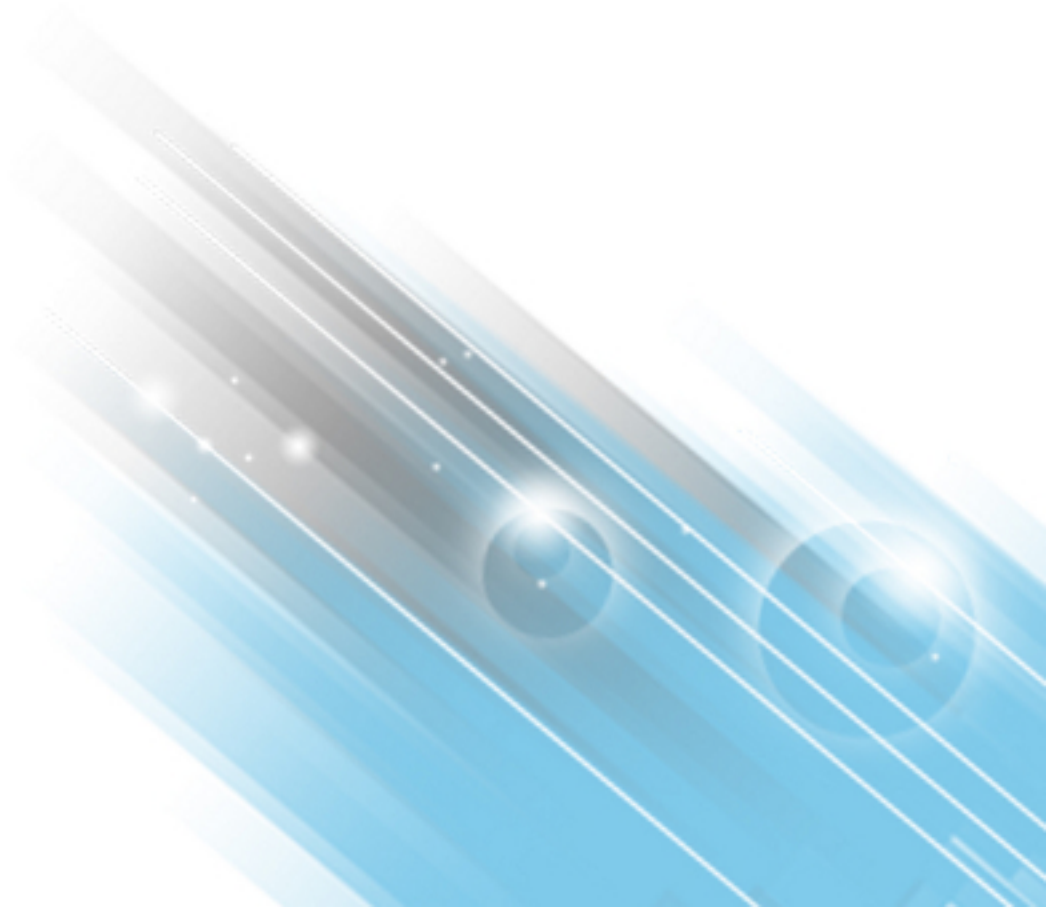


HP ALM

Software Version: 12.01

External Authentication Configuration Guide

Document Release Date: June 2014
Software Release Date: June 2014



Legal Notices

Warranty

The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP 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 Notice

© Copyright 2002 - 2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

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

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered trademark of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

- Chapter 1: External Authentication Overview 7
 - Smart Card Authentication Overview 7
 - Single Sign-On Overview 8
- Chapter 2: External Authentication Roadmap 9
- Chapter 3: Prerequisites 10
 - Configure Web Server as Reverse Proxy 12
- Chapter 4: Web Server Configuration 15
 - Configure Apache for External Authentication 16
 - Configure IIS for External Authentication 16
 - Configure Jetty for External Authentication 17
- Chapter 5: Smart Card Configuration 18
 - Prepare Certificates 19
 - Configure Apache as a Secure Reverse Proxy 20
 - Configure Apache to Require a Client Certificate 21
 - Configure the Apache SSL Proxy Server to Work with Smart Card 22
 - Configure IIS to Work with Smart Card 23
- Chapter 6: Single Sign-On Configuration 24
 - Configure SSO on IIS 25
- Chapter 7: Verification Checklist 28
- Chapter 8: ALM Configuration 29
 - Configure Site Administration 30
 - Verify External Authentication 32
 - Configure Smart Card Authentication for Performance Center 32
 - Configure SSO for Performance Center 34
 - Configure Smart Card Authentication for APIs 35

Configure SSO for APIs	36
Special Configurations for Smart Card Authentication	37
Special Configurations for SSO	38
Configure External Authentication for Remote Machines	39
Chapter 9: Limitations	40
Chapter 10: Troubleshooting	42
Chapter 11: External Authentication Site Parameters	44
Send Documentation Feedback	48

Chapter 1: External Authentication Overview

ALM supports external authentication, where a reverse proxy positioned in front of ALM is configured to support external authentication. Once the user is authenticated by the reverse proxy, the authenticated user details are passed to ALM, which completes the authentication and authorization process.

For example, a user who passes the reverse proxy authentication but does not exist in ALM will be denied access to ALM. A user who passes the reverse proxy authentication but does not have permissions to enter specific parts of ALM, will be denied access to those parts of ALM, such as Site Administration or Lab Management. Otherwise, the login process will complete and the user will enter ALM.

This guide contains information about external authentication systems, such as Smart Card Authentication and Single Sign-on, and how to configure these systems to work with ALM.

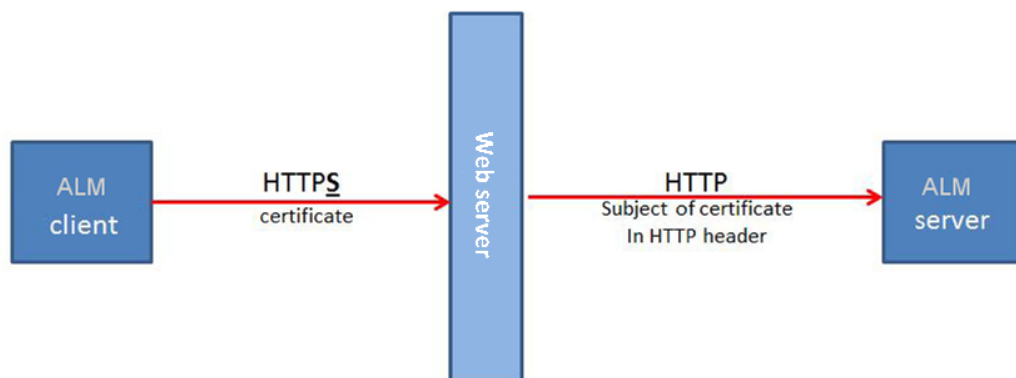
Smart Card Authentication Overview

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates that verify the user's identity and allow access to secure environments. Currently, ALM supports one type of smart card authentication, CAC (Common Access Card).

ALM can be configured to use these certificates in place of the standard model of each user manually entering a user name and password. You can define a method of extracting the user name from the certificate stored on each card or use the system defaults.

When ALM is configured to work with smart cards, users can only log in using a smart card. The option of logging in by manually typing in your user name and password is locked for all users.

The following figure illustrates the smart card authentication topology (the Web server is either Apache or IIS):



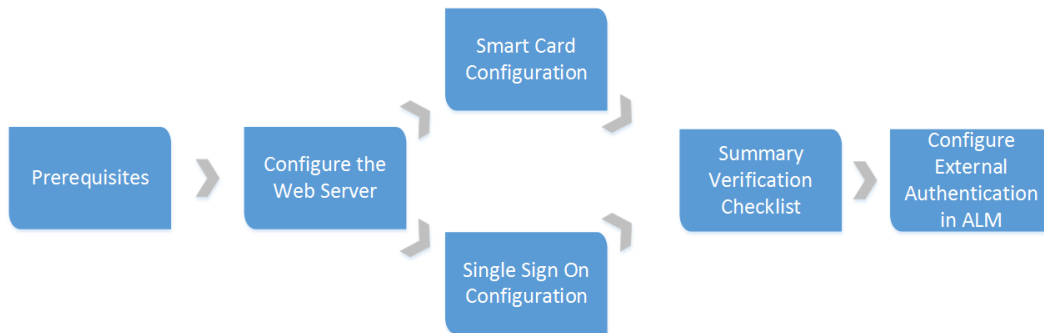
Single Sign-On Overview

Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password to access multiple applications. The process authenticates the user for all the applications to which the user has been given rights. This eliminates further prompts when the user switches applications during a particular session. Currently, ALM supports one type of SSO authentication, SiteMinder.

