HP Business Service Management

Software Version: 9.25

Smart Card Authentication Configuration Guide

Document Release Date: December 2015
Software Release Date: December 2015

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

Trademark Notices

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

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

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

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation 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: https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HP Software Support web site at: **https://softwaresupport.hp.com**

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

HP Software 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 **https://softwaresupport.hp.com** and click **Register**.

To find more information about access levels, go to: **https://softwaresupport.hp.com/web/softwaresupport/access-levels**

HP Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hp.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Chapter 1: Introduction

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates both verifying the user's identity and allowing access to secure environments.

BSM 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 using smart cards with BSM, users can only log in using the smart card. The option of logging in by manually typing in your username and password is locked for all users unless smart card configuration is disabled.

Chapter 2: Support Matrix

This chapter contains information about which BSM components and integrations support smart card authentication.

Supported Data Collectors and Components

- Business Process Monitor
- SiteScope
- BSM Connector
- Data Flow Probe
- Service Health Analyzer
- System Health
- TransactionVision

Supported Integrations:

- RUM
- UCMDB
- Service Manager
- Release Control
- Operations Orchestration
- PAL / ALM

Limitations

- When smart card authentication configuration is enabled, clients can only use Internet Explorer with BSM. FireFox is not supported.
- The following integrations and components are not supported:
  - HP Diagnostics
  - UCMDB - BSM Downtime Integration

- Executive Scorecard
- Enterprise Collaboration
- Systinet

Chapter 3: Smart Card Authentication Configuration Workflow

This section provides the high-level workflow for configuring smart card authentication in a multi-server BSM environment. The core of the workflow is the Smart Card Authentication Configuration Wizard, which enables smart card authentication and disables other authentication methods.

1. Obtain standard Client Authentication certificate(s) from your Certificate Authority (CA). Make sure that your BSM front-end server trusts this CA. These certificates will be distributed to the data collectors and used in the web services communication. They should be issued to a valid BSM user.

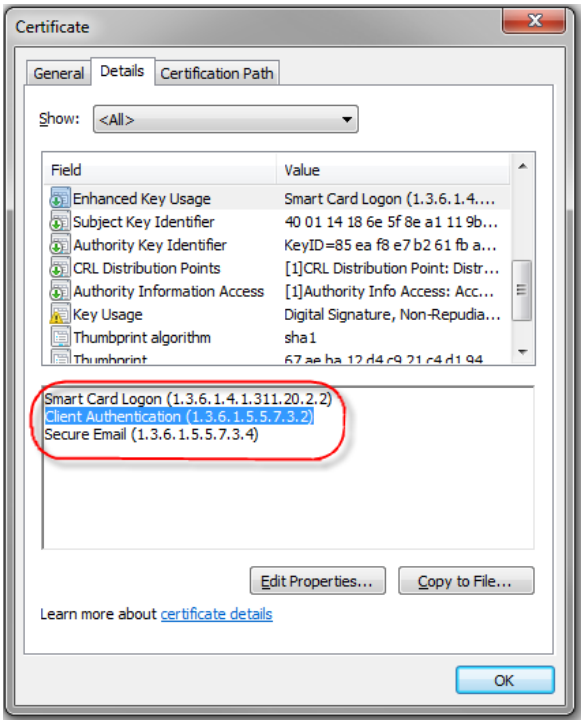
2. Verify that the Client Authentication certificate is correct.

    a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

    b. Click the **Details** tab.

    c. Click **Enhanced Key Usage**.

    d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



3. Obtain the root CA certificate and any intermediate CA certificates of the server CA used in the previous step.

4. If your BSM front-end server is a reverse proxy, perform the following steps:

   a. Follow the standard procedures for requiring a Client Authentication certificate specified on your Reverse Proxy. For details, see the third party documentation of your reverse proxy.

   b. Pass the Client Authentication certificate details in a header to the BSM Gateway server.

      This procedure differs depending on whether your reverse proxy is using the IIS or Apache web server. This procedure describes the general settings that are required, but you may need to refer to the web server documentation for the details. For details, see "How to Manually Configure Reverse Proxy for Smart Cards" on page 16.

5. Establish trust from the data collectors to the CA that issued the certificates above. Distribute the Client Authentication certificates to the data collectors and test the connections. For details, see the following topics:

   - Business Process Monitor. "Configure BPM to connect to BSM when Smart Card Authentication is Enabled" on page 19
   - System Health Analyzer. "Configuring SHA for Smart Card Authentication" on page 64
   - BSM Connector. "How to Configure BSM Connector to Connect to a BSM Server that Requires a Client Authentication Certificate" on page 39
   - SiteScope. "Configuring SiteScope with Server Side SSL (https)" on page 28
   - Data Flow Probe. "Connect the Data Flow Probe to BSM Using Client Authentication Certificates" on page 50
   - System Health. "How to install System Health in a secured environment" on page 56

6. Create a superuser in BSM and make sure there is a physical smart card with a certificate containing the user credentials (case sensitive). The user login value must be embedded in an attribute in the certificate. When you run the Smart Card Authentication Configuration Wizard you choose the attribute.

7. Enable smart card authentication on the BSM servers by running the wizard. For details, see "Smart Card Authentication on BSM Servers" on page 13.

   Note: If you enabled a Reverse Proxy on BSM, make sure you restarted the BSM servers (GW and DPS) before running this wizard.

8. Restart all BSM Gateway and Data Processing servers.

9. Verify that IIS8 is configured to support client authentication (optional).

If your front-end server is a BSM Gateway server and you are using IIS8, you may need to manually reconfigure the SSL bindings:

For example:

a. In the IIS Manager, select your web site.

b. In the actions pane, select Bindings.

c. Edit the HTTPS binding for port 443.

d. Reselect your server certificate in the SSL Certificate field and click **OK**.

