

# Partner Test Management – SAML2 Configuration



## Applies to:

SAP Solution Manager 7.1 and 7.2 – Test Suite – Partner Test Management – Adapter

## Summary

To Integrate the SAP Solution Manager & HP ALM (formerly HP QC), we need to enable the authentication using the SAML2 protocol. This document would explain you the required configurations for SAP Solution Manager as well as in the Partner.

**Author(s):** Benu Mariantony

**Company:** SAP Labs

**Created on:** 20 September 2016

## Author Bio



Detail-oriented Senior Development Expert with over 9 years' of experience in SAP HANA, SAPUI5, Fiori, ABAP (including the new features of 740/ 750), ABAP on HANA, ABAP Objects, ABAP – Webdynpro, Gateway Services (ODATA), FPM, HR-ABAP, Interfacing, ABAP XML Processing (XSLT, Simple Transformations, ODATA and JSON), Solution Manager 7.1/ 7.2 and upgrade. Skilled in both the "object" and the "classical" sides of ABAP stream, focusing on technical arena involved dynamic programming, design, optimization, and performance tuning.

## Contents

|  |    |
|--|----|
| 1. Overview .....  | 3  |
| 2. Enable SAML2 in Solution Manager System .....           | 3  |
| 3. Export Certificates from Solution Manager .....         | 6  |
| 4. Enable SAML on HP ALM .....                             | 7  |
| 5. Upload the Certificate in Solution Manager System ..... | 16 |
| 6. Add and Enable the HP ALM Trusted Provider .....        | 18 |

# 1. Overview

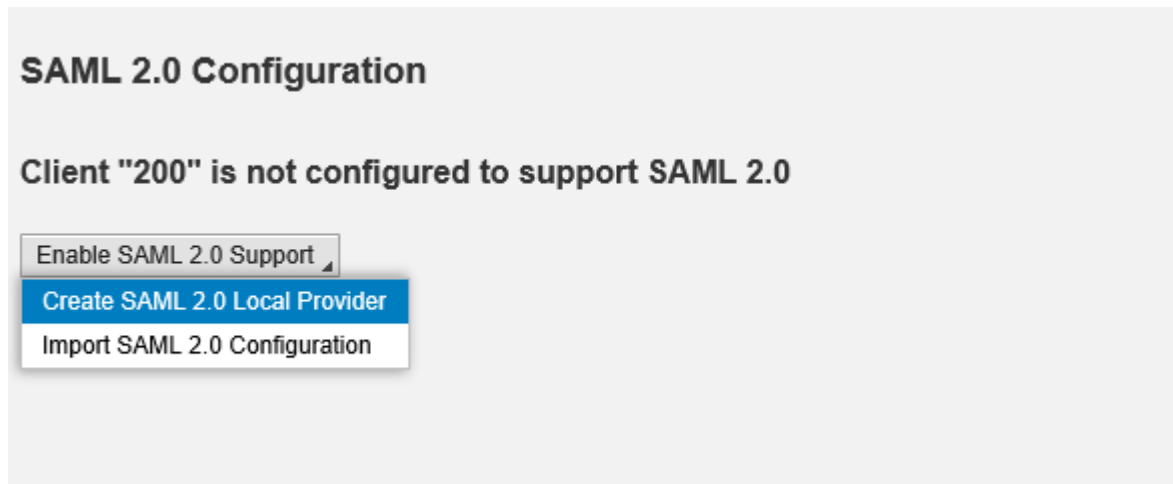
To enable the Partner Test Management – Adapter in Solution Manager, we need to enable the integration between Solution Manager and HP ALM (formerly HP QC). This document explains to trust the Solution Manager System and HP ALM system powered by SAML2 authentication mechanism. Please follow the following steps to enable the integration,

1. Enable SAML2 on the Solution Manager system
2. Export Certificates from Solution Manager
3. Enable SAML on HP ALM (In this document we will take HP ALM as an use case)
4. Import the HP ALM SAML certificate in Solution Manager
5. Add and Enable the HP ALM Trusted Provider

## 2. Enable SAML2 in Solution Manager System

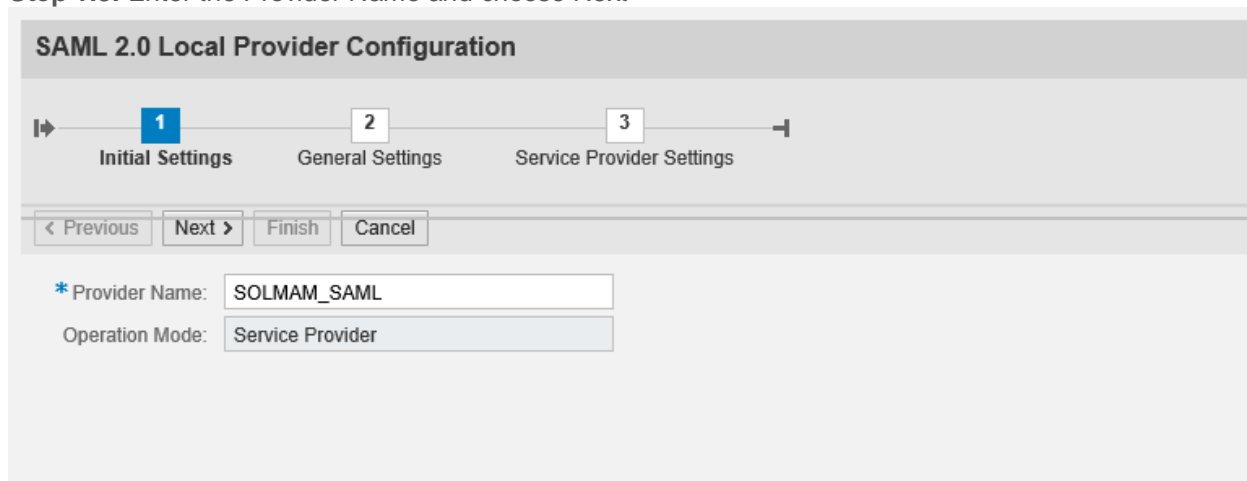
**Step 1.1:** Launch the transaction SAML2

If you do not get to see the below screen, please refer the Step – 1.6.



**Step 1.2:** Choose the Menu Item “Create SAML 2.0 Local Provider”

**Step 1.3:** Enter the Provider Name and choose Next



**Step 1.4:** Do not change anything in the “Step 2”. Click “Next”

## SAML 2.0 Local Provider Configuration

1 Initial Settings    2 General Settings    3 Service Provider Settings

< Previous    Next >    Finish    Cancel

### Miscellaneous

Clock Skew Tolerance:  Seconds

**Step 1.5:** Do not change anything in the Step – 3. Click on Finish

## SAML 2.0 Local Provider Configuration

1 Initial Settings    2 General Settings    3 Service Provider Settings

< Previous    Next >    Finish    Cancel

**Identity Provider Discovery: Common Domain Cookie (CDC)**  
 Selection Mode:

**Miscellaneous**  
 Affiliation Name:

**Assertion Consumer Service**  
 Supported Bindings: ☒ HTTP POST    ☒ HTTP Artifact    ☒ PAOS

**Single Logout Service**  
 Supported Bindings: ☒ HTTP Redirect    ☒ HTTP POST    ☒ HTTP Artifact    ☒ SOAP

**Artifact Resolution Service**  
 Mode:   
 Artifact Validity Period:  Seconds

The final state of SAML configuration should be the below,

**Step 1.6:** Enable the SAML by clicking on the “Enable” Button,


## SAML 2.0 Configuration of ABAP System: HF2/200

Local Provider Trusted Providers Policies Name ID Management

Edit Save Cancel **Enable** Metadata Delete Configuration Export Configuration

Provider Name: SOLMAM\_SAML

Operation Mode: Service Provider

Status:  Disabled

General Settings Authentication Contexts Service Provider Settings

**Signature and Encryption**

Signing Keypair: CN=HF2\_SSFA\_S2SVPS, OU=I0020270862, OU=SAP Web AS, O=SAP Trust Commr Details