Note: For HP tools such as UFT, ALM supports only SiteMinder basic authentication.

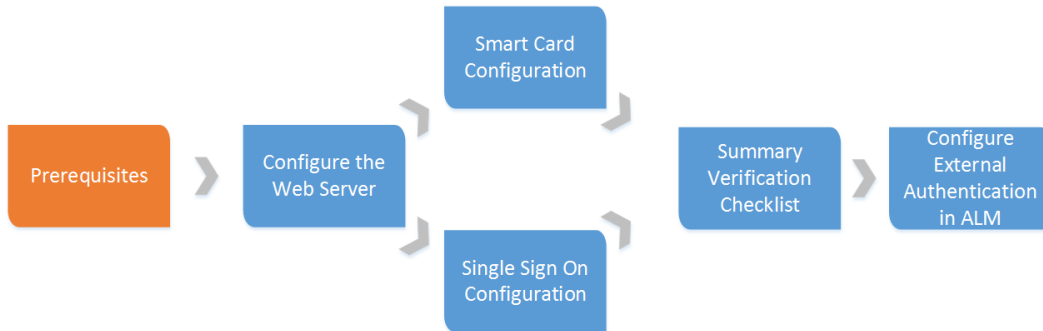
Chapter 2: External Authentication Roadmap

The external authentication roadmap includes the following phases:



Phase	Description
Prerequisites	Gather the information you need to configure external authentication for use with ALM. For details, see "Prerequisites" on page 10 .
Configure the Web Server	Configure the web server, either Apache or IIS, for external authentication. Also, configure Jetty for external authentication. For details, see "Web Server Configuration" on page 15 .
Smart Card Configuration	Configure the web server for smart card authentication. For details, see "Smart Card Configuration" on page 18 .
Single Sign-On Configuration	Configure the web server for single sign-on authentication. For details, see "Single Sign-On Configuration" on page 24 .
Verification Checklist	Verify that all of the necessary steps have been successfully implemented to use external authentication with ALM. For details, see "Verification Checklist" on page 28 .
Configure External Authentication in ALM	Configure ALM to work with external authentication. For details, see "ALM Configuration" on page 29 .

Chapter 3: Prerequisites



1. Ensure that the ALM server is installed and running.
2. Ensure that the web server, either Apache or IIS, is installed and running.

Note: It is recommended to install the web server and the ALM server on separate machines.

3. Configure the web server as a reverse proxy server. For details, see "[Configure Web Server as Reverse Proxy](#)" on page 12.
4. Disable IPv6 stack on the ALM server host using the operating system's network tool. This will improve communication performance between the IPv6 client and the ALM server. (Jetty 5.x does not support IPv6.)
5. Determine how the users will log in to ALM using external authentication (for example, using an email address), and ensure that this information is present in the user details in Site Administration. At the end of this process, the site administrator must be able to log in to ALM using external authentication. Only then can other users log in to ALM using external authentication.
6. If you are using LDAP, import the LDAP users.

Recommended ALM configuration:

For the list of supported system environments, refer to the *Readme*.

Note: The supported environment information in the *Readme* is accurate for the ALM 12.00 release, but there may be subsequent updates. For the most up-to-date supported environments, refer to the HP Software Web site using the following URL: http://www.hp.com/go/TDQC_SysReq.

Web Server system requirements:

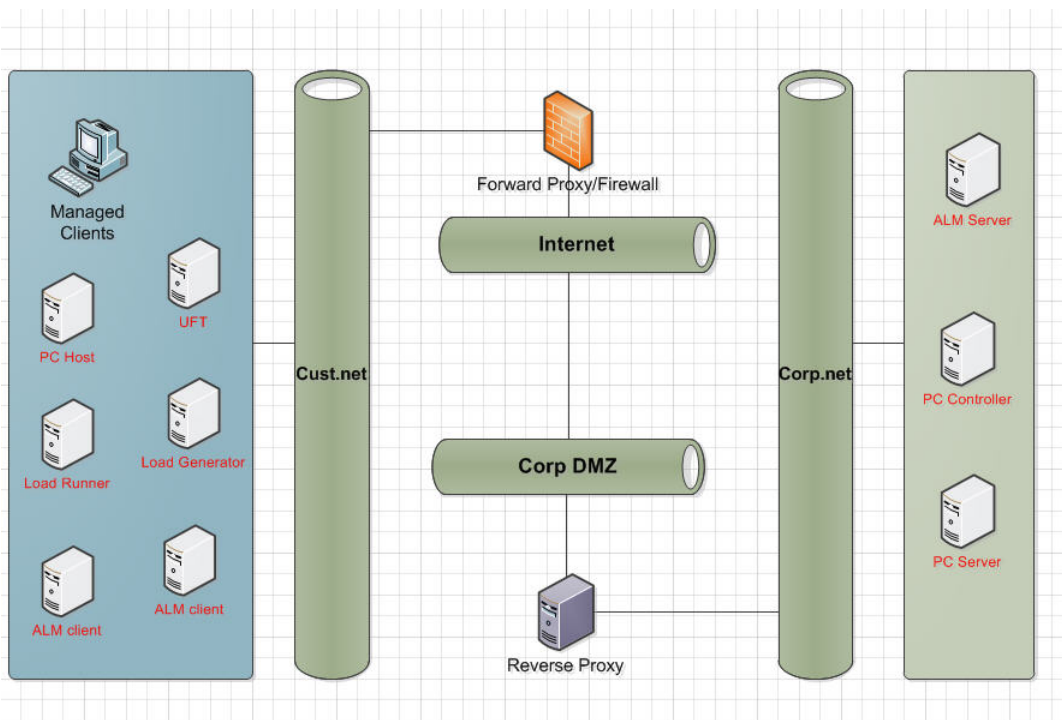
Operating System	Web Server
Windows	<ul style="list-style-type: none"> IIS 7.5 Apache 2.2 or later
Linux	Apache 2.4 or later

Make sure you have the following information about the host on which you are configuring smart card authentication or SSO: Server host name, server operating system type, and web server type (IIS or Apache).

Note: We recommend configuring the firewall so the only servers allowed to log in to the Jetty port are the reverse proxy's machine (IIS or Apache) or the PC server machine.

Segmented networks configuration:

ALM is certified in the following topology:



When ALM clients are located in a different network segment from the ALM server and require a forward proxy to access outside the segment, the ALM server is behind the reverse proxy or load balancer, and both proxies require Basic or NTLM authentication, following are the requirements for the proxies:

- The forward proxy and the reverse proxy must return different error codes.
- The forward proxy must support the 407 error code and the reverse proxy must support the 401 error code.
- The forward proxy must pass the authentication headers forward.

Note: You may experience problems if your topology does not meet these requirements.

ALM was certified with the following forms of authentication:

- Forward proxy: NTLM and Basic.
- Reverse proxy: Client authentication (in a Smart Card environment) and Basic authentication.

Configure Web Server as Reverse Proxy

To enhance the security of your ALM deployment, it is recommended to place the ALM server behind a secure reverse proxy, either an Apache or IIS web server. Such configuration is also required to support external authentication.

To integrate ALM with an IIS Web server, see HP Software Self-solve knowledge base article [KM1383166](http://h20230.www2.hp.com/selfsolve/document/KM1383166) (<http://h20230.www2.hp.com/selfsolve/document/KM1383166>). (Requires HP Passport sign-in credentials.)

To integrate ALM with an Apache Web server, you configure the Apache Web server to redirect requests to the ALM Application Server. You configure the Apache Web server to work in proxy HTTP mode.

Note: It is recommended that you use Apache HTTP Server version 2.2 for Windows or Apache HTTP Server version 2.4 for Linux.