10. Configure BSM to provide Client Authentication certificates.

    In some cases, the BSM server itself acts as a client with respect to other servers and must provide a Client Authentication certificate. If this is the case, it must be performed only once. For details, see "Configure BSM to Provide Client Authentication Certificate" on page 17.

11. Enable smart card authentication on the data collector or component servers. For details, see the following topics:

    - Business Process Monitor. "Configure BPM for Secure Access" on page 24
    - BSM Connector. "Setting Up Smart Card Authentication" on page 35
    - SiteScope. "Configuring SiteScope with Server Side SSL (https)" on page 28
    - System Health. "Enabling Smart Card Enforcement in System Health" on page 57

Chapter 4: Smart Card Authentication on BSM Servers

This chapter provides information about smart card authentication on BSM Gateway and Data Processing servers.

If smart card authentication is configured, you cannot log in without a valid smart card.

This chapter contains the following topics:

To access the Smart Card Authentication Configuration Wizard:

Select **Admin > Platform > Users and Permissions > Authentication Management > Smart Card Authentication Configuration > Configure** button.

How to Enable or Disable Smart Card Authentication

Smart cards are both enabled and disabled by using the Smart Card Authentication Configuration Wizard. To access the wizard, select **Admin > Platform > Users and Permissions > Authentication Management > Smart Card Authentication Configuration > Configure** button.

Note: Your machine must have the openssl command installed. This is included as part of the Apache installation included on Windows BSM environments. In Linux environments, it is sometimes included. To check if this is installed on your machine run

usr/bin/openssl

If you do not have this command, install it and make sure you can execute it from any path before configuring smart card authentication.

Smart Card Authentication Configuration Wizard Notes

The help for this wizard has been embedded in the "?" icons. The following section contains additional notes:

Server Certificate Page

Your Server Certificate Thumbprint can be found in the certificate details. To view the certificate details, the certificate must be installed into your browser (by double-clicking the certificate and using the wizard) or into the certificate store of your user account. If you installed the certificate and you are using Internet Explorer, you can view the details from **Tools > Internet Options > Content > Certificates > Personal**.

Client Certificate Page

- If you have more than one CA certificate issuer for the Client Authentication certificates (for example, there is an intermediate CA) follow the instructions below depending on your web server:
  - **IIS.** Include all entries in a .p7b file, or enter the root CA in the CA certificate issuer for the Client Authentication certificates (.cer) field and manually establish trust to the other CAs. To do so, install the certificates into the certificate store of your computer account.
  - **Apache.** Create a chain certificate of the certificates in base64 format.
- For the revocation verification method, Apache does not support online CRL or OCSP. If your revocation list is in CRL format, you need to manually download the CRL and convert it to PEM format. The conversion can be performed as seen in the following example:

  C:\HPBSM\WebServer\bin>openssl crl -inform DER -outform PEM -in <path to .crl> -out <path to .pem to be created>
- When defining the **Relevant part of the attribute** field, the attribute must be the user's unique identifier. You can find the certificate attributes in the certificate details. In Internet Explorer, these can be viewed from **Tools > Internet Options > Content > Certificates > Personal > Details > Subject** or **Subject Alternative Name**.

  If Subject has an attribute called *E*, *Email, emailaddress*, *email address*, *e-mail address*, *e-mailaddress*, *rfc822 name*, or *rfc822name*, select **SubjectDN** in the **Attribute used to identify users** field, and enter the value of the attribute in the **Relevant part of the attribute** field.

  If the Subject does not contain one of the attributes listed above, select **Subject Alternative Name** in the **Attribute used to identify users** field, and enter the attribute name (not its value) in the **Relevant part of the attribute** field. The attribute name may be one of the following: *Principal Name*, *Principalname*, *other name*, *principalname*, *principal name*, or *microsoft principal name*.

After completing the instructions in the Smart Card Authentication Configuration Wizard, BSM requires CAC authentication for all requests, including data collector API/REST calls. If there is no requirement for client certificate authentication between data collectors and BSM (SSL only), perform the following.

Note:

- With this change, the client certificate enforcements for all of the data collectors is no longer required. In other words, many of the data collector sections of the SmartCard Authentication Guide are no longer needed, as you can focus entirely on the setup of the user-related configuration that is documented in the guide.
- If you rerun the Smart Card Authentication Configuration Wizard for any reason, you need to repeat this procedure.

1. In the file **httpd-ssl.conf**, locate the following section:

```
SSLVerifyClient require
SSLVerifyDepth  10
SSLCACertificateFile /opt/HP/BSM/WebServer/conf/ssl/client_ca_root.pem
SSLOptions +ExportCertData
```

2. Wrap this section with a URL constraint as follows. This enables this particular URL to do the Smartcard authentication (and thus the PIN prompt), while the remainder of the application session will be server-authenticated https after a valid application session is established.

```
<LocationMatch ".*/topaz/login.jsp">
SSLVerifyClient require
SSLVerifyDepth  10
SSLCACertificateFile /opt/HP/BSM/WebServer/conf/ssl/client_ca_root.pem
SSLOptions +ExportCertData
</LocationMatch>
```

3. Restart the Apache web server to ensure that the configuration is activated.

How to Perform an Emergency Disable of Smart Card Authentication

Note: This procedure should only be used if you cannot access BSM normally.

If you cannot log in to BSM using any smart card and want to disable smart card authentication, run the following batch file from any BSM Gateway or Data Processing Server:

- **Windows:** <BSM Installation Directory>\bin\RevertHardening.bat
- **Linux:** <BSM Installation Directory>/bin/RevertHardening.sh

When the batch file is complete, restart all BSM Gateway Servers to activate the change.

Note: If you made any manual changes to the IIS configuration, the RevertHardening command will not disable smart card authentication. An indication that you made manual changes, is that after the RevertHardening process completes successfully, and you restart BSM on the Gateway server and open BSM in a browser, you still see the smart card authentication pop-up window. In this case:

{Vladimir will send!}

How to Manually Configure Reverse Proxy for Smart Cards

This procedure differs depending on whether your reverse proxy is using the IIS or Apache web server. This procedure describes the general settings that are required, but you may need to refer to the web server documentation for the details. It must be performed before you restart your BSM Gateway servers to enable smart card authentication.

