HPE Universal SLA Manager

Smart Card Configuration Guide

Release 4.3
Version: 1.0

Hewlett Packard
Enterprise

Legal Notices

Warranty

The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

License requirement and U.S. Government legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notices

Trademark notices

Adobe®, Acrobat® and PostScript® are trademarks of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a trademark of Oracle and/or its affiliates.

Microsoft®, Internet Explorer, Windows®, Windows Server®, and Windows NT® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

EnterpriseDB® software and Postgres Plus® database are registered trademarks of EnterpriseDB Corporation in the USA and in several other countries

UNIX® is a registered trademark of The Open Group.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

Red Hat® is a registered trademark of the Red Hat Company.

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

Contents

Legal Notices 2

Contents 3

Table of Figures .... **Error! Bookmark not defined.**

Preface 4

Intended Audience 4
Abbreviations and Acronyms 4
Software Versions 5
Associated Documents 5
Reference Documents 5
Typographic Conventions 6
Symbols used in this Guide 7
Support 7

Chapter 1 Apache HTTPD Installation 8

1.1 PCRE Installation 8
1.2 OPEN SSL Installation 8
1.3 HTTPD Installation 9

Chapter 2 Certification 11

2.1 Generate Self-signed Certificate 11
2.1.1 Generate Self-signed Root CA 11
2.1.2 Generate Self-signed Server Certificate 12
2.1.3 Generate Self-signed User Certificate 12
2.2 Import Self-signed Certificate 13

Chapter 3 Apache HTTPD Configuration 14

3.1 Enabled modules 14
3.2 Virtual Host configuration 14
3.3 Others 16
3.3.1 Specify HTTPS listener port as 443 16
3.3.2 Turn on rewrite engine 16

Chapter 4 JBoss/Tomcat AJP Configuration 17

Chapter 5 Trust Login 18

5.1 USLAM_SERVICE 18
5.2 BO 18
5.3 MyUSLAM 19

Preface

This guide is designed to be used as smart card configuration manual for the HPE Universal SLA Manager that is used to manage Service Level Agreements.

This document also contains information about how to install and configure smart card server side environment, including Apache HTTPD server installation & configuration, CRL setting, JBoss side AJP configuration, how to generate self-signed certificate.

Intended Audience

This document is intended for the following user:

- **HPE USLAM Administrator.**

Abbreviations and Acronyms

The following table describes the abbreviations and acronyms used in this document.

Abbreviation	Description
BO	SAP Business Objects
BODS	SAP Business Objects Data Services
BOE	SAP BusinessObjects Business Intelligence platform
BIAR	Business Intelligence Archive
CMS	Central Management Server
CI	Configuration Item
ID	Identifier
EDB PPAS	Enterprise DB Postgres Plus Advanced Server
ETL	Extract, Transform, and Load
KPI	Key Performance Indicator
LTU	License To Use
SLI	Service Level Indicator
SLA	Service Level Agreement
SLO	Service Level Objective
SLM	Service Level Management
SD	Service Definition

SI	Service Instance
SNMP	Simple Network Management Protocol
SM	Service Manager
TTR	Time To Repair
USLAM	Universal Service Level Agreement Manager

Software Versions

The software versions referred to in this document are as follows:

Software	Version
HPE Universal SLA Manager	V4.3
Red Hat Linux 6.5 64-bit	6.5 (*)
Apache HTTPD	2.4.20
OPEN SSL	1.0.2h
PCRE	8.39

(*) Specified servers versions have been successfully tested by Hewlett-Packard. Incremental releases of the specified versions defined by the last number in the server name will be supported as they are made available, but may not have been tested by Hewlett-Packard. Exceptions in support will be documented.

Associated Documents

A list of existing HPE Universal SLA Manager documents is given below for your reference:

- HPE Universal SLA Manager Release Notes
- HPE Universal SLA Manager Support Matrix
- HPE Universal SLA Manager User Guide

Reference Documents

A list of reference documents is given below for your reference:

Document Title	URL
Apache HTTPD Manual	https://httpd.apache.org/docs/2.4/
OPEN SSL	https://www.openssl.org/
PCRE	http://pcre.org/

Typographic Conventions

This document uses the following conventions to identify special information:

Convention	Information Type/Example
[ ] (square brackets)	Interface components requiring user actions e.g. Buttons. Ex: Click [Finish] to complete the Import wizard.
( ) [round brackets]	Supplementary information Ex: Configuration Item (CI).
Bold type	Fields names, menus, window pane names Ex of menus: Admin → Service Level Management → Repository.
Italic type	Important information and/or concepts. Ex: The output is an .XML file.

