

AES - Renew AES Cert using System Manager

AES certificate renewal if using SMGR certificate with CA Certificate and End Entity in place.

*This work will need a maintenance window for restarts of the AES.

1. Remove Certificate that is about to expire from AES.

Security | Certificate Management | Server Certificates Home | Help | Log

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
CA Trusted Certificates
Server Certificates

Server Certificates

Add Delete Export Import Renew View

Alias	Status	Issued To	Issued By	Expiration Date
• aeservices	alert	sps-aes.euronetservices.net	System Manager CA	Mar 24, 2019

2. Restart AE Server

Maintenance | Service Controller Home | Help | Log

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

3. Go to the System Manager> Security> Certificates> Authority> Search End Entities

AVAYA
Aura® System Manager 7.0

Home Security * Adv

CA Functions ^

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

RA Functions

- Add End Entity
- End Entity Profiles
- Search End Entities

Search End Entities

Search end entity with username

Search end entity with Certificate SN (hex)

Search end entities with status --

Search end entities with certificates expiring within Days

Made by PrimeKey Solutions AB, 2002–2014.

4. Verify the certificate for your AES by the CN and select *Edit End Entity*

Search end entities with certificates expiring within Days

Select	Username	CA	CN	OU	O (organization)	Status	
<input type="checkbox"/>	INBOUND_OUTBOUND_TLStmdefaultca	chi-smm.euronetservices.net			Avaya	Generated	View End Entity Edit End Entity View Certificates View History
<input type="checkbox"/>	avaya	tmdefaultca	chi-aes.euronetservices.net	SDP	AVAYA	Generated	View End Entity Edit End Entity View Certificates View History
<input type="checkbox"/>	avaya1	tmdefaultca	sps-aes.euronetservices.net	SDP	AVAYA	Generated	View End Entity Edit End Entity View Certificates View History