For the IIS web server:

1. Prerequisite: IIS is already configured to require Client Authentication certificate.
2. Configure the reverse proxy to forward the encoded Client Authentication certificate in the header **CLIENT_CERT_HEADER**.

For the Apache web server:

1. Prerequisite: Apache is already configured to require a Client Authentication certificate.
2. In httpd.conf, enable the **mod_headers.so**.
3. In httpd-ssl.conf, add the following line before </VirtualHost>:

   requestHeader set CLIENT_CERT_HEADER "%{SSL_CLIENT_CERT}s"

Configure BSM to Provide Client Authentication Certificate

In some cases, the BSM server itself acts as a client with respect to other servers and must provide a Client Authentication certificate. If this is the case, it must be performed only once.

For example, this is required in the following cases:

- When SHA is enabled in your BSM deployment.
- When a data collector such as SiteScope requires a Client Authentication certificate (for example, when smart cards authentication is required by the data collector).

1. Obtain software Client Authentication certificate from your CA issued to a user with appropriate permissions for this integration. You can use one of the certificates you obtained in the beginning of the "Smart Card Authentication Configuration Workflow" on page 10.
2. If the certificate is not already in java keystore (JKS) format, convert it to JKS.

   For example, if your certificate is in pfx format, you can convert it to JKS format as seen in the following example: **keytool.exe -importkeystore -srckeystore c:\certificate.pfx -destkeystore c:\certificate.jks -srcstoretype PKCS12**
3. Open **<BSM installation directory\EjbContainer\bin\product_run.bat** on **all** BSM GW and Data Processing servers and make the following changes on each server:

   a. Add the following line somewhere before the line **set JAVA_OPTS=....**

      set SECURITY_OPTS=-Djavax.net.ssl.keyStore=<path to certificate.jks> -Djavax.net.ssl.keyStorePassword=<keystore password> -Djavax.net.ssl.keyStoreType=JKS

   b. Add the following line after the line **set JAVA_OPTS=...**

      set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%

Notes and Limitations

- User names are case sensitive.
- When smart card authentication is enabled, the JXM console can only be accessed directly from the BSM servers.
- Clients can only access BSM via Internet Explorer when smart card authentication is enabled. Firefox is not supported.
- When creating an admin user as directed in the smart card authentication wizard, make sure you enter a secure password even though no password is required for authentication with smart cards. If smart card authentication is disabled, the user will still exist on the system and if an insecure password is defined it could pose a security risk.
- If the smart card device has two client certificates issued by the same certificate authority, the Java process will always prompt the user to select one of the certificates.

Chapter 5: Configuring Business Process Monitor for Smart Card Authentication

BPM can be configured to communicate with BSM servers that have enabled smart card authentication. Additionally, the BPM servers themselves can be closed to outside communication except for connections from BSM and direct connections using localhost.

This chapter contains the following topics:

Configure BPM to connect to BSM when Smart Card Authentication is Enabled

Configuring BPM to connect to a smart card authentication enabled BSM mainly involves establishing trust to the certfiicate authority, taking a Client Authentication certificate from the certificate authority, configuring it properly, and saving it on the BPM machine. This is done in three main steps:

Step 1: Obtain a CA Root Certificate and Establish Trust

This procedure involves obtaining the root CA certificate that signs the server certificate used by BSM, converting it to the proper format, and saving it on the BPM machine. This allows BPM to trust certificates coming from this authority.

To obtain a CA root certificate:

You must obtain the root certificate from the CA that signed the BSM server certificate.

If you do not have the root certificate of the CA that signed the BSM server certificate:

1. Obtain the CA root certificates for the BSM virtual gateway (front end) server URLs.

   a. In Internet Explorer, open a secured BSM web console (https://<BSM-GW-Server>/topaz).

   b. Click the **Security Report** button (located on the right side of URL field in the Internet Explorer browser) and click the **Viewcertificates** link.

   > **Note:** If you do not see the **Security Report** button, press **Alt** on your keyboard (to expand the upper toolbar options) and click **File > Properties** and click the **Certificates** button.

   c. Click the **General** tab and check that the following certificate fields are defined correctly:

      - **issued to:** BSM's host name
      - **issued by:** SomeRoot-CA

   d. Verify that the certificate did not expire.

   e. Click the **Certificate Path** tab and click the root node of the certificate path.

   > **Note:** The certificate path may contain a chain of certificates. You will need to obtain each of the certificates in the chain.

   f. Click **View Certificate**.

   g. Click the **Details** tab and click **Copy to File**.

   h. Click **Next** and select **Base 64 encoded binary**.

   > **Note: Base 64 encoded** supports both Apache and IIS. **DER encoded** works only with IIS).

   i. Specify the certificate file name and path (for example, C:\BSM_Root).

   j. Click **Next**.

   k. Click **Finish**.

   l. Click **OK** and exit the Certificate wizard. Make sure that the server certificate file was created in the requested path (for example, C:\BSM_Root.cer).

   m. Copy the created certificate and save it on the local machine (for example, under C:\).

   n. Repeat steps e - m for each CA root certificate in the chain of certificates.

2. If you do not have a CA root certificate in PEM format, convert the certificate to **PEM** format using OpenSSL:

   a. In BPM\bin\ directory, run openssl_10_x32.exe.

   b. When prompted, enter x509 -in <Certificate file full path in Base64 format> -out <Certificate file full path in PEM format>.

      For example: `x509 -in c:\ca.cer -out c:\ca.pem`

      Troubleshooting: If you receive an error during the x509 conversion, make sure your ca.cer is Base64 encoded. To check this, open the certificate in a text editor. If it starts with -----BEGIN CERTIFICATE----- then the file is Base64 encoded, otherwise the file is DER encoded.