Symbols used in this Guide

Symbols	Information
📄	Note Draws your attention to additional information about a software function/feature.
📢	Important Draws your attention to important information regarding the proper usage of a software function/feature.
⚠	Caution Draws your attention to an important warning.

Support

Please visit our HPE Software Support Online Web site at: https://softwaresupport.hpe.com/ for contact information, and details about HPE Software products, services, and support.

The Software support area of the Software Web site includes the following:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information.

Chapter 1
Apache HTTPD Installation

This chapter will describe how to install Apache HTTPD on Linux server. Including download source package, compile and build this HTTPD to support https.

1.1 PCRE Installation

Before install HTTPD we must make sure PCRE is installed.

1. Download PCRE package from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.39.tar.gz
2. Unpack into /opt/pcre

```
$gzip –d pcre-8.39.tar.gz

$tar xvf pcre-8.39.tar
```

3. Compile it with a prefix and install it

```
$/opt/pcre/configure --prefix=/usr/local/pcre

$make

$make itstall
```

1.2 OPEN SSL Installation

Before install HTTPD we must make sure OPEN SSL is installed.

1. Download Open SSL package from https://www.openssl.org/source/openssl-1.0.2h.tar.gz
2. Unpack into /opt/openssl

```
$gzip –d openssl-1.0.2h.tar.gz

$tar xvf openssl-1.0.2h.tar
```

3. Compile it with a prefix and install it

```
$/opt/openssl/configure --prefix=/usr/local/openssl

$make
```

```
$make itstall
```

1.3 HTTPD Installation

1. Download Apache HTTPD from http://ftp.wayne.edu/apache//httpd/httpd-2.4.20.tar.gz
2. Unpack into /opt/httpd

```
$gzip –d httpd-2.4.20.tar.gz

$tar xvf httpd-2.4.20.tar
```

3. Download APR and APR-Util

   http://mirror.cc.columbia.edu/pub/software/apache//apr/apr-1.5.2.tar.gz

   http://mirror.cc.columbia.edu/pub/software/apache//apr/apr-util-1.5.4.tar.gz

4. Unpack APR and APR-Util into /opt/httpd/srclib/apr and /opt/httpd/srclib/apr-util

```
$gzip –d apr-1.5.2.tar.gz

$tar xvf apr-1.5.2.tar

$gzip –d apr-util-1.5.4.tar.gz

$tar xvf apr-util-1.5.4.tar
```

5. Compile it

```
$/opt/httpd/configure --prefix=/opt/apache2 --with-pcre=/usr/loca/pcre --with-ssl=/usrl/local/openssl

$make

$make install
```

Chapter 2
Certification

This chapter describe how to generate self-signed certification used for Apache HTTPD server.

These certification include Root CA, Server side certification, Client side certification.

For those browse trusted Certificate Authority signed certification is not under our scope. You need contact them about how to generate those certification.

2.1 Generate Self-signed Certificate

Sometime for test purpose or development, we can just use self-signed certificate.

This kind of certificate is not trusted by web browser. It means if we use self-signed certificate, we need import these certificate into Browser as trusted one first.

2.1.1 Generate Self-signed Root CA

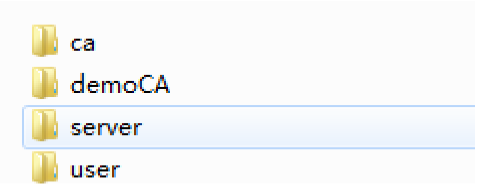
Before you generate certificate, you must sure openssl is installed on your PC. And it is set into environment PATH.

And below command is executed on Windows PC. If you want to use Linux server to do, you need do some minor adjustment.

Create a directory certificate which contains ca, demoCA, server and user four sub directory. Just like below screenshot. And demoCA contains another folder newcert and a file serial.