Encryption Keypair: CN=HF2\_SSFA\_S2SVPE, OU=I0020270862, OU=SAP Web AS, O=SAP Trust Commr Details

☐ Include Certificate in Signature

☒ Sign Metadata

**Miscellaneous**

Clock Skew Tolerance: 120 Seconds

The SAML is enabled now,


## SAML 2.0 Configuration of ABAP System: HF2/200

Local Provider Trusted Providers Policies Name ID Management

Edit Save Cancel Disable Metadata Delete Configuration Export Configuration

Provider Name: SOLMAM\_SAML

Operation Mode: Service Provider

Status:  Enabled

General Settings Authentication Contexts Service Provider Settings

**Signature and Encryption**

Signing Keypair: CN=HF2\_SSFA\_S2SVPS, OU=I0020270862, OU=SAP Web AS, O=SAP Trust Commr Details

Encryption Keypair: CN=HF2\_SSFA\_S2SVPE, OU=I0020270862, OU=SAP Web AS, O=SAP Trust Commr Details

☐ Include Certificate in Signature

☒ Sign Metadata

**Miscellaneous**

Clock Skew Tolerance: 120 Seconds

### 3. Export Certificates from Solution Manager

**Step 2.1:** Launch the transaction STRUST in Solution Manager System

**Step 2.2:** Export the SSL certificate

- Choose the server in the node “SSL Server Standard”
- Double click on the Subject as shown in the below screen shot.
- Go to an Edit Mode
- Export the certificate by clicking on the button “Export”
- Store the certificate in the local folder

Trust Manager: Change

SSL server Standard

Own Certificate

Subject

Certificate List

| Subject   |
|---|
| DN: #.wall.rap.ame, OU: FAZ, O: SAP, C: DE              |
| SP: Germany, DN: #.wall.rap.ame, OU: FAZ, O: SAP, C: DE |
| DN: SAPRSTCA CP, O: SAP, I: Walldorf, C: DE             |
| DN: SAP Global Root: CA, O: SAP AG, I: Walldorf, C: DE  |

Veri. PSE Password

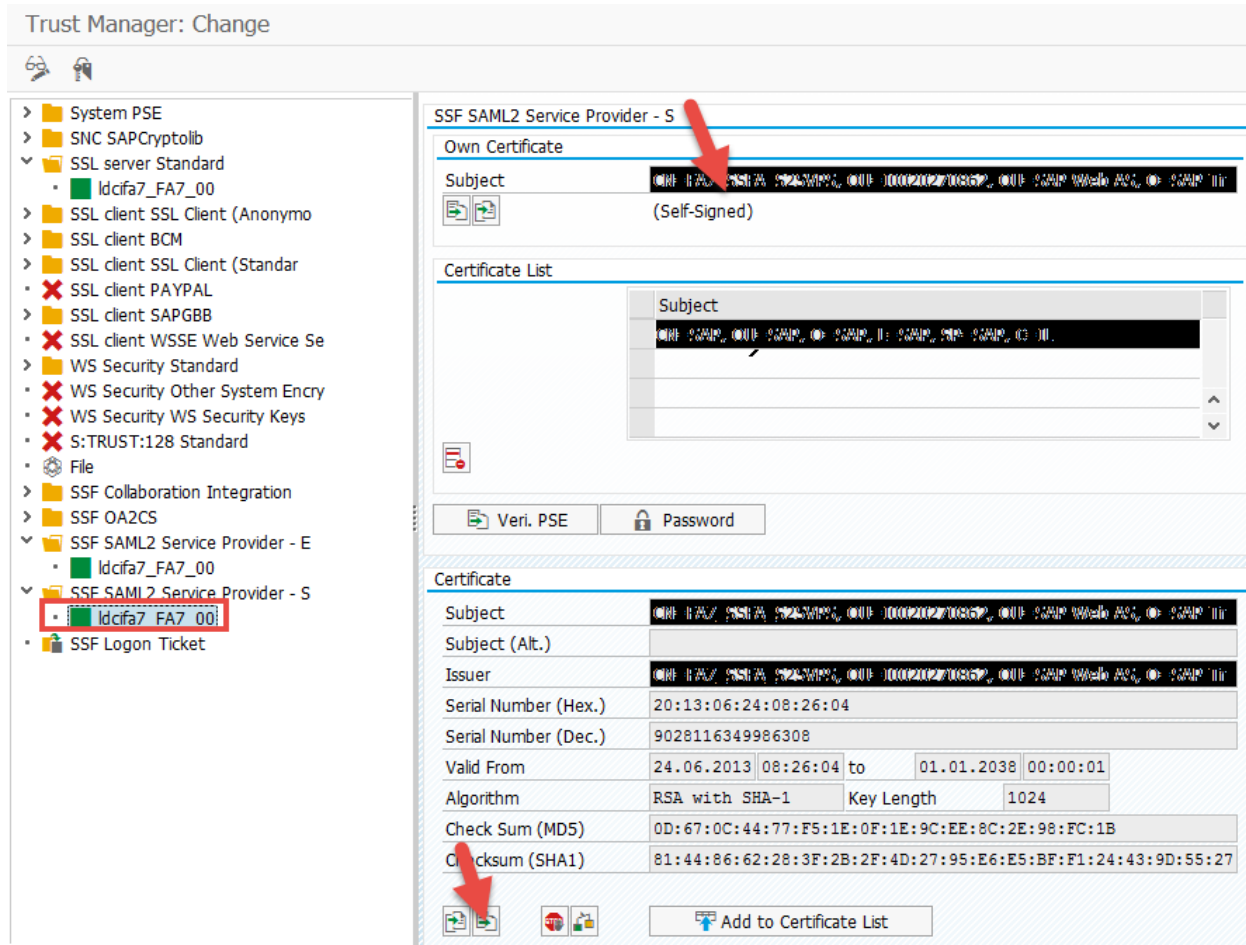
Certificate

|                      |   |
|----------------------|---|
| Subject              | DN: #.wall.rap.ame, OU: FAZ, O: SAP, C: DE                  |
| Subject (Alt.)       | dn: #.wall.rap.ame, OU: FAZ, O: SAP, C: DE                  |
| Issuer               | DN: SAPRSTCA CP, O: SAP, I: Walldorf, C: DE                 |
| Serial Number (Hex.) | 50:9A   |
| Serial Number (Dec.) | 20634   |
| Valid From           | 02.07.2015 10:12:47 to 02.07.2017 10:12:47                  |
| Algorithm            | RSA with SHA-256 Key Length 1024                            |
| Check Sum (MD5)      | 5E:F4:40:92:DD:33:37:A3:9B:E8:C9:AE:62:36:46:9D             |
| Check Sum (SHA1)     | CC:CD:92:51:13:F3:1C:1D:86:5A:48:AA:A1:B0:B8:62:7B:8A:E0:91 |

Add to Certificate List

**Step 2.3:** Export the SAML Certificate

- In the same STRUST transaction launch the node “SSF SAML2 Service Provider – S”
- Double click on the subject
- Go to the Edit Mode
- Export the certificate using an “Export Button”
- Save the certificate in the local folder