To configure Apache to work in proxy http mode:

1. Make sure the Apache Web server is stopped.
2. Navigate to the **<Apache Home directory>\conf** directory.
3. Open the **httpd.conf** file.
4. Uncomment or add the following load module commands:

```
LoadModule proxy_module modules/mod_proxy.so  
LoadModule proxy_http_module modules/mod_proxy_http.so
```

Note: Make sure that both modules exist in your Apache installation.

5. Add the following section to the end of the file:

```
# Turn off support for true Proxy behavior as we are acting as
# a reverse proxy
ProxyRequests Off

# Turn off VIA header as we know where the requests are proxied
ProxyVia Off

# Set the permissions for the proxy
<Proxy *>
AddDefaultCharset off
Order deny,allow
Allow from all
</Proxy>

# Turn on Proxy status reporting at /status
# This should be better protected than: Allow from all
ProxyStatus On
<Location /status>
SetHandler server-status
Order Deny,Allow
Allow from all
</Location>

# Configuring mod_proxy_http
# To connect to servlet container with HTTP protocol, the ProxyPass
# directive can be
# used to send requests received on a particular URL to a Jetty instance.
ProxyPreserveHost off

ProxyPass /qcbn http://<ALM server name>:8080/qcbn
ProxyPassReverse /qcbn http://<ALM server name>:8080/qcbn
```

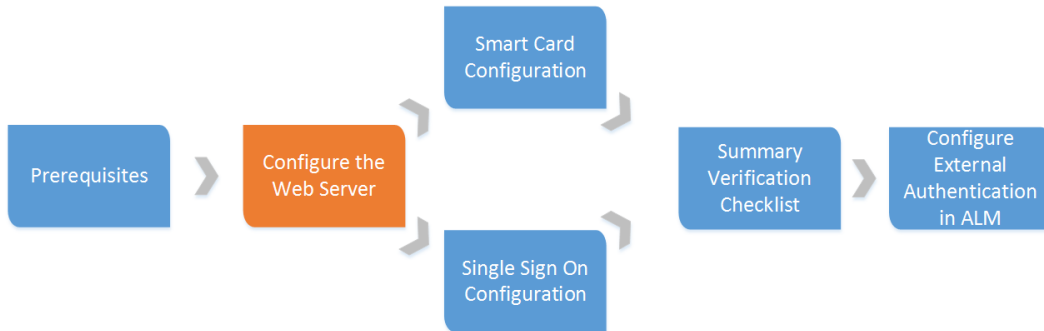
```
# For Performance Center deployments, add the following:
ProxyPass /loadtest http://<PC server name>/loadtest
ProxyPass /LoadTest http://<PC server name>/LoadTest
ProxyPass /Loadtest http://<PC server name>/Loadtest
ProxyPassReverse /loadtest http://<PC server name>/loadtest
ProxyPassReverse /LoadTest http://<PC server name>/LoadTest
ProxyPassReverse /Loadtest http://<PC server name>/Loadtest
# Rewrite rule trailing slash must be used in the VirtualHost section
LoadModule rewrite_module modules/mod_rewrite.so
RewriteEngine On
# Add trailing slash if was not present in the original request
RewriteRule ^/qcbins$ /qcbins/ [R]
```

Note: If you are connecting to ALM from a local machine, replace <ALM server name> with the localhost.

6. Save the changes to the file.
7. Restart the Apache Web server.

You can now connect to your ALM site using the following URL: **http://<ALM server name>[:<apache port number>]/qcbins**.

Chapter 4: Web Server Configuration



This chapter describes how to configure the web server and Jetty for external authentication.

This chapter includes

Configure Apache for External Authentication	16
Configure IIS for External Authentication	16
Configure Jetty for External Authentication	17

Configure Apache for External Authentication

Perform the following steps to configure the Apache web server for external authentication:

1. Navigate to the **<Apache Home directory>\conf** directory.
2. Create a backup copy of the **httpd.conf** file.
3. Open the **httpd.conf** file.
4. Uncomment or add the following load module command:

```
LoadModule headers_module modules/mod_headers.so
```

Note: Make sure that the module exists in your Apache installation.

5. Add the following section if encrypted communication terminates on the Apache server:

```
<IfModule headers_module>
#####
# add the following line if SSL is terminated/offloaded on Apache server
#####
RequestHeader set X-Forwarded-Proto https
</IfModule>
```

6. Add the following lines at the end of the file:

```
RequestHeader unset SM_USER
```

```
RequestHeader unset CERT
```

7. Save the **httpd.conf** file.
8. Restart Apache so it will read the configuration.

Configure IIS for External Authentication

Perform the following steps to configure the IIS web server for external authentication:

1. Edit the **qcbn** inbound rule and add the following server variable:

```
Set <set name="HTTP_X_FORWARDED_PROTO" value="https" />.
```

2. Select the server farm containing the ALM server and click **Proxy**.
3. Enable **Reverse rewrite host in response headers**.
4. Restart IIS so it will read the configuration.

Configure Jetty for External Authentication

Update the Jetty.XML file to allow HTTPS requests. This applies when ALM is behind a secure reverse proxy, which is mandatory for external authentication.

1. Make a backup of the **jetty.xml** file.
 - a. In Windows, navigate to the **<ALM deployment path>\server\conf** directory and make a backup of the **jetty.xml** file.
 - b. In Linux, navigate to the **/var/opt/HP/ALM/server/conf/** directory and make a backup of the **jetty.xml** file.

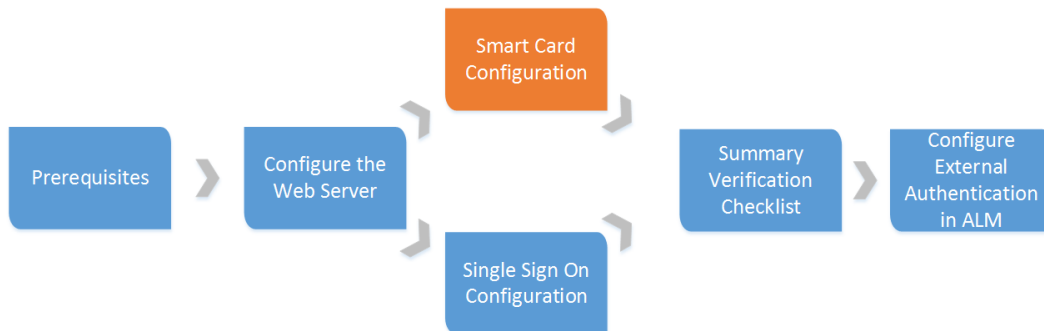
Caution: Make sure that you back up the jetty.xml file located in this directory.

2. Open the jetty.xml file. and in the **addConnector** section under the **Configure** element add the **<Set name="forwarded">true</Set>** command after the **SelectChannelConnector** line:

```
<New class="org.eclipse.jetty.server.nio.SelectChannelConnector">  
<Set name="forwarded">true</Set>
```

3. Restart the HP ALM service.

Chapter 5: Smart Card Configuration



When smart card authentication is enabled on ALM, users are required to provide a certificate when connecting. Once the user's certificate is validated, the user is authenticated by the ALM server. Before enabling smart card authentication, ensure the following steps are completed:

- The web server works over the HTTPS protocol. For details, see ["Configure Apache as a Secure Reverse Proxy" on page 20](#).
- The web server is configured as a reverse proxy that requires a client certificate. For details, see ["Configure Apache to Require a Client Certificate " on page 21](#).
- The web server is configured to pass certificate details to ALM. For details, see ["Configure the Apache SSL Proxy Server to Work with Smart Card" on page 22](#).

Note: For IIS, the above steps are described in ["Configure IIS to Work with Smart Card" on page 23](#).

Note: For non-interactive user communication, such as testing tools running on clients, you have obtained standard client certificates from your Certificate Authority (CA). Ensure that your ALM front-end web server trusts this CA. These certificates must be issued to a valid ALM user.