Here you can also use cert.zip to create such kind of folder.

cert.zip



By using below command to generate Root CA

```
openssl genrsa -out ca\ca.key

openssl req -new -key ca\ca.key -out ca\ca.csr
openssl x509 -req -days 365 -in ca\ca.csr -out ca\ca.crt -signkey ca\ca.key

openssl x509 -inform PEM -in ca\ca.crt -outform DER -out ca\ca.der
```

2.1.2 Generate Self-signed Server Certificate

Below command is used generate certificate used for GUI side application.

And you can also use similar command to generate certificate used for BO and MyUSLAM side application.

⚠ The FQDN must match your server IP address or domain name.

```
openssl genrsa -des3 -out server\gui.key

openssl req -new -key server\gui.key -out server\gui.csr

openssl ca -in server\gui.csr -cert ca\ca.crt -keyfile ca\ca.key -out server/gui.crt

copy server\gui.key server\gui.key.org

openssl rsa -in server\gui.key.org -out server\gui.key
```

2.1.3 Generate Self-signed User Certificate

Below command is used generate certificate used for GUI side application.

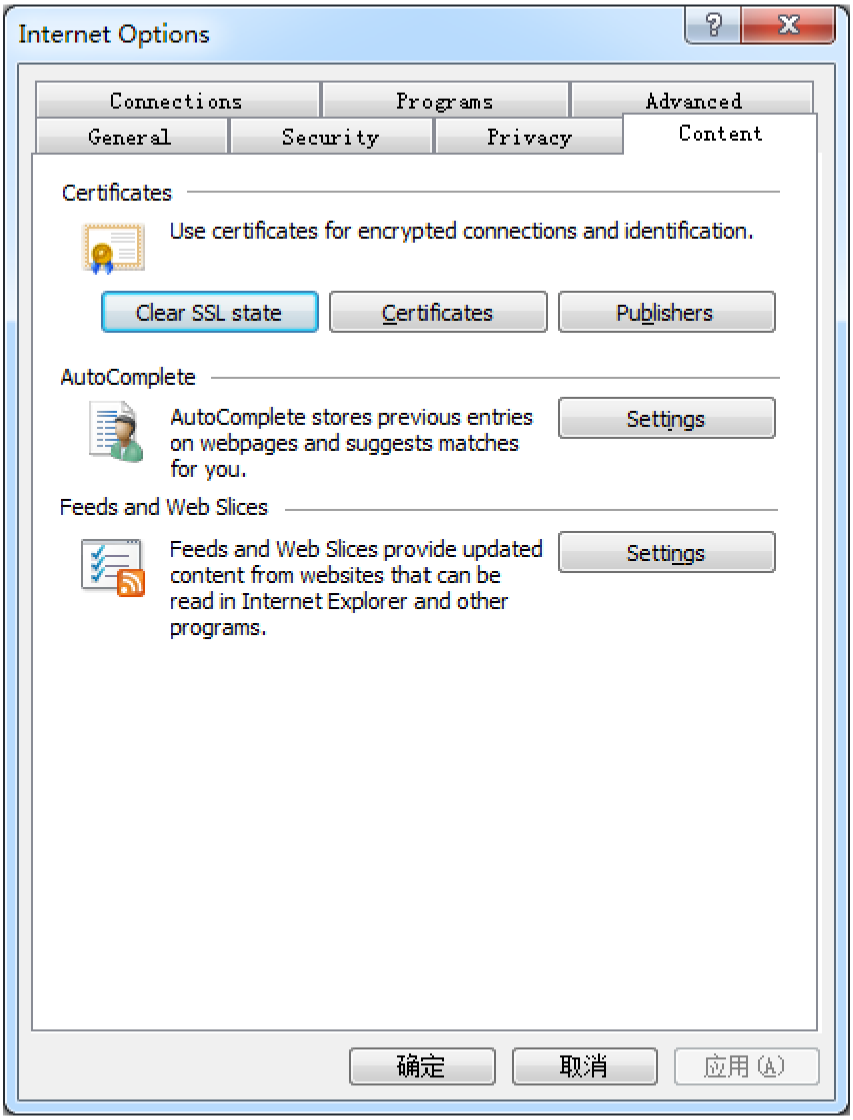
And you can also use similar command to generate certificate used for BO and MyUSLAM side application.

```
openssl genrsa -des3 -out user\user.key

openssl req -new -key user\user.key -out user\user.csr

openssl ca -in user\user.csr  -cert ca\ca.crt -keyfile ca\ca.key -out user\user.crt

openssl pkcs12 -export -clcerts -in user\user.crt -inkey user\user.key -out user\user.p12

openssl x509 -inform PEM -in user\user.crt -outform DER -out user\user.der
```

2.2 Import Self-signed Certificate

For self-signed certificate, they are not trusted by browser, we need import them as trusted one.