3. Establish trust using one of the following options:

   Option 1 - Specify the path to the CA root certificate in the user interface:

   a. In the security settings area of the user interface, set the **SSL authority certificate file** field to point to the CA root certificate file in PEM format.

   b. Click **Save** and wait for the instance to restart.

   Option 2 - Add the CA root certificate to the BPM truststore directly:

   a. Open the **BPM\dat\cert\default_auth_cert.pem** file.

   b. Append the content of the CA root certificate file (in PEM format) to the default_auth_cert.pem file you opened, and save it.

   c. Restart BPM.

Step 2: Obtain and Configure the CA Issued Client Authentication Certificate

To work with a CA Client Authentication certificate:

1. Request a Client Authentication certificate from your CA with keys marked as exportable, then export the certificate in PFX format with a password protected private key.

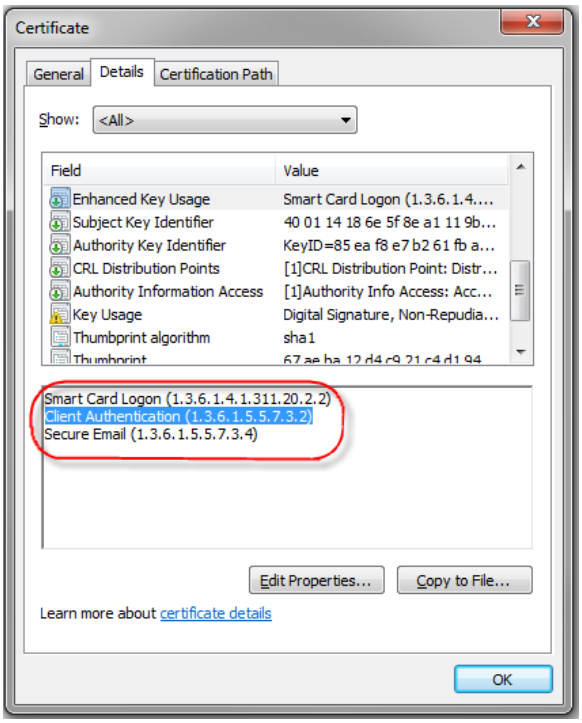
2. Verify that the Client Authentication certificate is correct.

   a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

   b. Click the **Details** tab.

c. Click **Enhanced Key Usage**.

d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



3. Split the Client Authentication certificate into two files in PEM format using OpenSSL:
   a. In the BPM\bin\ directory, run openssl_10_x32.exe.

   b. For setting the **SSL client certificate file** field in the security settings, when prompted enter pkcs12 -in <CA Client Authentication certificate in PFX format> -clcerts -nokeys -out <BPM Client Authentication certificate in PEM format>.

      For example, if the Client Authentication certificate in PFX format is bpm_client.pfx, enter: pkcs12 -in c:\bpm_client.pfx -clcerts -nokeys –out c:\bpm_client_cert.pem.

      Then set the **SSL client certificate file** field to point to <BPM Client Authentication certificate in PEM format>.

   c. For setting the **SSL private key file** field in the security settings, when prompted enter pkcs12 -in <CA Client Authentication certificate in PFX format> -out <BPM private key in PEM format> -nodes.

      For example, if the Client Authentication certificate in PFX format is bpm_client.pfx, enter: pkcs12 -in c:\bpm_client.pfx -out c:\bpm_client_key.pem -nodes.

      Then set the **SSL private key file** field to point to <BPM private key in PEM format>.

Step 3: Complete the SSL Settings in the BPM Instance Page

To access the Business Process Monitor Instance page, select an instance entity in the Business Process Monitor tree displayed in the left pane of the Business Process Monitor Admin console.

1. Open the Configuration Tab and locate the Security Settings Area.
2. Complete the user interface elements described below:

UI Element	Description
SSL Settings **Note:** • All certificates must be Base64 encoded. • Self-signed certificates are not supported.	
SSL client certificate file	**Note:** This field is relevant if the BSM Gateway server requires client-side certification. The path of the PEM file that holds the client-side certificate. **Syntax exceptions:** You cannot use a UNC (Uniform Naming Convention) path.
SSL private key file	**Note:** This field is relevant if the BSM Gateway server requires client-side certification. The path of the PEM file that holds the private key used as a public/private pair key for the public key in the client-side certificate. **Syntax exceptions:** You cannot use a UNC (Uniform Naming Convention) path.
SSL private key password	**Note:** This field is relevant if the BSM Gateway server requires client-side certification. The password of the private key, if the private key was encrypted with a password.
SSL authority certificate file	If the BSM Gateway server to which BPM connects is configured for SSL, enter the full path to the CA root certificate file for the authority that issued the **BSM server** certificate. Alternatively, you can add a CA root certificate file to BPM, in which case leave this field empty. **Syntax exceptions:** You cannot use a UNC (Uniform Naming Convention) path.

UI Element	Description
SSL host name validation	The type of host name validation. Valid types are: • Full • No host name validation • None **Default value:** Full (recommended)

Configure BPM for Secure Access

The BPM console cannot fully support smart card authentication because it does not normally require user authentication.

The solution that BPM provides is to disable open access to the BPM console, and only allow access directly from BSM or locally from a BPM server.

How to Restrict Access to BPM Admin

You can configure secure access for BPM Admin, thereby controlling who can access the BPM Admin user interface. When secure access is activated, access to BPM Admin is limited to:

- Local users (that is, those users who connect to BPM Admin on the actual BPM machine using the URL http://localhost:2696).
- Users who access a BPM Admin from BSM (select **Admin > End User Management > Settings > BPM Agents**, select a BPM and click the **Open a Business Process Monitor Agent's Console** button) sending the configured authentication.

  For more details, see the Business Process Monitor Administrator's Guide.