This chapter includes

Prepare Certificates	19
Configure Apache as a Secure Reverse Proxy	20
Configure Apache to Require a Client Certificate	21
Configure the Apache SSL Proxy Server to Work with Smart Card	22
Configure IIS to Work with Smart Card	23

Prepare Certificates

1. Obtain standard certificate(s) from your Certificate Authority (CA). Make sure that your ALM front-end server trusts this CA. Request the following from your certificate authority:
 - The certificate authority certificate. For Apache, the certificate must be in Base-64 format. For example, name the file **TrustedCA.pem**.
 - The server certificate issued to the reverse proxy server, either in an FQDN form or using a wildcard.
 - The software client certificate (for non-interactive users, when a smart card is not used).
2. Place the server certificate files in your web server configuration directory. For IIS, you can work with PFX or PKCS12 certificates. For Apache, you need to split the PFX certificate into two PEM files, the public certificate (for example, **WebServerPublicCert.pem**) and the private key (for example, **WebServerPrivateCert.pem**).

Note: If you receive certificates in different formats, you can use **openssl** to convert them. To install openssl, go to <http://www.openssl.org/related/binaries.html>.

- To convert from CER, use **openssl x509 -in /<webserver-directory>/conf/cert.cer -outform pem -out cert.pem**.
- To convert from PFX, do the following:
 - Export the public key by using **openssl pkcs12 -in /<webserver-directory>/conf/cert.pfx -clcerts -nokeys -out certPublic.pem**.
 - Export the private key by using **openssl pkcs12 -in /<webserver-directory>/conf/cert.pfx -nocerts -nodes -out certPrivate.pem**.

3. Create an ALM user and make sure there is a physical smart card with a certificate containing the user credentials. The user login value must be embedded in an attribute in the certificate. When you run the Smart Card Authentication Configuration Wizard you select the specific attribute.
4. If access to the CRL server requires a proxy, you must modify the **<ALM installation folder>\wrapper\wrapper.conf** file. Add the following:

```
# *** IMPORTANT ***
```

```
# If you enable any of the options below, you MUST change <n> to the next available
```

```
# consecutive number (based on the number of additional properties in the
current file).
# Otherwise, Java will not parse this properties file correctly!
wrapper.java.additional.<n>=-Dhttp.proxySet=true
wrapper.java.additional.<n+1>=-Dhttp.proxyHost=<the proxy host>
wrapper.java.additional.<n+2>=-Dhttp.proxyPort=<the proxy port>
wrapper.java.additional.<n+3>=-Dhttp.proxyUser=<the proxy user name>
wrapper.java.additional.<n+4>=-Dhttp.proxyPassword=<the proxy password>
```

5. Install the client certificate for the non-interactive user.

Configure Apache as a Secure Reverse Proxy

To configure Apache as a secure reverse proxy:

1. Open the **httpd.conf** file.

2. Uncomment **ssl_module**:

```
LoadModule ssl_module modules/mod_ssl.so
```

3. Uncomment the **httpd-ssl.conf** file:

```
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
```

4. Close the **httpd.conf** file and open the **httpd-ssl.conf** file. By default it is in **/<apache-directory>/conf/extra**.

5. In the **httpd-ssl.conf** file, activate the SSL port 443:

```
Listen 443
```

6. Add the **SSLProtocol** parameter:

```
SSLProtocol -SSLv2 -SSLv3 +TLSv1
```

7. Change the cache settings:

```
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
SSLSessionCache "shmcb:<apacheAbsoluteFolder>/logs/ssl_scache(512000)"
```

8. Modify the **VirtualHost** and **ServerName** parameters:

```
<VirtualHost <fully qualified server name>:443>  
ServerName <fully qualified server name>:443
```

9. Add the SSL certificates to the **VirtualHost** section (for details, refer to ["Prepare Certificates" on page 19](#)):

```
# Server Certificate  
SSLCertificateFile " /<apache-directory>/conf/WebServerPublicCert.pem"  
# Server Private Key:  
SSLCertificateKeyFile " /<apache-directory>/conf/WebServerPrivateCert.pem"
```

10. Restart Apache so it will read the new configuration.

```
Run <apache-directory>/bin/apachectl -k restart
```

11. Verify that Apache works as a secure proxy server.

Go to <https://webserver/qcbin>. Make sure the login screen is displayed.

12. After verifying that Apache works as a secure proxy server, close the non-secure port.

- a. Open the **httpd.conf** file.
- b. Comment out the **Listen** parameter:

```
#Listen 80
```

Configure Apache to Require a Client Certificate

To configure Apache to require a client certificate:

1. Open the **httpd-ssl.conf** file.
2. Find the related **VirtualHost** and modify as follows:
 - a. Add the certificate authority that Apache will trust for client certificates

```
# CA that Apache will trust for client certificates  
SSLCACertificateFile " /<apache-directory>/conf/TrustedCA.pem"
```

- b. Set the **SSLVerifyClient** parameter:

```
SSLVerifyClient require  
SSLVerifyDepth 10
```

- c. If you have a certificate revocation file, add the following line:

```
SSLCARevocationFile <full name of the revocation file> SSLCARevocationCheck  
chain
```

- d. If OCSP is needed, set the **SSLOCSPEnable** parameter:

```
SSLOCSPEnable on
```

3. Restart Apache so it will read the new configuration.

Run **<apache-directory>/bin/apachectl -k restart**

4. Verify that Apache accepts your smart authentication cards.

Go to **https://webserver/qcbin**. Make sure the ALM home page opens after you provide your smart card.

Note: If you have several client certificates that can be used, the browser should show the choice dialog box.

Configure the Apache SSL Proxy Server to Work with Smart Card

To configure the Apache SSL proxy server to work with Smart Card:

1. Open the **httpd.conf** file

2. Uncheck **headers_module**:

```
LoadModule headers_module modules/mod_headers.so
```

3. Open the **httpd-ssl.conf** file.

4. Find the related **VirtualHost** and modify as follows:

- a. Uncomment **SSLOptions** to extract the certificate:

```
SSLOptions +ExportCertData
```

- b. Set the header that ALM will use to authenticate (the default value is CERT):

```
RequestHeader set CERT "%{SSL_CLIENT_CERT}s"
```

5. Restart Apache so it will read the new configuration.

Run `<apache-directory>/bin/apachectl -k restart`

Configure IIS to Work with Smart Card

To configure IIS as a secure reverse proxy requiring client certification:

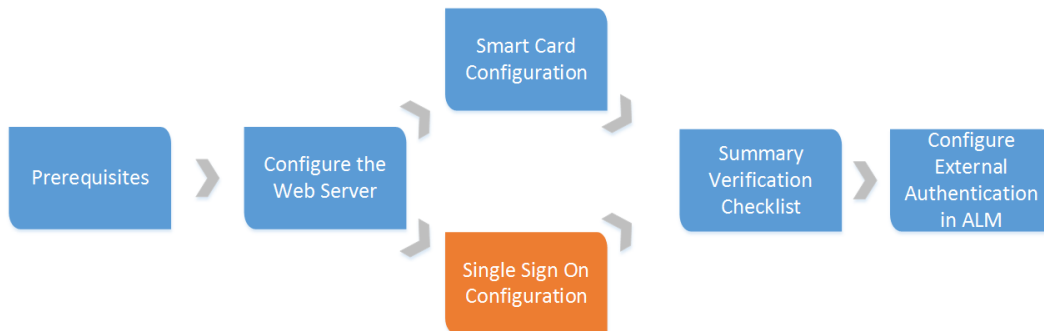
Note: For detailed instructions, refer to the IIS documentation.

1. Install the server certificates in IIS.
2. Configure IIS to require an SSL connection.
3. Configure IIS to require a client certificate.
4. Value **Forward encoded client certificate in the following header** with the name of the header that ALM will use to authenticate. The ALM default value is CERT.

Note: If the value is not CERT, you must set the **EXTERNAL_AUTH_CERT_HEADER_NAME** site parameter to match the value in **Forward encoded client certificate in the following header**.

5. Restart IIS so it will read the configuration.

Chapter 6: Single Sign-On Configuration



Implement a Single Sign-On (SSO) solution to use external authentication providers such as Siteminder.

Note: By default, Siteminder's Web agent configuration provides restrictions for characters in URL and URL query parts. To support ALM Web Client and REST over SiteMinder, these options must be modified.

This allows the ALM user to authenticate once through the external authentication point without any need to provide credentials again until the end of the user session.

The typical SSO server controls the user's access to various organizational resources, protecting confidential personal and business information from unauthorized users.

For details, see your SSO vendor's documentation.