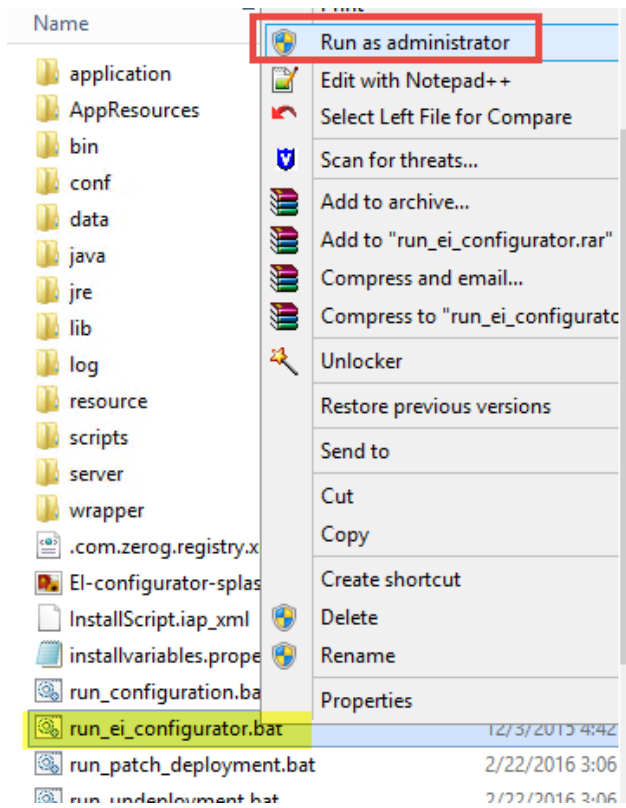


## 4. Enable SAML on HP ALM

In this activity, we will upload the Solution Manager's SSL and SAML certificates that was exported in the previous step.

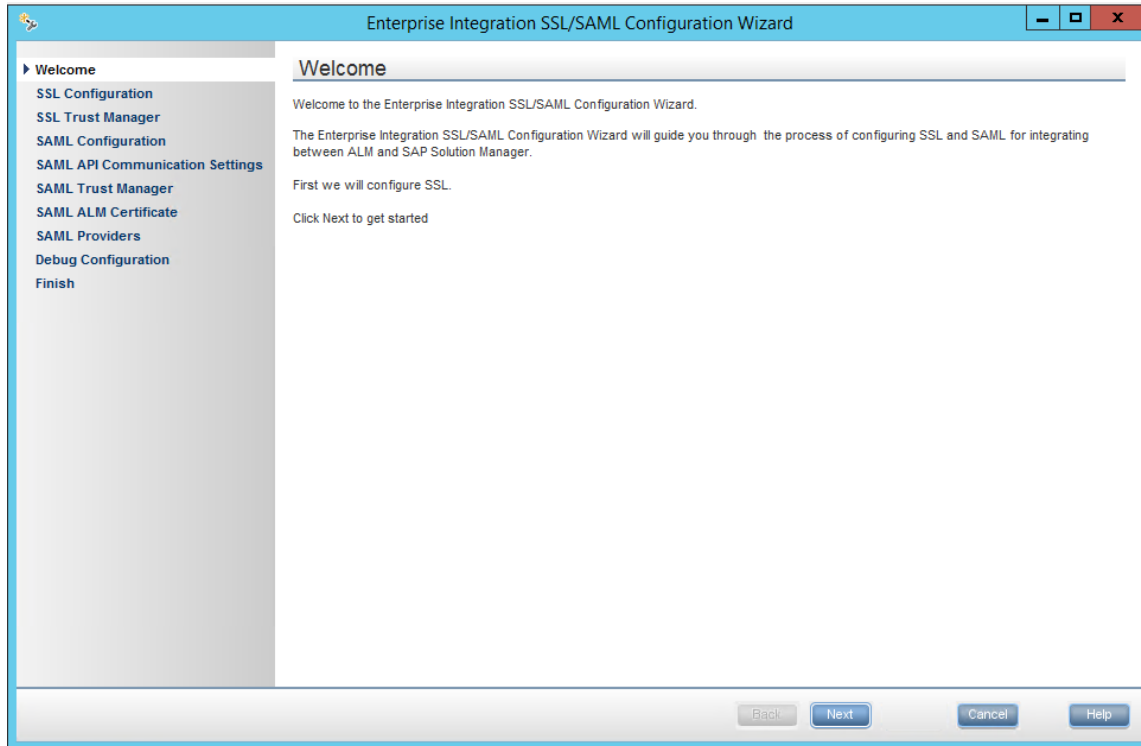
**Step – 3.1:** Launch the “Enterprise Integration Configuration Wizard”. Please follow the below instructions,

- Logon to the HP ALM server (The windows server where the HP ALM system is installed)
- go to the folder path “C:\Program Files\HP\ALM\ALM”
- Run the file “run\_ei\_configurator.bat” as administrator.

