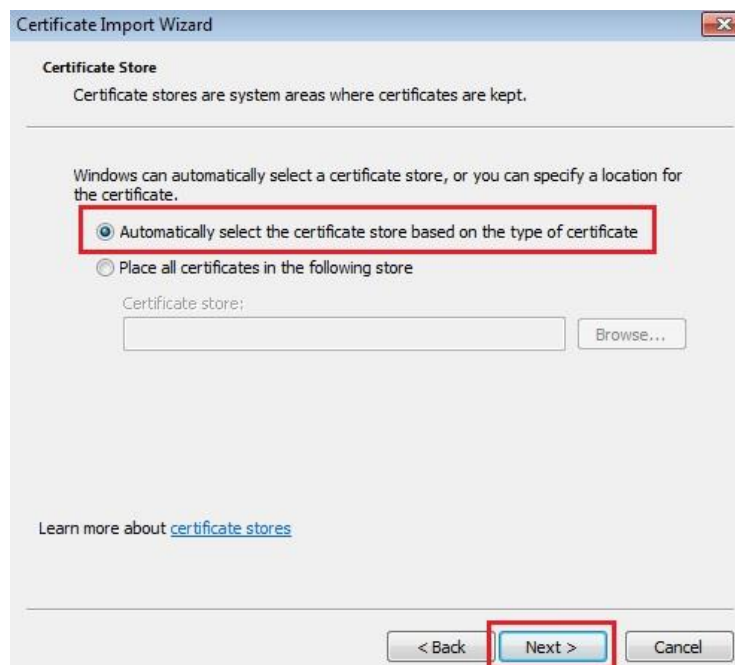
Click on **View Certificates**.



Ensure the new certificate in use is the third-party signed certificate created in **Section 5.3**.



In order to stop the web browser displaying certificate error when accessing System Platform Web console, select **Install Certificate** from the screen above. The certificate import wizard will open. Select **Next** (Not Shown). Use the default setting for certificate store and select **Next**.



Select **Finish**.



8. Conclusion

These Application Notes describe a sample configuration of Avaya Aura® System Platform using third-party signed security certificates. Security certificates are used for HTTPS connections to the Avaya Aura® System Platform Web Console.

9. Additional References

Avaya Product documentation relevant to these Application Notes is available at <http://support.avaya.com>.

- [1] Overview of Avaya Aura System Platform, Release 6.3.1, Issue 1, October 2013
- [2] Administering Avaya Aura System Platform, Release 6.3.1, issue 1, October 2013
- [3] Configuring Avaya Aura® System Manager 6.2 FP2 and Avaya Aura® Session Manager 6.2 FP2 to use Third-Party Security Certificates for Transport Layer Security - Issue 1.0
- [4] Configuring Avaya Aura® Communication Manager 6.2 FP2, Avaya Aura® Utility Services 6.3, Avaya 9641 IP Deskphone and Avaya 9620 IP Deskphone to use Third-Party Security Certificates for Transport Layer Security - Issue 1.0

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com