Configure your SSO server to secure the following ALM resources:

- /qcbn/*
- /loadtest/* (for Performance Center)

Note: Ensure that your authentication scheme supports non-browser clients. Otherwise, OTA integrations and add-ins will not work in an SSO environment.

Before configuring external authentication in ALM, ensure that the SSO log in process works. Ensure that you can pass SSO authentication before the ALM home page opens. If SSO is not working, work with your SSO administrator.

Note:

- It is recommended to use SSL with SSO. If SSL is not enabled, the SSO cookie is vulnerable to being intercepted.

- The SSO cookie must be HTTP-only. When it is set as a regular cookie, it is vulnerable to XSS attacks.

If the same LDAP settings were defined in ALM and in SSO, you can authenticate through both the SSO and ALM login screens using the same credentials. If not, verify that the LDAP settings in ALM match those used by SSO.

ALM requires the SSO vendor to pass the authenticated user name as a header on the HTTP request. Configure the header name and pattern in Site Administration. For more information, refer to "[Configure Site Administration](#)" on page 30

Note: There are no special processing considerations when configuring Apache for SSO.

Configure SSO on IIS

Note: We recommend using Apache as the web server with SiteMinder. To support ALM WebUI and REST over SiteMinder, you must use Apache as the web server.

When using IIS with an SSO solution that uses ISAPI filtering, such as SiteMinder, you must configure IIS using ISAPI redirect.

Configure the Apache Tomcat Connector for IIS

1. On the IIS server, download **isapi_redirect.dll** to C:\JAKARTA.
2. Create the **C:\JAKARTA\isapi_redirect.properties** file:

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=C:\jakarta\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file=C:\jakarta\workers.properties.minimal
```

```
# Full path to the uriworkermap.properties file  
worker_mount_file=C:\jakarta\uriworkermap.properties
```

3. Create the **C:\JAKARTA\workers.properties.minimal** file:

```
# workers.properties.minimal -  
#  
# This file provides minimal jk configuration  
# properties needed to  
# connect to Tomcat.  
#  
# Defining a worker named ajp13w and of type ajp13  
# Note that the name and the type do not have to  
# match.  
worker.list=AlmAjp  
worker.AlmAjp.type=ajp13  
worker.AlmAjp.host=<ALM server name>  
worker.AlmAjp.port=8009  
#END
```

4. Create the **C:\JAKARTA\uriworkermap.properties** file:

```
# uriworkermap.properties - IIS  
#  
# This file provides sample mappings for example:  
# ajp13w worker defined in workermap.properties.minimal  
# The general syntax for this file is:  
# [URL]=[Worker name]  
/qcbi*=AlmAjp  
#/webui
```

5. Create the **C:\JAKARTA\Jakarta_Install.bat** file:

```
%systemroot%\system32\inetsrv\APPCMD add app /site.name:"Default Web Site"  
/path:/jakarta /physicalPath:C:\Jakarta /applicationPool:DefaultAppPool  
%systemroot%\system32\inetsrv\APPCMD set config -  
section:system.webServer/isapiFilters /+"
```

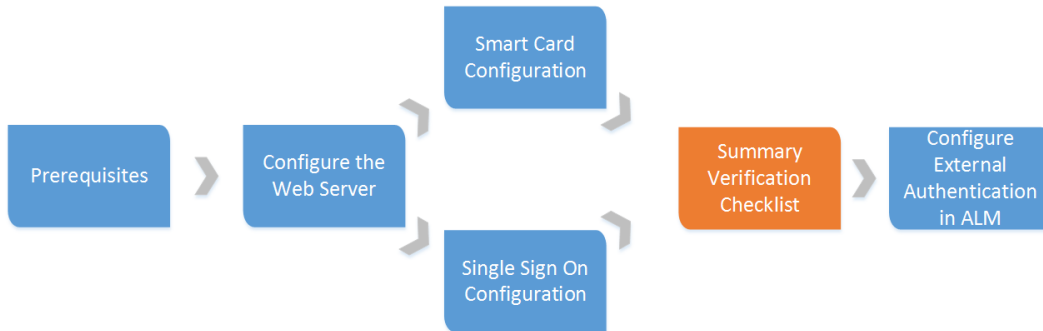
```
[name='jakartaFilter',path='C:\Jakarta\isapi_redirect.dll',enabled='True']"  
/commit:apphost  
  
%systemroot%\system32\inetsrv\APPCMD set config "Default Web Site/jakarta" -  
section:system.webServer/handlers /accessPolicy:Read,Script,Execute  
/commit:apphost  
  