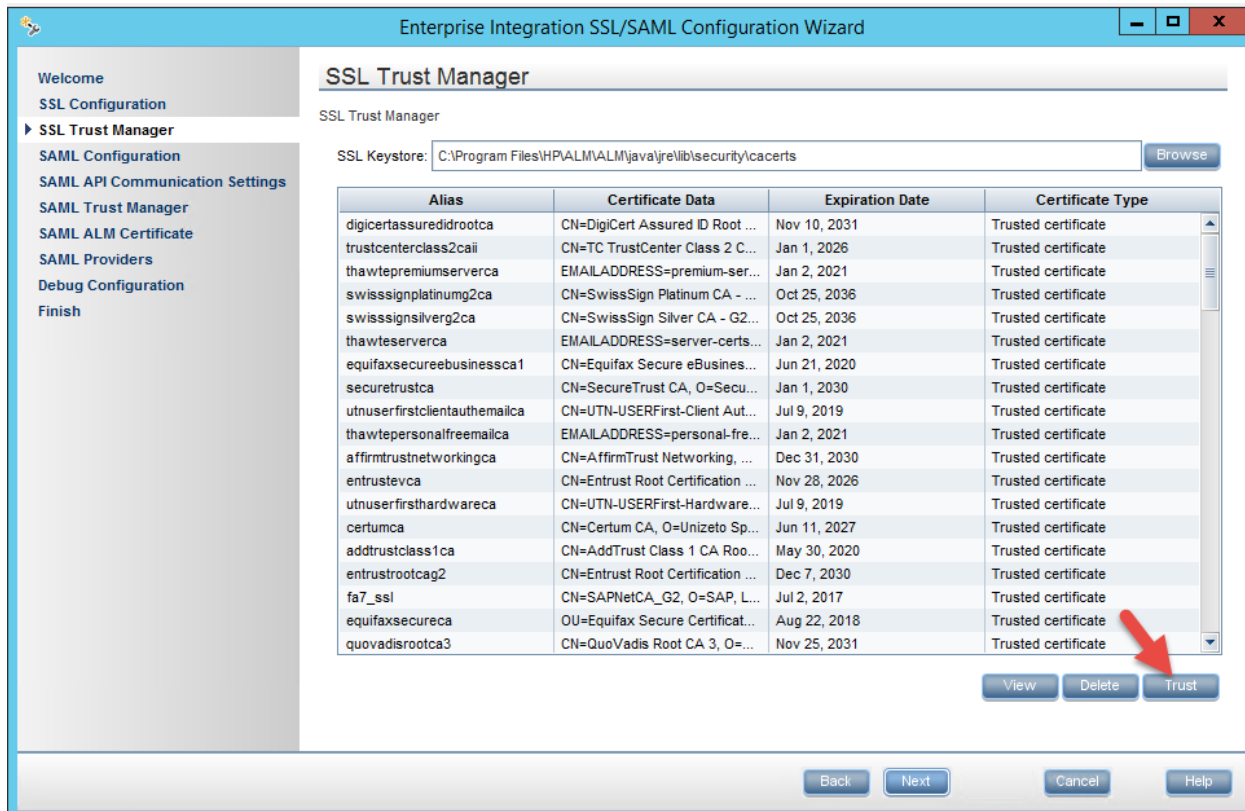


The following wizard would be launched





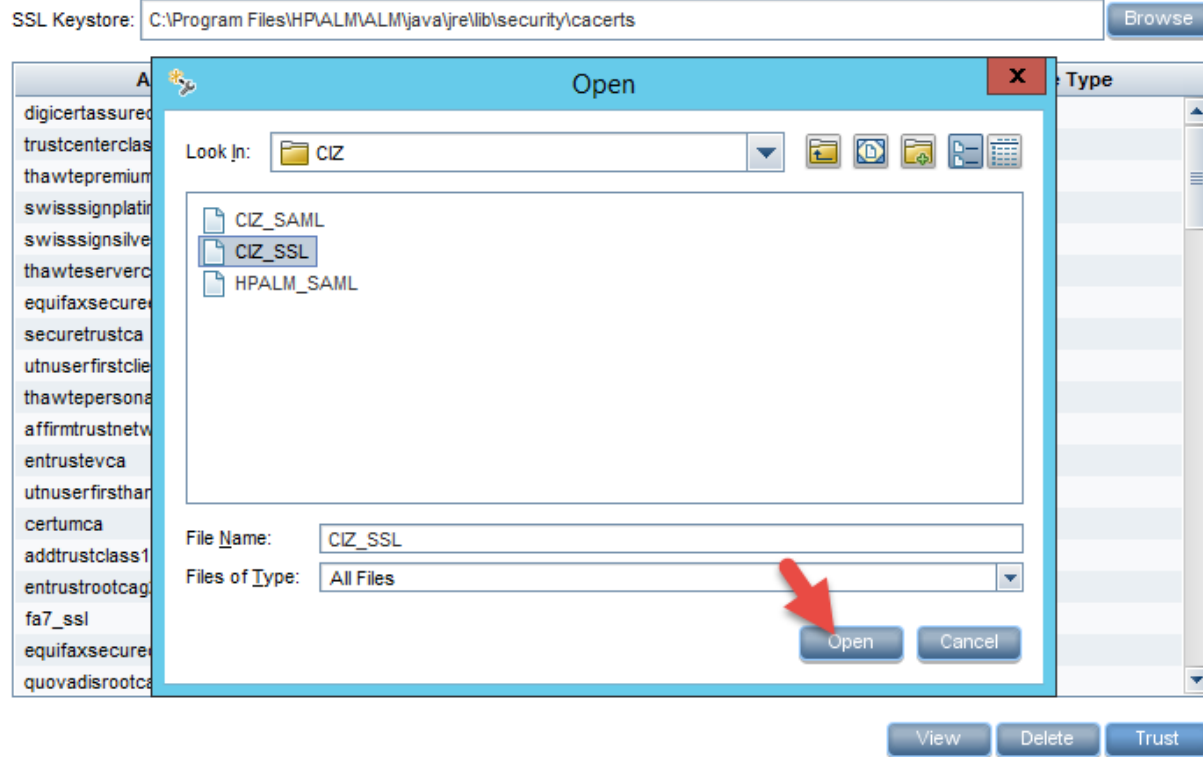
**Step – 3.2:** Navigate to the “SSL Trust Manager” by clicking on “Next”



Choose the SSL certificate exported from Solution Manager System,

## SSL Trust Manager

SSL Trust Manager



Provide an "Alias Name". Preferably <SID of Solution Manager>\_SSL



After this step, you will be able to see an entry in the list,

SSL Keystore:

| Alias                          | Certificate Data                | Expiration Date | Certificate Type    |
|--------------------------------|---------------------------------|-----------------|---------------------|
| quovadisrootca3                | CN=QuoVadis Root CA 3, O=...    | Nov 25, 2031    | Trusted certificate |
| quovadisrootca2                | CN=QuoVadis Root CA 2, O=...    | Nov 24, 2031    | Trusted certificate |
| digicerthighassuranceevrootca  | CN=DigiCert High Assurance ...  | Nov 10, 2031    | Trusted certificate |
| secomvalicertclass1ca          | EMAILADDRESS=info@valicer...    | Jun 26, 2019    | Trusted certificate |
| fbt                            | CN=SAPNetCA_G2, O=SAP, L...     | May 18, 2017    | Trusted certificate |
| equifaxsecureglobalebusines... | CN=Equifax Secure Global eB...  | Jun 21, 2020    | Trusted certificate |
| geotrustuniversalca            | CN=GeoTrust Universal CA, O...  | Mar 4, 2029     | Trusted certificate |
| ciz_ssl                        | CN=SAP Global Root CA, O=S...   | Mar 17, 2025    | Trusted certificate |
| verisignclass3ca               | OU=Class 3 Public Primary Ce... | Aug 3, 2028     | Trusted certificate |
| thawteprimaryrootcag3          | CN=thawte Primary Root CA - ... | Dec 2, 2037     | Trusted certificate |
| thawteprimaryrootcag2          | CN=thawte Primary Root CA - ... | Jan 19, 2038    | Trusted certificate |
| deutsche Telekomrootca2        | CN=Deutsche Telekom Root C...   | Jul 10, 2019    | Trusted certificate |
| buypassclass3ca                | CN=Buypass Class 3 Root CA...   | Oct 26, 2040    | Trusted certificate |
| utnuserfirstobjectca           | CN=UTN-USERFirst-Object, O...   | Jul 10, 2019    | Trusted certificate |
| geotrustprimaryca              | CN=GeoTrust Primary Certific... | Jul 17, 2036    | Trusted certificate |
| buypassclass2ca                | CN=Buypass Class 2 Root CA...   | Oct 26, 2040    | Trusted certificate |
| baltimorecodesigningca         | CN=Baltimore CyberTrust Cod...  | May 18, 2025    | Trusted certificate |
| verisignclass1ca               | OU=Class 1 Public Primary Ce... | Aug 3, 2028     | Trusted certificate |
| baltimorecybertrustca          | CN=Baltimore CyberTrust Root... | May 13, 2025    | Trusted certificate |

### Step – 3.3: Navigate to “SAML API Communication Settings”

Enable the SAML for the below operations,

- Blueprint/ Solution Documentation Integration
- Incident/ Defect Integration
- BPCA Integration (if required)

Enterprise Integration SSL/SAML Configuration Wizard

**SAML API Communication Settings**

Use SAML authentication for:

- ☒ Blueprint/Requirement integration
- ☒ Incident/Defect integration
- ☒ BCPA Integration

### Step – 3.4: Navigate to “SAML Trust Manager” to upload the SAML certificate

Welcome

SSL Configuration

SSL Trust Manager

SAML Configuration

SAML API Communication Settings

► SAML Trust Manager

SAML ALM Certificate

SAML Providers

Debug Configuration

Finish

## SAML Trust Manager

SAML Trust Manager

SAML Keystore:  Browse

| Alias        | Certificate Data            | Expiration Date | Certificate Type    |
|--------------|-----------------------------|-----------------|---------------------|
| flq_saml     | CN=FLQ_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fl7_saml2    | CN=FL7_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fa7_saml_new | CN=FA7_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fbt_saml     | CN=FBT_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fq7_saml     | CN=FLQ_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |

View Delete Trust

Click on the “Trust” button to upload the SAML certificate exported from Solution Manager system,

flq\_saml

fl7\_saml2

fa7\_saml\_new

fbt\_saml

fq7\_saml

Open

Look In: CIZ

CIZ\_SAML

CIZ\_SSL

HPALM\_SAML

File Name: CIZ\_SAML

Files of Type: All Files

Open
Cancel

View Delete Trust

Provide the Alias Name,



After uploading the SAML certificate, you must see an entry in the list,

## SAML Trust Manager

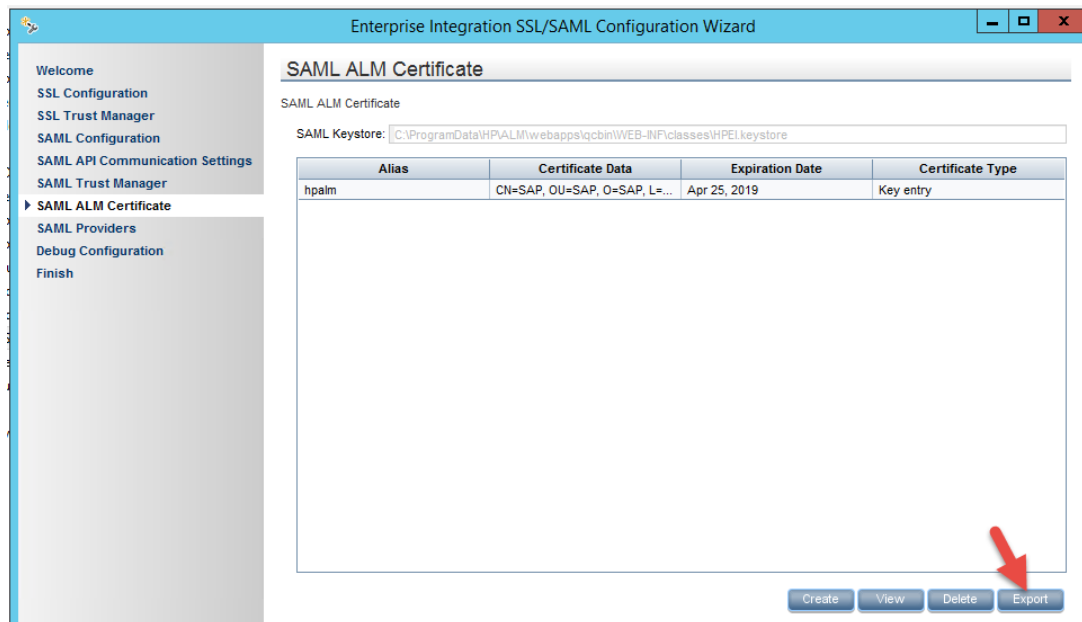
SAML Trust Manager

SAML Keystore:

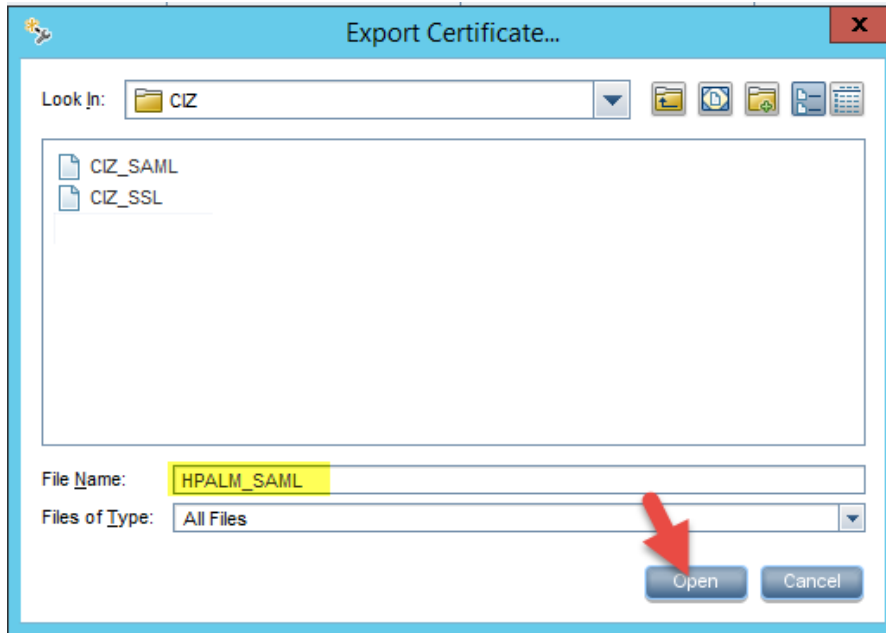
| Alias        | Certificate Data            | Expiration Date | Certificate Type    |
|--------------|-----------------------------|-----------------|---------------------|
| flq_saml     | CN=FLQ_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fl7_saml2    | CN=FL7_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fa7_saml_new | CN=FA7_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fbt_saml     | CN=FBT_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| fq7_saml     | CN=FLQ_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |
| ciz_saml     | CN=CIZ_SSFA_S2SVPS, OU=L... | Jan 1, 2038     | Trusted certificate |

**Step – 3.5:** Navigate to the step “SAML ALM Certificate” to export the HP ALM – SAML certificate

Select the certificate & click on the button “Export” as shown in the screenshot below,

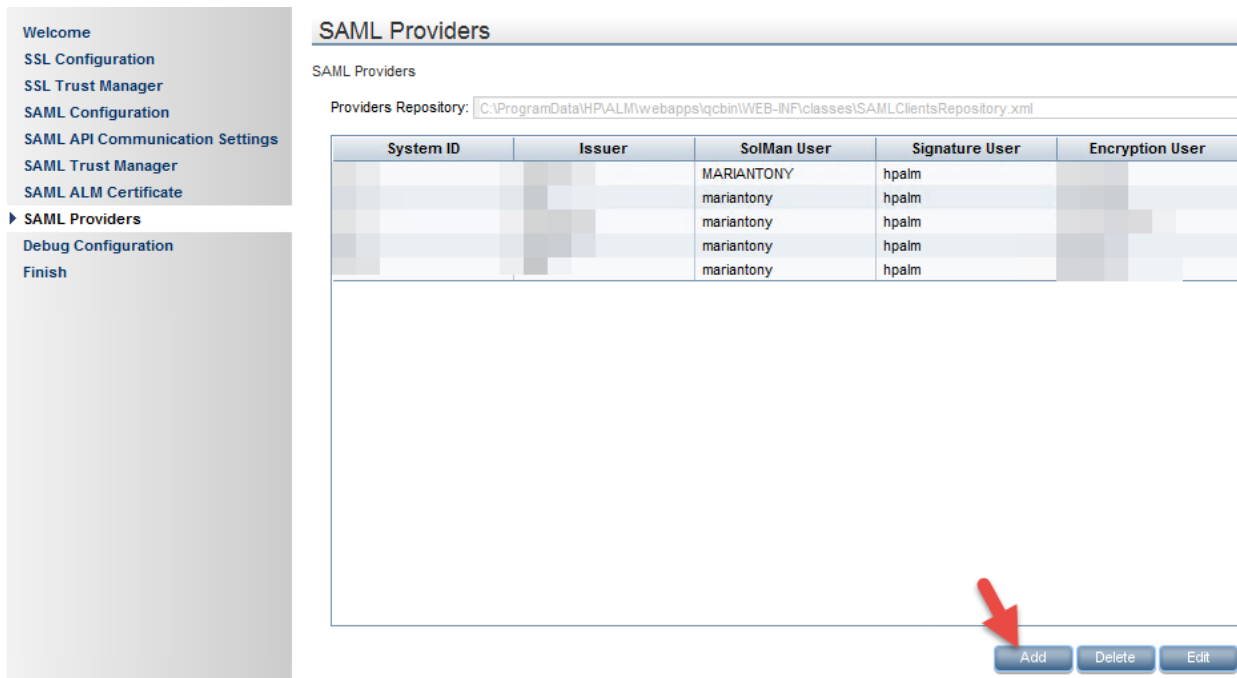


Export the certificate in the local folder,



The exported SAML certificate will be imported in the Solution Manager system in the Step – 4.

**Step – 3.6:** Navigate to “SAML Providers” to assign the Solution Manager System (CIZ) and user, Click on “Add” button,



Provide the following information,

|           |                 |   |
|-----------|-----------------|---|
| System ID | CIZ             | Solution Manager SID  |
| Issuer    | <u>HPEI_CIZ</u> | This is an issuer identify. The same name has to be provided while adding the SMAL authentication |

|                       |                        |   |
|-----------------------|------------------------|---|
| Solution Manager User | SM_HPCOM/<br>HPCOMUSER | The Technical User created for SAML authentications               |
| Signature User        | hpalm                  | This would be filled by default                                   |
| Encryption User       | ciz_saml               | Choose the SAML Alias Name which you had provided in the Step – 5 |

**SAML Provider**

System ID: CIZ

Issuer: HPEI\_CIZ

Solution Manager User: MARIANTONY

Signature User: hpalm

Encryption User: ciz\_saml

OK Cancel

Confirm the SAML provider in the confirmation popup,

**Info**

Is System ID=CIZ, Issuer=HPEI\_CIZ, Solution Manager User=MARIANTONY, Signature User=hpalm, Encryption User=ciz\_saml correct?