5. Change the status to New, enter the passwords and then Save

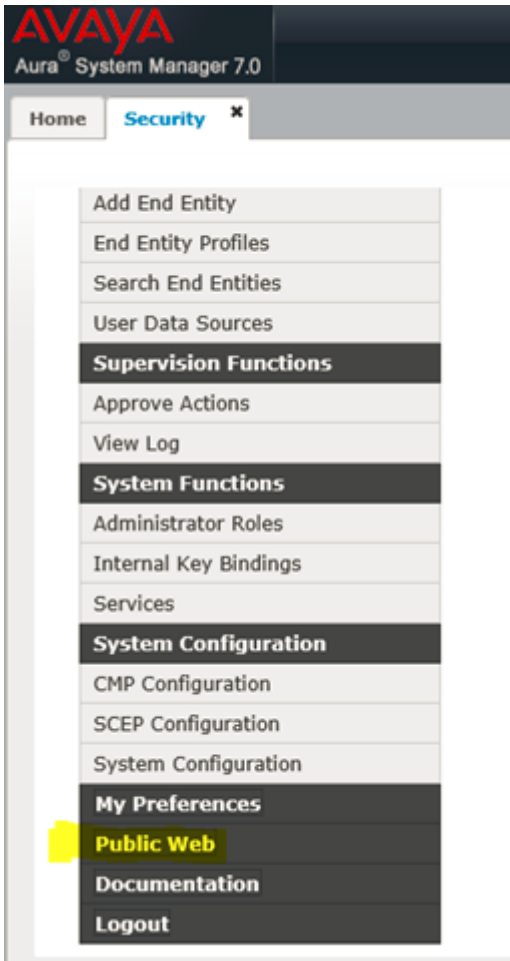
Edit End Entity

End Entity Profile INBOUND_OUTBOUND_TLS Req

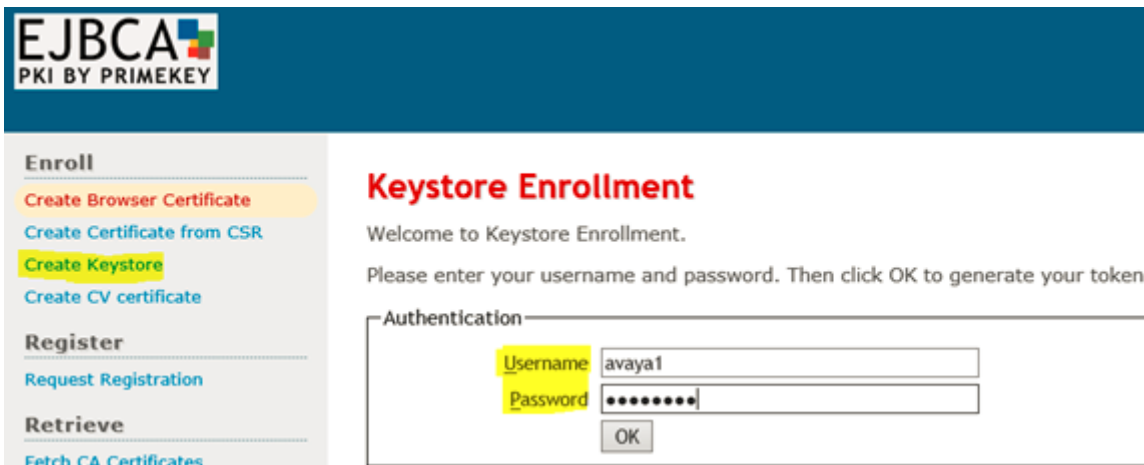
Status **New**

Username avaya1	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	<input checked="" type="checkbox"/>
Confirm Password	<input type="checkbox"/>
Maximum number of failed login attempts	<input type="checkbox"/> <input type="text"/> <input checked="" type="radio"/> Unlimited
Remaining login attempts	<input type="text"/> <input type="checkbox"/> Reset login attempts
E-mail address	<input type="text"/> @ <input type="text"/> <input type="checkbox"/>
Subject DN	
CN, Common name	sps-aes.euronetservices.net <input checked="" type="checkbox"/>
CN, Common name	<input type="text"/> <input type="checkbox"/>
O, Organization	AVAYA <input type="checkbox"/>
C, Country (ISO 3166)	US <input type="checkbox"/>
OU, Organizational Unit	SDP <input type="checkbox"/>
L, Locality	<input type="text"/> <input type="checkbox"/>
ST, State or Province	<input type="text"/> <input type="checkbox"/>
Other subject attributes	
Subject Alternative Name	
DNS Name	<input type="text"/> <input type="checkbox"/>
DNS Name	<input type="text"/> <input type="checkbox"/>
IP Address	<input type="text"/> <input type="checkbox"/>
Main certificate data	
Certificate Profile	ID_CLIENT_SERVER <input checked="" type="checkbox"/>
CA	tmdefaultca <input checked="" type="checkbox"/>
Token	P12 file <input checked="" type="checkbox"/>

6. Scroll to the bottom of the page and select *Public Web*.



7. Select Create Keystore and then enter the username and password from the End Entity and select OK.



8. Select 2048 bits and then Select Enroll.

Enroll

Create Browser Certificate

Create Certificate from CSR

Create Keystore

Create CV certificate

Register

Request Registration

Retrieve

Fetch CA Certificates

Fetch CA CRLs

List User's Certificates

Fetch User's Latest Certificate

Inspect

EJBCA Token Certificate Enrollment

Welcome to keystore enrollment.

If you want to, you can manually install the CA certificate(s) in your browser, other automatically when your certificate is retrieved.

Install CA certificates:

[Certificate chain](#)

Please choose a key length, then click OK to fetch your certificate.

Options

Leave values as default if unsure.

Key length: 2048 bits

Enroll

Once you click enroll the certificate will be downloaded (depending on your browser you can select where it is saved or find it in downloads from windows explorer).

Next Import the new AE Services server certificate into the AES

1. Using the AE Services Management Console navigate to "Security > Certificate Management > Server Certificates"
2. Click on the Import button and upload the new AE Services server certificate you created above (this will be the .p12 file). Select an alias (server) from the drop down menu
3. Click the "Apply" button.

- > AE Services
- > Communication Manager Interface
- > High Availability
- > Licensing
- > Maintenance
- > Networking
- ▼ Security
- > Account Management
- > Audit
- ▼ Certificate Management
- CA Trusted Certificates
- ☐ Server Certificates

Server Certificates

Add Delete Export Import Renew View

Alias	Status	Issued To	Issued By

4. Select Choose file, Establish Chain of Trust and Certificate Alias.

Security | Certificate Management | Server Certificates

- > AE Services
- > Communication Manager Interface
- > High Availability
- > Licensing
- > Maintenance
- > Networking
- ▼ Security
- > Account Management
- > Audit
- ▼ Certificate Management
- CA Trusted Certificates
- ☐ Server Certificates

Server Certificate Import

File Path*: Choose file Dave.p12

Establish Chain of Trust

Certificate Alias* server ▼

Apply Close

5. Enter the PKCS12 password (from the End Entity) and select Apply and then on the next page Apply again.

Navigation menu (left):

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security

Dialog Box: Server Certificate Import Continue

PKCS12 Password* [masked]

Buttons: Apply, Close

Navigation menu (left):

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
 - Account Management
 - Audit
 - Certificate Management
 - CA Trusted Certificates
 - Server Certificates

Dialog Box: Server Certificate Import

Warning! You are importing the server certificate. The new server certificate can only take effect when the AE services restarts.

⚠ Please use the Maintenance -> Service Controller page to restart AE Server.

Buttons: Apply, Cancel

6. Restart the Linux server.

Page Header: Maintenance | Service Controller

Navigation menu (left):

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
 - Date Time/NTP Server
 - Security Database
 - Service Controller
 - Server Data
- Networking
- Security
- Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, Restart Web Server