%systemroot%\system32\inetsrv\APPCMD set config -  
section:system.webServer/security/isapiCgiRestriction /+ "  
[path='C:\Jakarta\isapi_  
redirect.dll',allowed='True',description='jakartaFilter']" /commit:apphost
```

6. Install Jakarta on IIS.
 - a. Run **C:\JAKARTA\Jakarta_Install.bat**.
 - b. Restart IIS.
 - c. Ensure that the ISAPI filter and extension are installed on IIS.
 - d. Ensure that Jakarta appears in IIS.
7. Enable **Anonymous Authentication** on IIS.
8. Restart IIS.

Enable Support of the AJP Protocol on ALM

1. Open the **start.ini** file on the ALM server and uncomment **jetty-ajp.xml**.
2. Restart the ALM server.

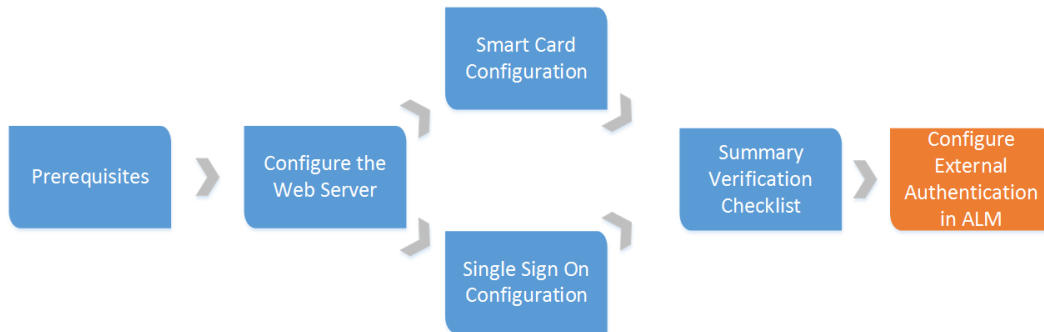
Chapter 7: Verification Checklist



Perform the following verifications:

- Verify that the web server works as a reverse proxy.
- Verify that the site administration user can pass through the reverse proxy authentication, either Smart Card or SSO.
- Verify that the same site administration user exists in ALM and can log in to ALM. Keep a separate session open and do not log out until the external authentication process has been successfully completed.

Chapter 8: ALM Configuration



This chapter describes how to configure ALM for external authentication environments.

This chapter includes

Configure Site Administration	30
Verify External Authentication	32
Configure Smart Card Authentication for Performance Center	32
Configure SSO for Performance Center	34
Configure Smart Card Authentication for APIs	35
Configure SSO for APIs	36
Special Configurations for Smart Card Authentication	37
Special Configurations for SSO	38
Configure External Authentication for Remote Machines	39

Configure Site Administration

1. Log in to Site Administration using the site administrator user.
2. Enable external authentication.
 - a. Click the **Site Users** tab, click the **User Settings** button, and select **Authentication Settings**.
 - b. Under **Authentication type**, select **External Authentication** and click **Advanced Settings**.
 - c. Select the **Principal Type** of authentication and enter the **Pattern**. The default pattern is `[eE][^]=([^,]*@[^,]*)`, which is the pattern for the email address.

Note: For smart card authentication, enter the **Pattern** you are using, or leave the **Pattern** empty if you are using the default pattern. For SSO authentication, enter `(.*)` as the **Pattern**.

For more information, refer to the *Enabling External Authentication for Users* section in the *HP Application Lifecycle Management Administrator Guide*.

3. Set the site parameters as needed. For information on setting site parameters, refer to the *HP Application Lifecycle Management Administrator Guide*. For a list of external authentication site parameters, see "[External Authentication Site Parameters](#)" on page 44.

Note: Before setting the site parameters, click **Refresh** to see which site parameters were set when you enabled external authentication.

The following site parameters are required for external authentication:

- Valuing **EXTERNAL_AUTH_MODE** with Y invokes external authentication.

Note: This parameter can be set in the Authentication Settings screen.

- Value **EXTERNAL_AUTH_HEADER_NAME** for SSO authentication with the name of the header in the HTTP request that contains the string from which ALM extracts the user search key for the external authentication. The default value is SM_USER.
- Value **EXTERNAL_AUTH_CERT_HEADER_NAME** for smart card authentication with the name of the header in the HTTP request that contains the string from which ALM extracts the user search key for the external authentication. The default value is CERT.
- **EXTERNAL_AUTH_USER_FIELD_PATTERN** contains a regular expression pattern. ALM

replaces the string that matches the regular expression pattern with the value that matches the pattern defined between the first pair of braces. For example, if the pattern is `.*[eE][/^=]*=([^,]*@[/^,]*)` and the input string is `CN=QA, E=qa@hp.com`, ALM extracts `qa@hp.com` as the user search key.

Note: This parameter can be set in the External Authentication Advanced Settings screen.

- **EXTERNAL_AUTH_USER_FIELD_TYPE** determines how to search for the valid ALM user with the extracted user search key. If this parameter is valued with **email**, ALM searches for a user email that matches the user search key. If this parameter is valued with **name**, ALM searches for a user name (in the user description field) that matches the user search key. If this parameter is valued with **email+name**, ALM searches for a user email that matches the user search key. If no match is found, ALM then searches the user description field for a match to the user search key.

Note: This parameter can be set in the External Authentication Advanced Settings screen.

The following site parameters are optional, depending on the specific external authentication mode:

- The client certificate validity should be verified by the authentication proxy. However, some proxies do not perform some required verifications, so ALM performs the verification. Valuing **EXTERNAL_AUTH_CERTIFICATE_POLICY_CHECK** with Y invokes the ALM verification. If the certificate contains policy information, the verification is performed. If the certificate does not contain policy information and **EXTERNAL_AUTH_IS_POLICY_REQUIRED** is valued with Y, ALM does not allow the user to log in. If the value is N, ALM ignores the verification.
- When ALM performs the verification, it checks whether the client certificate has at least one policy defined in **EXTERNAL_AUTH_CERTIFICATE_VALID_POLICY**. If this parameter is not valued, ALM does not allow the user to log in.
- Value **EXTERNAL_AUTH_CERTIFICATE_CRL_CHECK** with Y to check whether the client certificate is in the certificate revocation list (CRL). If the client certificate does not contain information about the CRL distribution point, ALM does not perform this check even if it is enabled. If the client certificate is in the CRL or if ALM cannot access the CRL distribution point, ALM does not allow the user to log in.
- Value **EXTERNAL_AUTH_CERTIFICATE_LOCAL_CRL_CHECK** with Y to check whether the client certificate is in a local CRL. The folder that contains the CRL is defined in **EXTERNAL_AUTH_CERTIFICATE_CRL_FOLDER**. If this parameter is not set, ALM does not perform this check even if it is enabled. The CRL files have `.crl` or `.pem` extensions.
- Value **EXTERNAL_AUTH_CERTIFICATE_OCSP_CHECK** with Y to check the client certificate status using an online certificate status protocol (OCSP). This check is not performed if **EXTERNAL_AUTH_CERTIFICATES_FILE** is not valued. If the client certificate contains OSCP URLs, ALM perform this verification. If the client certificate does not contain OSCP URLs and **EXTERNAL_AUTH_CERTIFICATE_OCSP_REQUIRED** is Y, ALM does

not allow the user to log in. If this parameter is N and the client certificate does not contain OSCP URLs, ALM ignores this check. If ALM fails to access the OCSP URL, the user is not allowed to log in.

Verify External Authentication

1. Verify that the external authentication mode is active and working.
 - Do not log out of Site Administration.
 - From another client machine, try to log in to Site Administration using external authentication.
 - Go to ALM using the web server address (<https://<webserver>/qcbn/>).
 - Click Site Administration. Site Administration should open without displaying the username and password screen.

Note: If you cannot log in, see ["Troubleshooting" on page 42](#).

2. Verify that the external authentication mode is working for other users, such as project administrators.

Configure Smart Card Authentication for Performance Center

After configuring smart card authentication for ALM, perform the following steps:

1. Edit the web.config file located in the following path: <install path>\PCWEB.
2. Set the following:

```
<add key="CAOnly" value="true"/>
```
3. Restart IIS on the Performance Center server.
4. Configure the Reverse Proxy (web server):
 - a. For Apache: Open the httpd.conf file. By default it is in /<apache-directory>/conf. Configure the ProxyPass:

```
ProxyPass /loadtest http: // REAL_PC_SERVER/loadtest  
ProxyPass /LoadTest http: // REAL_PC_SERVER/LoadTest
```



```
ProxyPass /Loadtest http: // REAL_PC_SERVER/Loadtest
ProxyPass /SNV http://REAL_PC_SERVER/SNV
ProxyPassReverse /loadtest http: // REAL_PC_SERVER/loadtest
ProxyPassReverse /LoadTest http: // REAL_PC_SERVER/LoadTest
ProxyPassReverse /Loadtest http: // REAL_PC_SERVER/Loadtest
ProxyPassReverse /SNV http://REAL_PC_SERVER/SNV
```

Note: The lines containing /SNV are needed only when working with Shunra Network Virtualization.

- b. For IIS:
 - i. Edit the inbound rule for the Performance Center server.
 - ii. Set **Requested URL** to **Matches the Pattern**.
 - iii. Set **Using** to **Regular Expressions**.
 - iv. Set **Pattern** to **loadtest***.
 - v. Enable **Ignore case**.
5. Configure Performance Center servers in Lab Management.
 - a. Open Lab Management.
 - b. Go to **Servers > PC Servers**.
 - c. Click **ALM Connection**
 - d. In the ALM Connection dialog box, value:
 - i. **Internal URL** with the connection URL of the ALM server.
 - ii. **External URL** with the address of the reverse proxy using https, followed by /qcbn (for example, https://<reverse proxy machine>/qcbn).
 - e. Click **New PC Server**.
 - f. In the New PC Server dialog box, value:
 - i. **Name** with the new PC server name.
 - ii. **Internal URL** with the connection URL of the Performance Center server.
 - iii. **External URL** with the address of the reverse proxy using https (for example, https://<reverse proxy machine>).

Configure SSO for Performance Center

After configuring SSO for ALM, perform the following steps:

1. Edit the web.config file located in the following path: <install path>\PCWEB.
2. Set the following:

```
<add key="SiteMinderOnly" value="true"/>  
<add key="SiteMinderHeader" value="SM_USER"/>
```

Note: If you used another header instead of SM_USER when configuring the external authentication mode in ALM, use that header name to value the SiteMinderHeader key.

3. Restart IIS on the Performance Center server.
4. Define the Performance Center server in SSO.
5. Configure the Reverse Proxy (web server):
 - a. For Apache: Open the httpd.conf file. By default it is in /<apache-directory>/conf. Configure the ProxyPass:

```
ProxyPass /loadtest http: // REAL_PC_SERVER/loadtest  
ProxyPass /LoadTest http: // REAL_PC_SERVER/LoadTest  
ProxyPass /Loadtest http: // REAL_PC_SERVER/Loadtest  
ProxyPass /SNV http://REAL_PC_SERVER/SNV  
ProxyPassReverse /loadtest http: // REAL_PC_SERVER/loadtest  
ProxyPassReverse /LoadTest http: // REAL_PC_SERVER/LoadTest  
ProxyPassReverse /Loadtest http: // REAL_PC_SERVER/Loadtest  
ProxyPassReverse /SNV http://REAL_PC_SERVER/SNV
```

Note: The lines containing /SNV are needed only when working with Shunra Network Virtualization.

- b. For IIS:

Note: Performance Center does not work with SSO when using IIS as the web server.

6. Configure Performance Center servers in Lab Management.

- a. Open Lab Management.
- b. Go to **Servers > PC Servers**.
- c. Click **ALM Connection**
- d. In the ALM Connection dialog box, value:
 - i. **Internal URL** with the connection URL of the ALM server.
 - ii. **External URL** with the address of the reverse proxy using https, followed by /qcbn (for example, https://<reverse proxy machine>/qcbn).
- e. Click **New PC Server**.
- f. In the New PC Server dialog box, value:
 - i. **Name** with the new PC server name.
 - ii. **Internal URL** with the connection URL of the Performance Center server.
 - iii. **External URL** with the address of the reverse proxy using https (for example, https://<reverse proxy machine>).

Configure Smart Card Authentication for APIs

To use APIs with smart card authentication, the following changes must be made.

- OTA API:

When the user attempts to log in, a window appears and the user selects the proper certificate to establish an SSL connection. If the application is not supposed to work in interactive mode or if the user frequently logs in, the user can specify a default certificate.

To specify the default certificate, in ALM go to **Help > ALM Tools > Webgate Customization**. On the Web Server Settings tab, select the appropriate WebClient certificate mode, and select your default certificate.

The WebClient certificate modes are explained as follows:

- **Not specify mode** – This mode is for backward compatibility with applications developed before external authentication was available. If the certificate is not applied, it works like the **Interactive mode**.
- **Interactive mode** – This mode is for interactive use, where a screen appears if the certificate is not provided or cannot be applied to the connection. To enable this mode, use `ITDConnection9::SetExecutionMode()`.

- **Non-interactive mode** – This mode is for non-interactive use, where an error code is returned if the certificate is not provided or cannot be applied to the connection. To enable this mode, use `ITDConnection9:: SetExecutionMode()`.
- REST API:

Note: The REST API is a technical preview.

- Web browser extension (REST clients) – The web browser establishes the SSL connection. When attempting to connect, a certificate selection window appears. After the certificate is applied, REST API continues as usual.
- Non browser REST Clients – The REST client establishes the SSL connection, after which REST API continues as usual.

Configure SSO for APIs

To use APIs with SSO authentication, the following changes must be made.

- OTA API:

When the user attempts to log in, a window appears and the user selects the proper certificate to establish an SSL connection. If the application is not supposed to work in interactive mode or if the user frequently logs in, the user can specify a default certificate.

To specify the default certificate, in ALM go to **Help > ALM Tools > Webgate Customization**. On the Web Server Settings tab, select the appropriate WebClient certificate mode, and select your default certificate.

The WebClient certificate modes are explained as follows:

- **Not specify mode** – This mode is for backward compatibility with applications developed before external authentication was available. If the certificate is not applied, it works like the **Interactive mode**.
- **Interactive mode** – This mode is for interactive use, where a screen appears if the certificate is not provided or cannot be applied to the connection. To enable this mode, use `ITDConnection9:: SetExecutionMode()`. Use `ITDConnection9::CreateSession` instead of `ITDConnection2::Login`.

Note: Remove any UI in your application prompts for user credentials. The credentials are taken from the client certificate.

- **Non-interactive mode** – This mode is for non-interactive use, where an error code is returned if the certificate is not provided or cannot be applied to the connection. To enable this mode, use

ITDConnection9:: SetExecutionMode(). Use ITDConnection9::CreateSession instead of ITDConnection2::Login.

- REST API:

Note: The REST API is a technical preview.

- Web browser extension (REST clients) – The web browser authenticates via the connection itself, so when attempting to connect, the browser requests the SSO credentials. After the SSO credentials are applied, REST API continues as usual.
- Non browser REST Clients – The REST client passes the SSO authentication, after which REST API continues as usual.

Note: SiteMinder does not allow sending URLs that include the ['] character (single quote). To send such URLs, either replace the single quote with double quotes or change the SiteMinder settings to allow the single quote character.

Special Configurations for Smart Card Authentication

To use the following ALM components and features with smart card authentication, the following changes must be made.

- HP ALM Client MSI Generator:

HP ALM Client MSI Generator does not fully support external authentication. To use MSI Generator with external authentication, perform the following:

- Install HP ALM Client MSI Generator on the ALM server.
- Value the **ALM server address** field in MSI Generator with the URL of the ALM server on which ALM Client MSI Generator is installed.
- Specify the URL of the server that end users access in the **Additional Servers** section of the Generate Client MSI for HP ALM Server page.

- Smart Repository

Smart Repository FTP access is not available from remote clients when external authentication is enabled. To access Smart Repository, the user must connect to it from any client (including localhost) after the web proxy, with ALM credentials.

Note: Only ALM credentials are used. If LDAP integration was enabled with external authentication, ensure that the user's ALM credentials are valued.

Special Configurations for SSO

To use the following ALM components and features with SSO, the following changes must be made:

- All QCCH (QC Connectivity Helper) integrations:

You can only integrate with components and features, such as UFT, Load Runner, and Business Views Excel reports, over QCCP, using the basic authentication mode.

Note: We recommend using the *Basic authentication over SSL* option.

- HP ALM Client MSI Generator:

HP ALM Client MSI Generator does not fully support external authentication. To use MSI Generator with external authentication, perform the following:

- Install HP ALM Client MSI Generator on the ALM server.
- Value the **ALM server address** field in MSI Generator with the URL of the ALM server on which ALM Client MSI Generator is installed.
- Specify the URL of the server that end users access in the **Additional Servers** section of the Generate Client MSI for HP ALM Server page.

- Microsoft Word and Excel add-ins:

- a. In the Web Server Settings tab of the Webgate Customization tool, enable **Add basic authentication header** and select **Do not add when a cookie is present**.
- b. When exporting data to ALM from Word or Excel:
 - i. In the HP ALM Export Wizard - Step 1 of 5 dialog box, enter the ALM URL, enable **Force Basic Authentication** as needed, and click **Next**.

Note: **Force Basic Authentication** is optional, and should only be enabled if you get an **invalid server response** message.

- ii. Enter your credentials and click OK.

Note: If your credentials are defined in the Webgate Customization tool, the HP ALM Export Wizard - Step 3 of 5 dialog box opens without requiring any login details.

- iii. Continue with the HP ALM Export Wizard.

Note: After making any changes in the Webgate Customization tool, you must restart Excel and Word for the changes to take effect.

- Smart Repository

Smart Repository FTP access is not available from remote clients when external authentication is enabled. To access Smart Repository, the user must connect to it from any client (including localhost) after the web proxy, with ALM credentials.

Note: Only ALM credentials are used. If LDAP integration was enabled with external authentication, ensure that the user's ALM credentials are valued.

Configure External Authentication for Remote Machines

To run tests on remote machines, configure the remote machine to interact with the ALM server using any batch certificate.

1. Install the batch certificate on the remote machine.
2. On the Import Certificate Wizard, uncheck **Enable strong private key protection**.
3. Run the Webgate Customization tool. In ALM, go to **Help > ALM Tools > Webgate Customization**.
4. Under **Webclient Certificates**, select **Use client certificate - Non-interactive mode**, and select the batch certificate.
5. Run the test from the ALM server. The remote machine connects to the ALM server using the batch certificate.

Chapter 9: Limitations

The following ALM components and features are not supported with Smart Card external authentication:

- ALI
- Analysis items sharing
- Enterprise Collaboration for HP ALM
- HP ALM Explorer
- HP ALM Lab Service
- HP ALM Synchronizer
- HP Enterprise Integration Module for SAP Solution Manager
- HP Service Test Management
- Lab Server-Side Execution
- Performance Center host over cloud
- QC Sense
- Service Virtualization
- Sprinter
- TaskTop
- Web Client
- Workflow - you cannot connect as another user via workflow

The following ALM components and features are not supported with SSO external authentication:

- ALI
- Analysis items sharing
- Enterprise Collaboration for HP ALM
- HP ALM Lab Service

- HP Enterprise Integration Module for SAP Solution Manager
- HP Service Test Management
- Lab Server-Side Execution
- Performance Center host over cloud
- QC Sense
- Service Virtualization
- Synchronizer
- TaskTop
- Test Types:
 - Custom Test
 - Sprinter
 - System Test

Chapter 10: Troubleshooting

Following are troubleshooting suggestions for issues relating to external authentication:

Problem:

SSO header and data are unknown.

Resolution:

- Turn off External Authentication.
- Add the **DUMP_REQUEST_HEADERS** site parameter with a value of Y and set the debug level for the site administration logs to **Debug**.
- Try to log in to ALM Site Administration.
- Check the Site Administration logs to see what data the Authentication server sent. Search for your user ID and identify the header that contains it. This header must be used in the External Authentication wizard.
- Apply the correct header and pattern.
- Once the problem is solved, turn off debug and set **DUMP_REQUEST_HEADERS** to N.

Problem:

Authentication to Site Administration failed due to an incorrect configuration.

Possible Cause:

- User with SSO data was not added to the Site Administrators list.
- Incorrect or missed SSO data in the user's properties.
- The pattern or header is incorrect.

Resolution:

- Execute the following SQL query :