1. Open IE Internet Options-Certificates



Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

2. Import server.crt into Trusted Root Certification Authorities
3. Import user.p12 into Personal

Chapter 3
Apache HTTPD Configuration

3.1 Enabled modules

Below modules must be enabled

Modules
ssl_module modules/mod_ssl.so
setenvif_module modules/mod_setenvif.so
rewrite_module modules/mod_rewrite.so
proxy_http_module modules/mod_proxy_http.so
proxy_express_module modules/mod_proxy_express.so
proxy_module modules/mod_proxy.so
headers_module modules/mod_headers.so
env_module modules/mod_env.so
authz_user_module modules/mod_authz_user.so

3.2 Virtual Host configuration

```
<VirtualHost gui.xxx.com:443>

  SSLEngine on

  ServerName gui.xxx.com:443

  SSLCertificateFile "${SRVROOT}/cert/server/gui.crt"

  SSLCertificateKeyFile "${SRVROOT}/cert/server/gui.key"

  SSLVerifyClient      optional

  SSLVerifyDepth       2

  SSLCACertificateFile "${SRVROOT}/cert/ca/ca.crt"
  RewriteCond %{SSL:SSL_CLIENT_VERIFY} !^SUCCESS$

  RewriteRule .* /help/ssl-client-auth-required.html [L]



  RewriteCond     %{SSL:SSL_CLIENT_S_DN_CN} =""

  RewriteRule .* /help/ssl-client-auth-required.html [L]



  RequestHeader set SSL_CLIENT_S_DN "%{SSL_CLIENT_S_DN}s"

  RequestHeader edit SSL_CLIENT_S_DN (.*)CN=(.*)\\,OU(.*) $2



  ProxyPass "/sla-repository" ajp://15.107.17.90:9009/sla-repository

  ProxyPassReverse "/sla-repository" ajp://15.107.17.90:9009/sla-repository



  DocumentRoot "${SRVROOT}/htdocs"

  CustomLog "${SRVROOT}/logs/ssl_request.log" "%t %h %{SSL_PROTOCOL}x
%{SSL_CIPHER}x \"%r\" %b"

        <Directory "${SRVROOT}/htdocs">

                Options Indexes Includes FollowSymLinks

                AllowOverride AuthConfig Limit FileInfo

                Require all granted

        </Directory>

</VirtualHost>
```

We need copy gui.crt, gui.key and ca.crt into some directory where Apache HTTPD can read them.

help/ssl-client-auth-required.html is an error page, when client side certificate verify failed. This page will be displayed.

We set SSL_CLIENT_S_DN into http header and pass this value to application server. This variable contains user profile information.

RewriteRule and ProxyPassReverse will forward http request to backend application server.

3.3 Others

3.3.1 Specify HTTPS listener port as 443

```
Listen 443
```

3.3.2 Turn on rewrite engine

```
RewriteEngine On
```

3.3.3 OCPS Status

Please refer to HTTPD doc for detail about OCPS Status

https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html

3.3.4 Revocation file

Please refer to HTTPD doc for detail about revocation file

https://httpd.apache.org/docs/current/mod/mod_ssl.html#sslcarevocationfile

Chapter 4
JBoss/Tomcat AJP Configuration

This chapter will describe how to configure USLAM Server, MyUSLAM and BO working with AJP mode.

By default AJP mode is enable on these 3 application servers. We just need confirm the AJP port is same as configuration in Apache HTTPD.

Server	Location
BO	${TOMCAT_HOME}/conf/server.xml
USLAM_SERVICE	${USLAM_SERVICE_HOME}/jboss/server/default/deploy/jbossweb.sar/server.xml
MYUSLAM	${MYUSLAM_HOME}/jboss/standalone/configuration/standalone.xml

We can search ajp to find related configuration and change port number.