Yes No

Make sure the “SAML Provider” is added in the list,

## SAML Providers

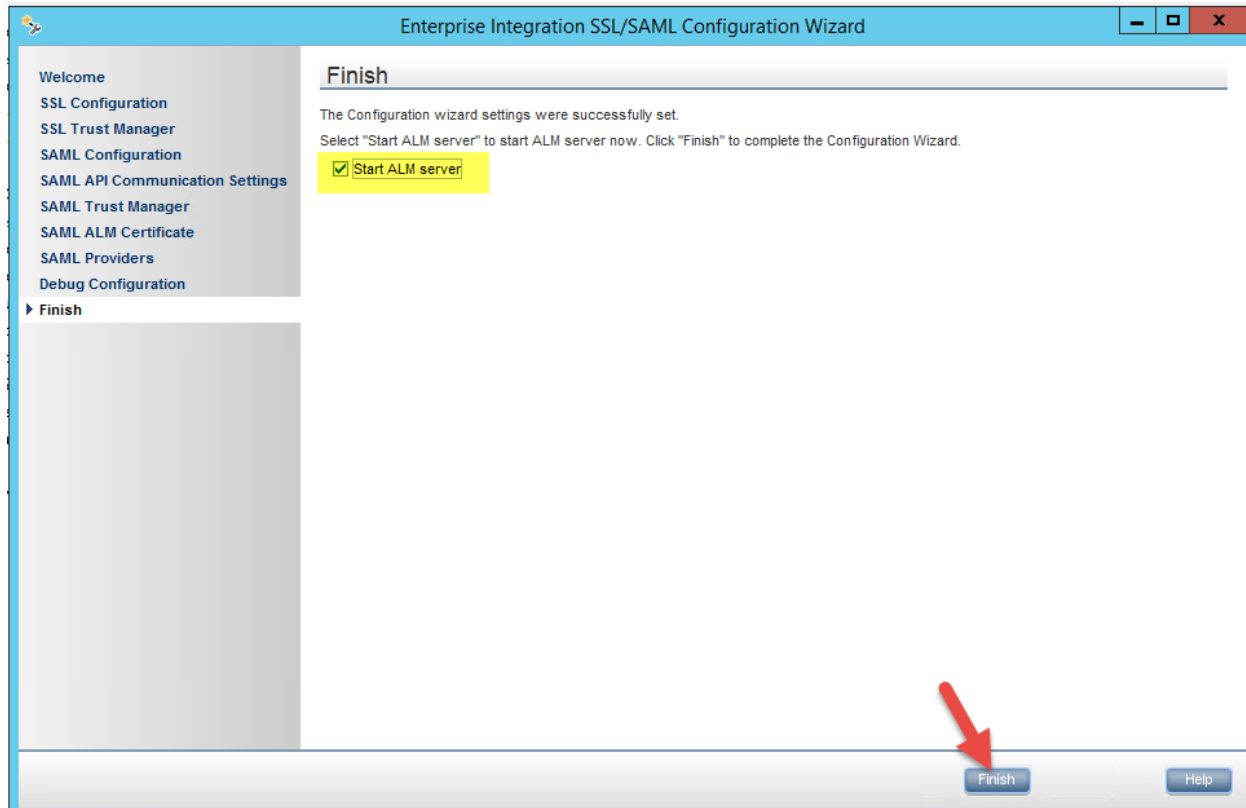
SAML Providers

Providers Repository: C:\ProgramData\HPIALM\webapps\qcbn\WEB-INF\classes\SAMLClientsRepository.xml

| System ID | Issuer    | SoIMan User | Signature User | Encryption User |
|-----------|-----------|-------------|----------------|-----------------|
| FQ7       | HPEI_FQ7  | MARIANTONY  | hpalm          | fq7_saml        |
| FL7       | HPEI      | mariantony  | hpalm          | fl7_saml2       |
| FA7       | HPEI_BENU | mariantony  | hpalm          | fa7_saml_new    |
| FBT       | HPEI_FBT  | mariantony  | hpalm          | fbt_saml        |
| FLQ       | HPEI      | mariantony  | hpalm          | flq_saml        |
| CIZ       | HPEI_CIZ  | MARIANTONY  | hpalm          | ciz_saml        |

**Step – 3.7:** Navigate to the “Finish” step,

Choose “Start ALM Server” to restart the server for the aforementioned setting to take effect,



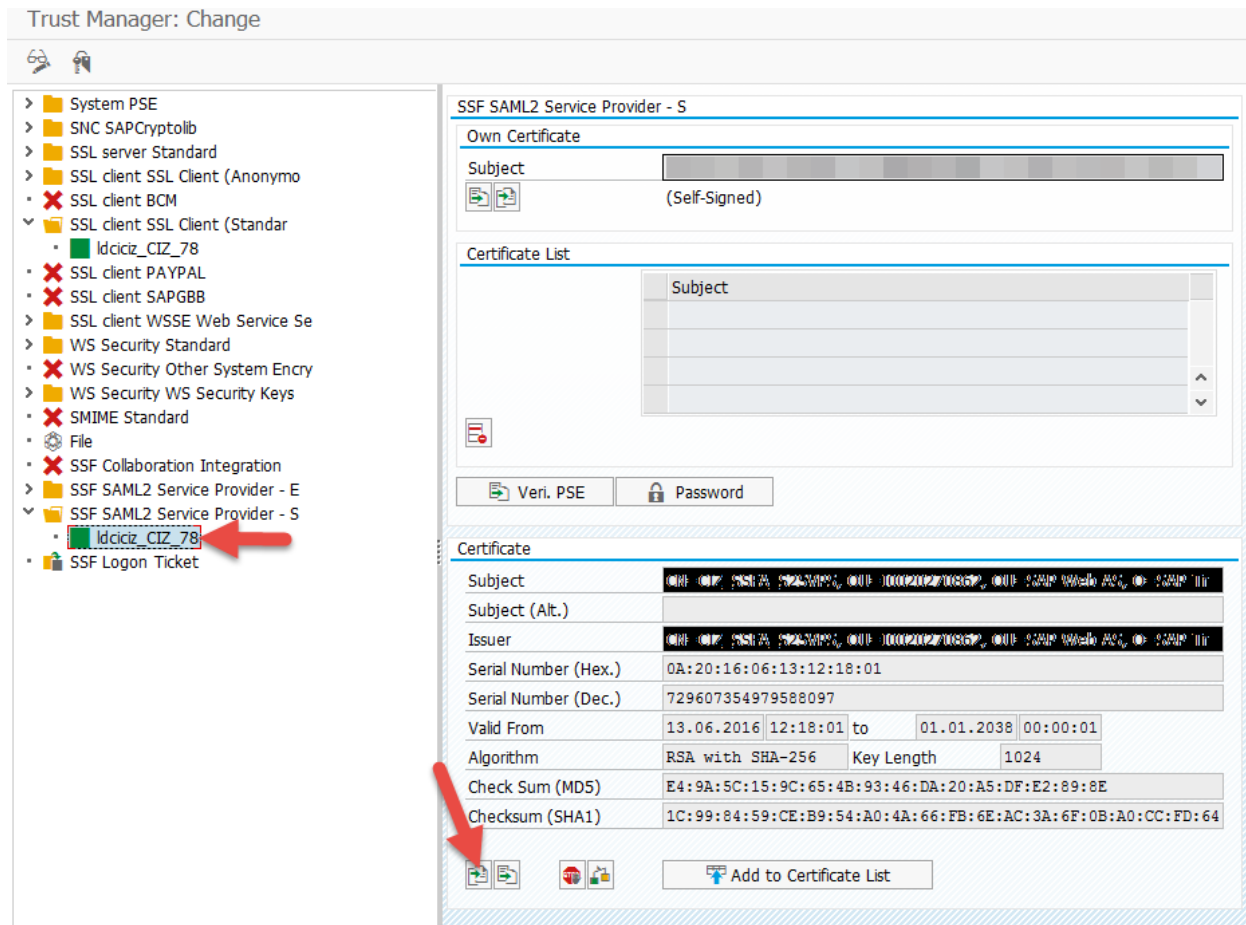
This would restart the server.