```
UPDATE PARAMS SET PARAM_VALUE='N' WHERE PARAM_NAME='EXTERNAL_AUTH_MODE'
```

- Restart HP ALM service.
- Log in to Site Administration and verify the configuration.

Information about the Site Administration schema and database can be found at siteadmin.xml, located in <ALM_INSTALLATION_FOLDER>\application\20qcbn.war\WEB-INF.

Problem:

Performance Center configuration fails with an Action not authorized message.

Possible Cause:

- The ALMinternal URL is incorrect.
- The Performance Center server internal URL is incorrect.

Resolution:

Ensure that the ALMinternal URL and the Performance Center server internal URL are correct.

Problem:

When you must apply a client certificate to a connection, for example when running VAPI-XP tests, the Select Certificate dialog box is not seen.

Possible Cause:

The Select Certificate dialog box is open, but is sometimes hidden.

Resolution:

Manually switch to the Select Certificate dialog box.

Problem:

Debugging in ALM requires internal authentication, and therefore does not work in external authentication mode.

Resolution:

Switch from external authentication to ALM authentication to get the debug information and then switch back to external authentication.

Problem:

When working with Smart Card authentication, the authentication screen appears when ALM makes an independent connection. For example, when the ALM Welcome page or the ALM Help opens, the authentication screen also appears.

Resolution:

Enter the required authentication information each time the authentication screen appears.

Chapter 11: External Authentication Site Parameters

Following are the external authentication site parameters:

Parameter	Description
EXTERNAL_AUTH_MODE	<p>Determines if external authentication is invoked (Y).</p> <p>Default: N</p> <p>This parameter can be set in the Authentication Settings screen.</p> <p>Note: Configure other parameters before switching ALM to external authentication mode, otherwise you can lose ALM connectivity.</p>
EXTERNAL_AUTH_HEADER_NAME	<p>The name of the header in the HTTP request that contains the string from which ALM extracts the user search key for the external authentication.</p> <p>This parameter is used for SSO authentication.</p> <p>Default: SM_USER</p> <p>Note: This parameter and EXTERNAL_AUTH_CERT_HEADER_NAME cannot both be set.</p>
EXTERNAL_AUTH_CERT_HEADER_NAME	<p>The name of the header in the HTTP request that contains the PEM encoded public client certificate from which ALM extracts the user search key for the external authentication. ALM extracts the user search key from the subject field of the certificate.</p> <p>This parameter is used for smart card authentication.</p> <p>Default: CERT</p> <p>Note: This parameter and EXTERNAL_AUTH_HEADER_NAME cannot both be set.</p>
EXTERNAL_AUTH_USER_FIELD_TYPE	<p>Determines how the user is identified in the external authentication data (email, name, or email+name).</p> <p>Default: email+name</p> <p>This parameter can be set in the External Authentication Advanced Settings screen.</p>

Parameter	Description
EXTERNAL_AUTH_USER_FIELD_PATTERN	<p>Determines how to extract authentication data from the HTTP header specified by the EXTERNAL_AUTH_HEADER_NAME or the EXTERNAL_AUTH_CERT_HEADER_NAME parameter.</p> <p>Default:</p> <ul style="list-style-type: none"> • When user matches by email field: <code>*[eE][^=]*=(^[,]*@[^,]*)*</code> • When user matches by description field: <code>*?[cC][nN] *= *([^\,]*)*</code> <p>This parameter can be set in the External Authentication Advanced Settings screen.</p>
EXTERNAL_AUTH_VALIDATE_USER_IN_LDAP	<p>Determines whether ALM contacts the LDAP server (if it exists) to ensure that this user is active.</p> <p>Default: N</p>
EXTERNAL_AUTH_DEBUG_LEVEL	<p>The level of the debug information related to external authentication.</p> <p>Default: 1</p>
EXTERNAL_AUTH_CERTIFICATES_FILE	<p>The name of the file that holds all the CA and Intermediate certificates trusted by ALM. The file must contain PEM format concatenated certificates.</p>
EXTERNAL_AUTH_CERTIFICATE_CRL_CHECK	<p>Determines whether to enable or disable the online certificate revocation list (CRL) check.</p> <p>Default: Y</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: For smart card authentication, if the online certification revocation list (CRLDP) is required, set this parameter to Y.</p> </div>
EXTERNAL_AUTH_CERTIFICATE_LOCAL_CRL_CHECK	<p>Determines whether to enable or disable the local CRL check.</p> <p>Default: Y</p>
EXTERNAL_AUTH_CERTIFICATE_DELTA_CRL_CHECK	<p>Determines whether to enable or disable the delta CRL validation.</p> <p>Default: Y</p>

Parameter	Description
EXTERNAL_AUTH_MATCH_DELTACRL_BY_ISSUER	<p>Determines ALM behavior when the folder in EXTERNAL_AUTH_CERTIFICATE_CRL_FOLDER contains delta CRL files without base CRL files.</p> <p>If this parameter is valued with Y, login is disabled for users if the delta CRL file is issued by same issuer.</p> <p>If this parameter is valued with N, then login is disabled even if there is one delta CRL file in the folder.</p> <p>Default: Y</p>
EXTERNAL_AUTH_CERTIFICATE_CRL_FOLDER	<p>The full path to the folder containing the CRL files.</p> <p>Note: For smart card authentication, if delta CRL validation is needed, value this parameter with the location of the folder on the server that contains the CRL files. This parameter does not replace the parameter in the Apache configuration file. Both Apache and the ALM server check the CRL files.</p>
EXTERNAL_AUTH_CERTIFICATE_DATE_CHECK	<p>Determines whether to enable or disable the certificate date check.</p> <p>Default: Y</p>
EXTERNAL_AUTH_CERTIFICATE_POLICY_CHECK	<p>Determines whether to enable or disable the certificate policy check.</p> <p>Default: Y</p>
EXTERNAL_AUTH_CERTIFICATE_VALID_POLICY	<p>The list of valid certificate policy IDs.</p> <p>Note: For smart card authentication, if certificate policy validation is needed, value this parameter.</p>
EXTERNAL_AUTH_IS_POLICY_REQUIRED	<p>Determines if each client certificate is required to have a policy.</p> <p>Default: Y</p> <p>Note: If the value is Y, each client certificate must have a valid policy which matches the EXTERNAL_AUTH_CERTIFICATE_VALID_POLICY parameter. If the value is N, the client certificate does not need to have a policy. However, whenever a policy is defined in the certificate, it must always match the EXTERNAL_AUTH_CERTIFICATE_VALID_POLICY.</p>

Parameter	Description
EXTERNAL_ AUTH_ HARDWARE_ CARD_IS_ REQUIRED	Determines whether each client certificate is required to have a hardware extended key (relevant for Interactive and Not Specified client execution modes). Default: Y
EXTERNAL_ AUTH_ EXTENDED_ HARDWARE_ KEYS	The valid hardware extended keys, separated by commas. Default: 1.3.6.1.4.1.311.20.2.2
EXTERNAL_ AUTH_ EXECUTION_ MODE_ HEADER_NAME	The name of the header in the HTTP request that holds the execution mode of the client (NOT_SPECIFIED, INTERACTIVE, NON_INTERACTIVE). Default: NOT_SPECIFIED
EXTERNAL_ AUTH_ CERTIFICATE_ OCSP_CHECK	Determines whether to enable or disable the online certificate status protocol (OCSP) check. Default: N
EXTERNAL_ AUTH_ CERTIFICATE_ OCSP_ REQUIRED	Determines whether each client certificate is required to have an OCSP link. Default: Y

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on External Authentication Configuration Guide (ALM 12.01)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-Doc@hp.com.

We appreciate your feedback!