BO&USLAM_SERVICE

```
    <Connector protocol="AJP/1.3" port="8009" address="${jboss.bind.address}"

      redirectPort="8443" />
```

MyUSLAM

```
<socket-binding name="ajp" port="8009"/>
```

Chapter 5 Trust Login

On application side we also need enable Trust Login to support Smart Card

5.1 USLAM_SERVICE

We can turn on Trust Login mode on GUI setting page.

We shall select Trust-login mode, and provide customized login name method and display name method.

And USLAM also prepared predefined TrustLogin implementation.

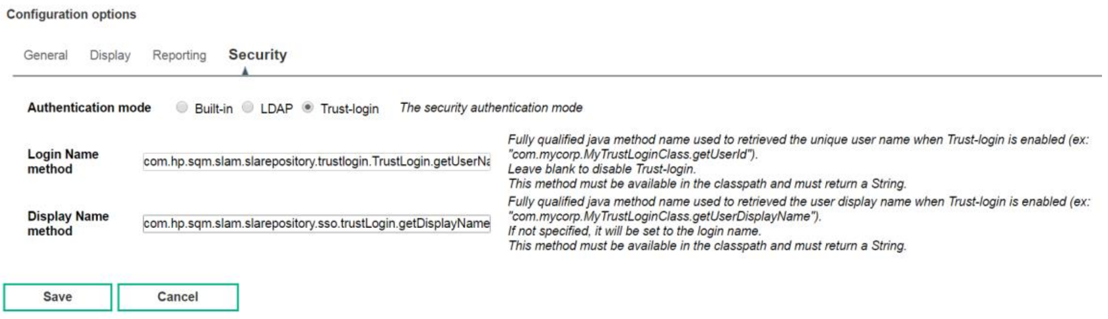
You can set as below.

com.hp.sqm.slam.slarepository.trustlogin.getUserName

com.hp.sqm.slam.slarepository.trustlogin.getDisplayName

This TrustLogin just simply fetch UserName and DisplayName from

HTTP Header - SSL_CLIENT_S_DN



Authentication mode ○ Built-in ○ LDAP ● Trust-login *The security authentication mode*

Login Name method: com.hp.sqm.slam.slarepository.trustlogin.TrustLogin.getUserNa

Fully qualified java method name used to retrieved the unique user name when Trust-login is enabled (ex: "com.mycorp.MyTrustLoginClass.getUserId"). Leave blank to disable Trust-login. This method must be available in the classpath and must return a String.

Display Name method: com.hp.sqm.slam.slarepository.sso.trustLogin.getDisplayName

Fully qualified java method name used to retrieved the user display name when Trust-login is enabled (ex: "com.mycorp.MyTrustLoginClass.getUserDisplayName"). If not specified, it will be set to the login name. This method must be available in the classpath and must return a String.

5.2 BO

The trust login with header can be configured with the following steps.

1. Access the CMC URL http://localhost:8080/BOE/CMC with a browser. Navigate to CMC > Authentication > Enterprise
2. Scroll down to the bottom and check the box for Trusted Authentication is enabled
3. Click the button for New Shared Secret
4. Click the button for Download Shared Secret
5. Save the TrustedPrincipal.conf to one of following locations on your application server:
<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\
6. Click Update to save the settings. NOTE: missing this step or doing it out of order results in the following error in KBA 1954424 where trustedprinicpal.conf files are out of synch with the CMS

7. Navigate to C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
8. Create a file named global.properties and add the following information: (Warning: Copy/paste may add a space at the end of the following lines that will break TA SSO)

   ```
   sso.enabled=true
   trusted.auth.user.param=SSL_CLIENT_S_DN
   trusted.auth.user.retrieval=HTTP_HEADER
   ```
9. Restart Tomcat

5.3 MyUSLAM

For MyUSLAM, the Trust Login is not provided in current 4.3.0 release. We will support it in next release.

Chapter 6 Cross Launch

After Trust Login is enabled. USLAM Service can support Cross Launch feature for Agreement Status Snapshot page.

The URL will be like below

http://gui.xxx.com/sla-repository/AgreementsStatusSnapshot.seam?conversationPropagation=begin.agreements-status-snapshot.jpdl&slaId=SLA-Sites-ReportingPeriods&customerId=GreenCafe&refDateStr=20150501&serviceId=Sites_ReportingPeriods

Parameter	Description
slaId	SLA ID
customerId	Customer ID
refDateStr	Reference period stat date
serviceId	Service ID