## 5. Upload the Certificate in Solution Manager System

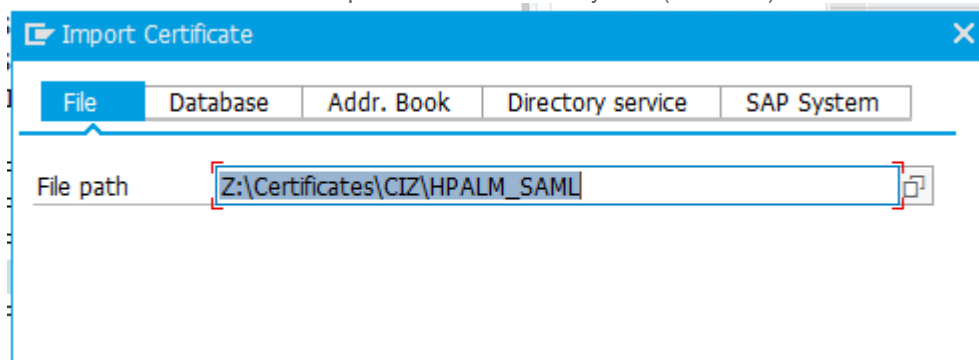
**Step 4.1:** Launch the STRUST Transaction & choose the node “SSF SAML2 Service Provider – S (Standard)”

Go to the “EDIT” mode & click on the Import button as shown in the screenshot below,






Choose the SAML Certificate exported in the HPALM system (in the 3.5)




Once the certificate is imported, click on the “Add to Certificate List” button. This would be added in the “Certificate List”. Please refer the below screenshot,


**SSF SAML2 Service Provider - S**



**Own Certificate**

Subject  (Self-Signed)


**Certificate List**


 Subject  
CN=SAP, OU=SAP, O=SAP, L=SAP, SP=SAP, C=IL





 Veri. PSE  Password


**Certificate**

Subject 

Subject (Alt.) 

Issuer 

Serial Number (Hex.) 





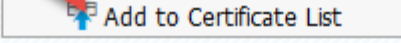
Serial Number (Dec.) 

Valid From 08.12.2015 11:40:40 to 25.04.2019 11:40:40

Algorithm RSA with SHA-1 Key Length 1024

Check Sum (MD5) 49:53:BD:FA:54:DE:9B:63:0F:1A:D7:25:BB:08:59:48

Checksum (SHA1) A DD:E2:E1:31:85:85:B7:59:A0:AA:93:22:80:0B:F5:4F:A9:85:CB

Save the STRUST transaction.

## 6. Add and Enable the HP ALM Trusted Provider

**Step 5.1:** Launch the transaction SAML2 & launch the “Trusted Providers” Tab. (This would launch the “SAML2 Configuration” in the web browser)

## SAML 2.0 Configuration of ABAP System: CIZ/001

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Identity Providers Edit Save Cancel Disable Add Remove

| Active | Default | Name | Alias |
|--------|---------|------|-------|
|        |         |      |       |
|        |         |      |       |
|        |         |      |       |
|        |         |      |       |
|        |         |      |       |

Change the Trusted Provider to “Security Token Services” & click on “Add – Manually”

## SAML 2.0 Configuration of ABAP System: CIZ/001

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Security Token Services Edit Save Cancel Disable Add Remove

Manually  
Upload Metadata File

| Active | Name |
|--------|------|
|        |      |
|        |      |
|        |      |
|        |      |
|        |      |

**Step 5.2:** Provide the name of the Trusted Security Token Service.

**IMPORTANT:** This name has to be the same when you had provided in the step – 3.6. The name we had provided in this blog is (HPEI\_CIZ)

## SAML 2.0 Configuration

**New Trusted Security Token Service**

1 Provider Name 2 Signature and Encryption 3 Endpoints

< Previous Next > Finish Cancel

\* Name: HPEI\_CIZ

**Step 5.3:** Launch the next step “Signature and Encryption”

In this step, the “Primary Signing Certificate” needs to be assigned with the HPALM SAML certificate.  
 →To do this click on the browser button & choose the HP ALM SAML certificate you had uploaded in the step – 3.5.

**SAML 2.0 Configuration**

**New Trusted Security Token Service**

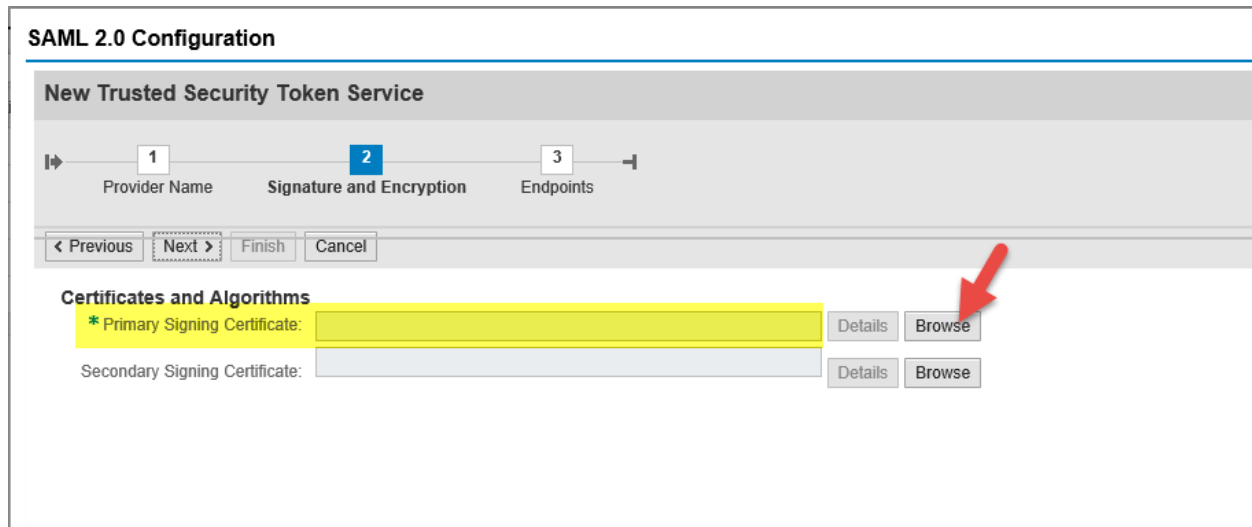
1 Provider Name      2 Signature and Encryption      3 Endpoints

< Previous    Next >    Finish    Cancel

**Certificates and Algorithms**

\* Primary Signing Certificate:  Details Browse

Secondary Signing Certificate:  Details Browse



→Upload the HPALM SAML certificate, in the popup window as shown below,

**SAML 2.0 Configuration**

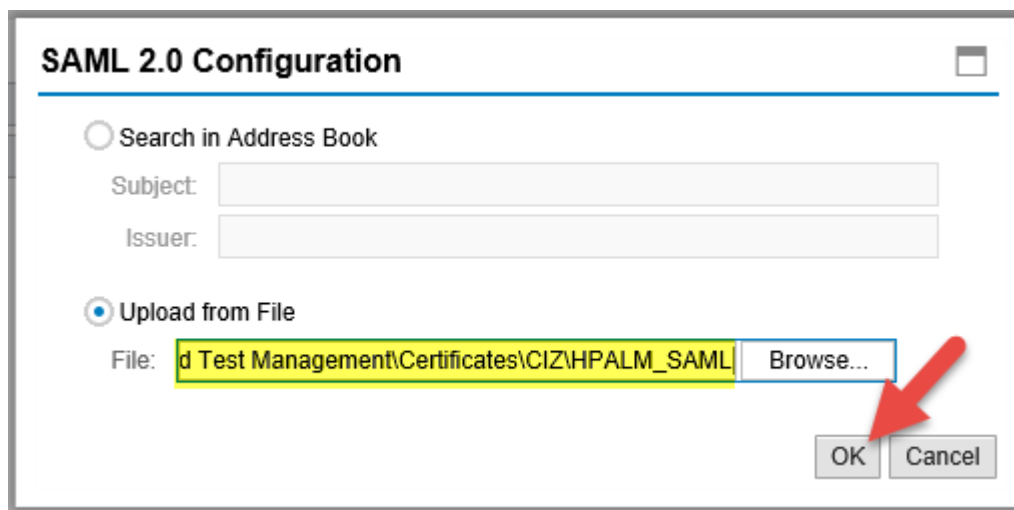
☐ Search in Address Book

Subject:

Issuer:

☒ Upload from File

File:  Browse... OK Cancel



**SAML 2.0 Configuration**

**New Trusted Security Token Service**

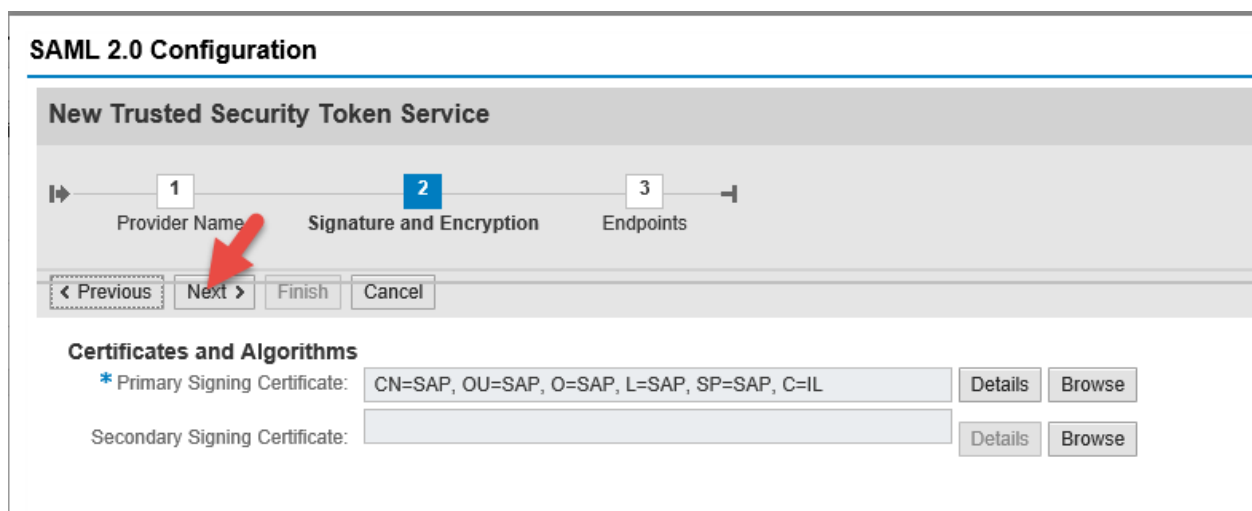
1 Provider Name      2 Signature and Encryption      3 Endpoints

< Previous    Next >    Finish    Cancel

**Certificates and Algorithms**

\* Primary Signing Certificate: CN=SAP, OU=SAP, O=SAP, L=SAP, SP=SAP, C=IL Details Browse

Secondary Signing Certificate:  Details Browse



Once you are done with assigning the HP ALM certificate, navigate to the next step,

**Step 5.4:** Navigate to the next step & click on “Finish” button.


→ Do not change anything in this step

→ While creating the Trusted Provider you might get an error “New trusted provider cannot be saved. The corresponding PSE is locked by user MARIANTONY” (like the error mentioned below in the screenshot)

**SAML 2.0 Configuration**

---

**New Trusted Security Token Service**

 New trusted provider can not be saved. The corresponding PSE is locked by user MARIANTONY

1 2 3

Provider Name Signature and Encryption Endpoints

< Previous Next > Finish Cancel

**Endpoints**

---

**SAML 2.0 Configuration**

---

**New Trusted Security Token Service**

1 2 3

Provider Name Signature and Encryption Endpoints

< Previous Next > Finish Cancel

**Endpoints**

Add Remove

| Location URL | Metadata Exchange (MEX) URL |
|--------------|-----------------------------|
|              |                             |
|              |                             |
|              |                             |

#### How to resolve this error?

- This means the STRUST is launched in an EDIT mode
- Exit the STRUST transaction
- Click on “Finish button” to create a Trusted Provider

This activity would create a Trusted Provider

## SAML 2.0 Configuration of ABAP System: CIZ/001

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Security Token Services

| Active                              | Name     |
|-------------------------------------|----------|
| <input checked="" type="checkbox"/> | HPEI_CIZ |
|                                     |          |
|                                     |          |
|                                     |          |
|                                     |          |

**Details of Security Token Service "HPEI\_CIZ"**

Supported SAML Versions: ☒ SAML 1.1 ☒ SAML 2.0

Assertion Validity (holder-of-key):  minutes

**Step 5.5:** Enable the Trusted Provider.

1. Click on the EDIT button
2. Choose the "Identity Federation" Tab
3. Add the format "Unspecified"
4. Choose Supported SAML Versions as "SAML 1.1"
5. Save it

Refer the below screenshot for more information,

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Security Token Services

| Active                              | Name     |
|-------------------------------------|----------|
| <input checked="" type="checkbox"/> | HPEI_CIZ |
|                                     |          |
|                                     |          |
|                                     |          |
|                                     |          |

**Details of Security Token Service "HPEI\_CIZ"**

Supported SAML Versions: ☒ SAML 1.1 ☐ SAML 2.0

Assertion Validity (holder-of-key):  minutes

Endpoints **Identity Federation** Signature and Encryption

**Supported NameID Formats**

| Name        |
|-------------|
| Unspecified |
|             |
|             |
|             |
|             |
|             |

**Details of NameID Format "Unspecified"**

User ID Source:  User ID Mapping Mode:

→After the save you will be able to see the "Enable" button. Enable the Trusted Provider

**SAML 2.0 Configuration of ABAP System: CIZ/001**

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Security Token Services

| Active                   | Name     |
|--------------------------|----------|
| <input type="checkbox"/> | HPEI_CIZ |
|                          |          |
|                          |          |
|                          |          |
|                          |          |

**Details of Security Token Service "HPEI\_CIZ"**

Supported SAML Versions: ☒ SAML 1.1 ☐ SAML 2.0

Assertion Validity (holder-of-key):  minutes

This would activate the Trusted Provider,

**SAML 2.0 Configuration of ABAP System: CIZ/001**

Local Provider **Trusted Providers** Policies Name ID Management

**List of Trusted Providers**

Show: Security Token Services

| Active                              | Name     |
|-------------------------------------|----------|
| <input checked="" type="checkbox"/> | HPEI_CIZ |
|                                     |          |
|                                     |          |
|                                     |          |
|                                     |          |

**Details of Security Token Service "HPEI\_CIZ"**

Supported SAML Versions: ☒ SAML 1.1 ☐ SAML 2.0

Assertion Validity (holder-of-key):  minutes

## Copyright

© Copyright 2011 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

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

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Oracle Corporation.

JavaScript is a registered trademark of Oracle Corporation, used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.