To configure BPM for secure access:

1. In BSM, select **Admin > Platform > Users and Permissions > Authentication Management**.
2. Copy the value of the **Token Creation Key (initString)** property.
3. On the BPM machine, paste the copied value in the **initString** parameter in the **<BPM installation directory>\ServletContainer\webapps\ROOT\WEB-INF\classes\lwssofmconf.xml** file. For example:

```
<lwssoValidation id="ID000001">
                    <domain></domain>
```

```
                    <crypto cipherType="symmetricBlockCipher"
directKeyEncoded="false" directKeyEncoding="Hex"
                            encodingMode="Base64Url" engineName="AES"
initString="<copied value from BSM>" keySize="256"
paddingModeName="CBC"/>
                </lwssoValidation>
```

4. On the BPM machine, edit the **<BPM installaiton directory>\config\topaz_agent_ctrl.cfg** file and in the **General** section, change the setting for the **SecureAccess** parameter to **1**.

   Note: If this parameter does not exist, add it to the file.

Configure SSL Support for BPM Admin

When you connect to BPM Admin from a remote machine using a browser, information is sent using http. This means that the data that you configure in BPM Admin, including passwords (for example, when adding/configuring a BPM instance), is sent "as is", in plain text. The passwords are encrypted only after arriving at the BPM Admin machine.

If you want this data to be sent encrypted, it is possible to configure BPM Admin to work with SSL. This enables all communication between the remote browser and BPM Admin to be encrypted. The following procedure describes how to set BPM Admin to run using SSL configuration.

To configure BPM Admin to run using SSL:

1. Obtain or create the server certificate in one of the following methods:

   Option 1: Obtain the server certificate from your corporate Certificate Authority in **.pfx (PKCS12)** format and skip to "Modify the server.xml:" on the next page.

   Option 2: Create a java keystore with the server certificate as follows (replace the string "changeit" below with your password):

   a. Generate a keystore with a private key.

      ```
      keytool.exe -genkeypair -validity 1065 -keysize 2048 -keyalg rsa -keystore mykeystore -storepass changeit -alias myserver.mydomain
      ```

      Where validity (in days) and keysize depend on your certificate authority requirements.

   b. Generate a server certificate request to have it signed by your internal certificate authority.

      ```
      keytool.exe -keystore mykeystore -storepass changeit -alias myserver.mydomain -certreq -file CERTREQFILE.csr
      ```

   c. Download the signed server certificate **cert_signed.cer** from your certificate authority.

d. Obtain the root authority certificate **CA.crt** (and any intermediate authority certificates if applicable).

e. Import the root certificate authority certificate (and any intermediate authority certificates if applicable) into the keystore created earlier in this procedure.

```
keytool.exe -import -trustcacerts -keystore mykeystore -storepass changeit -alias myRootCA -file CA.crt
```

f. Import the signed certificate into the same keystore under the original alias.

```
keytool -import -v -alias myserver.mydomain -file cert_signed.cer -keystore mykeystore -keypass changeit -storepass changeit
```

g. Verify that the keystore contains at least two entries: **Trusted Cert Entry** and **Private Key Entry**.

```
keytool -list -keystore mykeystore
```

2. Modify the server.xml:

a. Open the **<Business Process Monitor root directory>\ServletContainer\conf\server.xml** file in a text editor.

b. Uncomment the section with Connector port="8443":

```
<--!

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxthreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS" />

-->
```

c. Add information about your keystore (location, password, type). If your server certificate is in PKCS12 format, the keystore type should be **"PKCS12"**. Otherwise, it should be **"JKS"**. For example:

```
keystoreFile="c:\mykeystore" keystoreType="JKS"
keystorePass="myprivatekeypassword"
```

The section should now look similar to this:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxthreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

keystoreFile="c:\mykeystore" keystoreType="JKS"
keystorePass="myprivatekeypassword"

/>
```

d. Save your changes.

3. Import the root authority certificate into the trustore used by BPM:

```
cd <BPM root directory>/JDK/bin

> keytool -import -alias <myCA> -file c:\myCArootcert.cer -keystore

..\lib\security\cacerts -trustcacerts -storepass changeit
```

4. Restart BPM.

5. Verify that you can open the BPM Admin console using the secure connection:

```
https://<BPM server FQDN>:8443
```

6. When you have succeeded in connecting securely, close the unsecure port in the server.xml by commenting out the section with Connector port="2696".

7. Restart BPM.

8. On the BPM server, modify the shortcut to the BPM Admin Console to use the secure URL.

9. In End User Management Administration in BSM, modify the **BPM console URL** to use the secure connection. For details, see "Edit Business Process Monitor Properties Dialog Box" in the BSM Application Administration Guide.

Troubleshooting

If it is still impossible to access the BPM Admin console via SSL, check the latest **catalina.<current date>.log** file located in:

- **Windows Server 2003 and Windows XP** – C:\Documents and Settings\All Users\Application Data\HP\BPM\Tomcat\logs
- **Windows Server 2008, and Windows 7** – C:\ProgramData\HP\BPM\Tomcat\logs

Chapter 6: Configuring SiteScope for Smart Card Authentication

SiteScope can be configured to communicate with BSM servers that have enabled smart card authentication. Additionally, the SiteScope servers themselves can be configured to support smart card authentication.

This chapter contains the following topics:

Configuring SiteScope with Server Side SSL (https)

You can use the SiteScope Hardening Tool to configure SiteScope to work over SSL (https).

To configure SiteScope to work over SSL:

1. Run the SiteScope Hardening Tool. For details, see "Using the SiteScope Hardening Tool" on page 30.
2. When prompted in the tool, select the option "Configuring SiteScope Standalone to work over SSL (https)".

   Alternatively, if you want to perform all the hardening configuration tasks listed in "Using the SiteScope Hardening Tool" on page 30, select the option "Full SiteScope hardening configuration (all of the configuration options)".
3. Confirm that you want to configure SiteScope to work over SSL.
4. Select one of the following methods to create the SiteScope server keystore to hold the SiteScope server certificate:

   - **Import a server keystore in .jks format.**

     The tool prompts you to select an alias in which the key for SiteScope SSL authentication is located.

Follow the instructions in the tool.

- **Create a server keystore by signing a request on a certified Certificate Authority server.**

  Selecting this option creates a new keystore and generates a key request to a certificate authority for a signed certificate. The generated certificate is then imported into the keystore.

  The tool prompts you to enter server keystore parameters. We recommend that for the Common Name, you enter your machine's URL (for example, `yourserver.domain.com`), and for the alias name, your machine's name (for example, `yourserver`).

- **Import a server keystore from a server certificate in .pfx format.**

  Selecting this option creates a keystore from a certificate in **.pfx** format. This certificate must contain its private key.

  The SiteScope Hardening Tool automatically ensures that the keystore password and the private key are the same each time a keystore is created.

5. Enter a username property for the Client Authentication certificate. The default username is `Other Name`.

   The server certificate is imported to the server keystore. The certificate alias appears in the tool.

6. Confirm if you want to enable SiteScope client authentication.

   If you enable client SSL authentication, SiteScope performs full client SSL authentication upon the SSL handshake and extracts a Client Authentication certificate. This Client Authentication certificate is checked against the SiteScope user management system.

7. Confirm if you want to enable smart card enforcement.

   If you enable smart card enforcement, SiteScope verifies that the Client Authentication certificate originates from a hardware device. For more details about smart card enforcement, see "Configuring Smart Card Authentication Enforcement" on page 32.

8. Enter a password for the SiteScope server TrustStore. The default password is `changeit`.

   For SiteScope to trust a Client Authentication certificate, SiteScope must trust the Certificate Authority that issued the Client Authentication certificate. For SiteScope to trust a Certificate Authority, the Certificate Authority's certificate must be stored in the SiteScope server and main TrustStores. To import Certificate Authority certificates into SiteScope TrustStores, see "Importing Certificate Authority Certificates into SiteScope TrustStores" on page 32.

Changes in configuration take effect only after you exit the SiteScope Hardening Tool.

Using the SiteScope Hardening Tool

The SiteScope Hardening Tool enables you to configure SiteScope to perform a full or partial hardening of SiteScope.

You can use the SiteScope Hardening Tool to perform all or a combination of the following configuration tasks:

- Configure SiteScope to work over SSL.
- Enable smart card enforcement.
- Configure SiteScope and SiteScope public API client for client certificate authentication.
- Import Certificate Authority certificates into SiteScope TrustStores.
- Configure SiteScope to verify Client Authentication certificate revocation via CRL and OCSP.
- Configure SiteScope integration with BSM when BSM requires Client Certificate Authentication. For details, see *Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate* in the HP SiteScope Deployment Guide.
- Configure JMX remote access.

  For details, see the HP SiteScope Deployment Guide.

Running the SiteScope Hardening Tool

To run the SiteScope Hardening Tool, do the following:

1. (Optional) If you want to enable LDAP user authentication, configure LDAP integration before running the tool:

   a. Configure the LDAP server on SiteScope. For details, see "How to Set Up SiteScope to Use LDAP Authentication" in the Using SiteScope Guide in the SiteScope Help.

   b. Create a new role in SiteScope user management for LDAP users.

   c. Change the SiteScope administrator login name to the email address of a user located in LDAP. Do not enter a password.

2. Stop the SiteScope service:

   Windows:

- If you are running SiteScope from go.bat, close the command line terminal or press **CTRL+C**.
- If you are running SiteScope as a service:
  i. In Windows Explorer, search for **services**. The Component Services window opens.
  ii. In the left pane, select Services (Local).
  iii. In the services list in the center pane, select **HP SiteScope**.
  iv. In the area to the left of the service list, click **Stop the service**.

Linux:

Run the command line:

```
cd /opt/HP/SiteScope/
./stop
```

Caution: You should *not* run the SiteScope Hardening Tool when SiteScope is running.

3. Start the tool by running the command line:

   Windows:

   ```
   <SiteScope Installation directory>\tools\SiteScopeHardeningTool>
   runSSLConfiguration.bat
   ```

   Linux:

   ```
   cd <configuration tool directory>
   ./runSSLConfiguration.sh
   ```

   The SiteScope Hardening Tool opens.

4. When prompted in the tool, select the option "SiteScope hardening configuration". The existing SiteScope configuration is automatically backed up.

5. When prompted, enter a backup description to allow easy recognition in case you want to restore that backup in the future.

   Note: When using the SiteScope Hardening Tool, the Tomcat configuration **server.xml** file in the **/opt/HP/SiteScope/Tomcat/conf** directory is overwritten and any modifications made to that file before running the tool are removed. To restore these modifications, you must reapply them to this file after running the tool.

6. Select one or a combination of the tasks listed above. If you want to perform all of these tasks, select the option "Full SiteScope hardening configuration (all of the configuration options)".

For details on using the SiteScope Hardening Tool to perform configuration tasks, see the task list above.

Note: Changes in configuration take effect only after you exit the SiteScope Hardening Tool.

Configuring Smart Card Authentication Enforcement

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates both verifying the user's identity and allowing access to secure environments.

SiteScope supports user authentication using smart cards. If smart card authentication is configured, you cannot log in to SiteScope without a valid smart card.

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

When SiteScope is configured for smart card authentication, users can log in to SiteScope only with a valid smart card. The option of logging in by manually typing in your username and password is locked for all users unless smart card configuration is disabled.

If smart card authentication is configured in BSM and you want to integrate SiteScope with BSM, you must configure SiteScope smart card authentication to authenticate the BSM Client Authentication certificate. For details, see "Enabling Smart Card Enforcement" below.

Enabling Smart Card Enforcement

To enable SiteScope smart card authentication, you should use the SiteScope Hardening Tool to configure SiteScope to work over SSL. For details, see "Configuring SiteScope with Server Side SSL (https)" on page 28. When prompted in the tool, enable smart card enforcement.

Note: If smart card enforcement is enabled, the only supported browser is Internet Explorer running on a Windows operating system.

If smart card enforcement is disabled, but client certificate authentication is enabled, to use SiteScope in Firefox, see "Using Firefox When Client Certification is Enabled" on page 34.

Importing Certificate Authority Certificates into SiteScope TrustStores

For SiteScope to trust a Client Authentication certificate, SiteScope must trust the Certificate Authority that issued the Client Authentication certificate. For SiteScope to trust a Certificate Authority, the

Certificate Authority's certificate must be stored in the SiteScope server and main TrustStores.

The SiteScope server TrustStore is responsible for authentication of all incoming connection request from clients (API and browsers).

The SiteScope main TrustStore is a Certificate Authority Java TrustStore that is located in Java directory in the SiteScope install directory. This TrustStore is responsible for SiteScope certificate management.

You use the SiteScope Hardening Tool to import Certificate Authority certificates into SiteScope server and main TrustStores.

Note: Before importing Certificate Authority certificates into SiteScope TrustStores, you must configure SiteScope to work over SSL by importing a SiteScope server certificate into the SiteScope server keystore.

If you have not already done this, the SiteScope Hardening Tool prompts you to perform a full SiteScope hardening configuration. For details, see "Configuring SiteScope with Server Side SSL (https)" on page 28.

To import Certificate Authority certificates into SiteScope TrustStores:

1. Run the SiteScope Hardening Tool. For details, see "Using the SiteScope Hardening Tool" on page 30.
2. When prompted in the tool, select the option "Import CA certificates into SiteScope main and server trustStores".
3. Follow the instructions in the tool.

Tips:

- The tool accepts file paths in regular Windows format only. In UNIX format, where a blank space in a file path is preceded by a backslash (“\”) to indicate that a blank space follows, you should remove the backslash.

Format	File path
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** change to: **/user/temp dir/certificate.cer**

- Changes in configuration take effect only after you exit the SiteScope Hardening Tool.

Using Firefox When Client Certification is Enabled

If smart card enforcement is disabled, but client certificate authentication is enabled, to open the SiteScope user interface in Firefox, you must:

1. Import your personal certificate into Firefox, as follows:

    a. In Firefox, go to **Tools** > **Options** > **Advanced** > **Encryption** > **View Certificates**. The Certificate Manager dialog box opens.

    b. Click **Import...** and open your personal certificate in **.pfx** (or **.p12**) file format. The Password Entry Dialog dialog box opens.

    c. Enter the password used to encrypt this certificate backup and click **OK**. The certificate appears in the Certificate Manager dialog box, confirming that the certificate is added to Firefox.

2. Import your personal certificate into the client JRE, as follows:

    a. In the JRE, open the Java Control Panel.

    b. Go to **Security > Certificates** and select Client Authentication as the Certificate type.

    c. Click **Import** and open the Client Authentication certificate that you imported into Firefox.

    d. Click **OK**. The personal certificate appears in the JRE.

3. Enter the SiteScope URL in Firefox. The User Identification Request dialog box opens. Select the personal certificate that you created in step 1 to present as identification.

Chapter 7: Configuring BSM Connector for Smart Card Authentication

This chapter contains the following topics:

Setting Up Smart Card Authentication

BSM Connector supports user authentication using smart cards. If smart card authentication is configured, you cannot log in without a valid smart card.

This section includes:

Configure BSM Connector to Connect to a BSM Server That Requires Smart Card Authentication

BSM Connector can be configured to communicate with BSM servers that have enabled smart card authentication.

1. Configure BSM Connector to connect to a BSM server that requires a Client Authentication certificate. By completing this step, you ensure that metrics data is sent and indicator data is received securely.

   For details, see "How to Configure BSM Connector to Connect to a BSM Server that Requires a Client Authentication Certificate" on page 39.

2. Configure BSM Connector to send topology to a BSM server that requires a Client Authentication certificate. By completing this step, you ensure that topology data is sent securely.

   "How to Configure the Topology Discovery Agent in BSM Connector when the BSM Server Requires a Client Authentication Certificate" on page 44.

Enable Smart Card Authentication in BSM Connector

To configure smart card authentication in BSM Connector, complete the following tasks:

1. Stop BSM Connector:

   Windows: Stop the **HP BSM Connector** service in the **Administrative Tools > Services**.

   Linux: Stop the BSM Connector main process, type `/opt/HP/BSMConnector/stop`.

2. Configure the BSM Connector Tomcat server to require a Client Authentication certificate for mutual authentication:

   a. Configure the Tomcat server to request a Client Authentication certificate by locating the following section of the **<BSM Connector root directory>/Tomcat/conf/server.xml** configuration file:

   ```
   <Connector port="30000" maxThreads="150"
              minSpareThreads="25" maxSpareThreads="75"
              enableLookups="true" disableUploadTimeout="true"
              acceptCount="100" debug="0"
              scheme="https" secure="true" clientAuth="false"
              sslProtocol="TLS"
              keystore="../groups/serverKeystore"
              keystoreType="JKS"
              keystorePass="changeit"/>
   ```

   Note: The keystore password must be the same as the one set for the BSM Connector keystore in "How to Prepare BSM Connector for Using SSL" on page 44.

   Change clientAuth="true", and add the following attributes:

   ```
              clientAuth="true"
              ...
              truststoreFile="../templates.certificates/truststore.jks"
              truststorePass="changeit"
              truststoreType="JKS"
    />
   ```

   b. Import the certificate of your certificate authority to the BSM Connector Tomcat truststore (**<BSM Connector root directory>/templates.certificates/truststore.jks**) by running the command from the **<BSM Connector root directory>/java/bin** directory:

```
keytool -import -trustcacerts -alias <your alias> -keystore <BSM Connector
root directory>/templates.certificates/truststore.jks -file <certificate
file>
```

3. Import the HP Operations Agent certificate to the BSM Connector Tomcat truststore:

   a. On the BSM Connector system, use the **ovcoreid** command line tool to find out the core ID:

   ```
   ovcoreid
   ```

   b. Export the HP Operations Agent certificate to a file, type:

   ```
   ovcert -exportcert -file agent_client.p12 -alias <core ID>
   ```

   c. Import the HP Operations Agent certificate to the Tomcat truststore:

   ```
   <BSM Connector root directory>/java/bin/keytool -importkeystore -srckeystore
   agent_client.p12 -srcstoretype pkcs12 -srcalias <core ID> -destkeystore <BSM
   Connector root directory>/templates.certificates/truststore.jks -destalias
   agentcert
   ```

4. Modify the following parameters of the Java Virtual Machine:

   Windows:

   a. Edit the BSM Connector's service key in the registry. Use regedit to open the Registry Editor.

   b. In the Registry Editor, navigate to `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/<BSM Connector service name>/serviceParam`. The default service name is `HP BSM Connector`.

   c. Modify the serviceParam default and add the following properties, for example at the beginning of the data string:

   ```
   -Djavax.net.ssl.keyStore="<full_path_to_keystore.jks>"
   -Djavax.net.ssl.keyStorePassword=<keystore_pass>
   ```

   Example:

   ```
   -Djavax.net.ssl.keyStore="<BSM Connector root
   directory>/templates.certificates/.ks"
   -Djavax.net.ssl.keyStorePassword=<keystore_pass>
   ```

   Linux:

   a. Navigate to `<BSM Connector root directory>/bin` and edit the `start-monitor` script.

   b. In the script, add the following properties to the `JAVA_OPTS` section:

```
-Djavax.net.ssl.keyStore=<full_path_to_keystore.jks>
-Djavax.net.ssl.keyStorePassword=<keystore_pass>
```

Example:

```
-Djavax.net.ssl.keyStore="<BSM Connector root
directory>/templates.certificates/.ks"
-Djavax.net.ssl.keyStorePassword=<keystore_pass>
```

5. Start BSM Connector:

   Windows: Start the **HP BSM Connector** service in the **Administrative Tools > Services**.

   Linux: Start the BSM Connector main process, type `/opt/HP/BSMConnector/start`.

6. Add users to BSM Connector using the BSM Connector **user** command line tool:

   a. In the Subject Alternative Name (SAN) field of the certificate, look for the value of the User Principal Name (UPN) in Other Name (OID: 1.3.6.1.4.1.311.20.2.3).

   b. Use the **user** command line tool to add a user to BSM Connector:

   ```
   user -add <value of UPN> <password>
   ```

   Note: The user tool requires a password for each user. However, the password is not used when logging into BSM connector using a smart card. Users must enter their smart card PIN instead.

Disable Smart Card Authentication in BSM Connector

1. Edit the following section in the **<BSM Connector root directory>/Tomcat/conf/server.xml** configuration file:

```
<Connector port="30000" maxThreads="150"
           minSpareThreads="25" maxSpareThreads="75"
           enableLookups="true" disableUploadTimeout="true"
           acceptCount="100" debug="0"
           scheme="https" secure="true" clientAuth="true"
           sslProtocol="TLS"
           keystore="../groups/serverKeystore"
           keystoreType="JKS"
           keystorePass="changeit"
           truststoreFile="../templates.certificates/truststore.jks"
           truststorePass="changeit"
           truststoreType="JKS"
/>
```

2. Change `clientAuth="false"`.
3. Restart BSM Connector:

   Windows: Restart the **HP BSM Connector** service in the **Administrative Tools > Services**.

   Linux: Restart the BSM Connector main process, type `/opt/HP/BSMConnector/stop` followed by `/opt/HP/BSMConnector/start`.

How to Configure BSM Connector to Connect to a BSM Server that Requires a Client Authentication Certificate

This task describes the steps involved in enabling secure communication between BSM Connector and BSM when the BSM server requires a Client Authentication certificate. By completing this procedure, you ensure that metrics data is sent and indicator data is received securely.

1. If you obtained the Client Authentication certificate in Java keystore (JKS) format, copy it to the **<BSM Connector root directory>/templates.certificates** directory, and then continue with "Check the keystore contents." on page 42.

   If the Client Authentication certificate already exists in PKCS#12 format, convert it to JKS format using the following command from the **<BSM Connector root directory>/java/bin** directory, and then continue with "Check the keystore contents." on page 42:

   ```
   keytool -importkeystore -srckeystore <keystore with Client Authentication
   certificate>.pfx -destkeystore <BSM Connector root
   directory>/templates.certificates/.ks -srcstoretype PKCS12
   ```

   Example:

   ```
   keytool -importkeystore -srckeystore c:\client.pfx -destkeystore
   C:\BSMConnector\templates.certificates\.ks -srcstoretype PKCS12
   ```

   Note:

   - Make sure the Client Authentication certificate is issued to an existing BSM user.
   - Make sure that the private key password is at least six characters long, and that the private key and keystore passwords are the same.
   - Make sure that the above keystore contains the CA certificate that issued it.

Otherwise, perform the following steps (if you did not obtain the Client Authentication certificate in JKS or PKCS#12 format). See also the section "Creating a Keystore" in the BSM Hardening Guide.

a. Create a keystore under **<BSM Connector root directory>/templates.certificates** by running the following command from the **<BSM Connector root directory>/java/bin** directory:

   ```
   keytool -genkeypair -keyalg RSA -alias bsmc -keystore <BSM Connector root directory>/templates.certificates/.ks -storepass <your_keystore_password>
   ```

   Example:

   ```
   keytool -genkeypair -keyalg RSA -alias bsmc -keystore
   C:\BSMConnector\templates.certificates\.ks -storepass changeit
   What is your first and last name?
   [Unknown]: domain.name
   What is the name of your organizational unit?
   [Unknown]: dept
   What is the name of your organization?
   [Unknown]: XYZ Ltd
   What is the name of your City or Locality?
   [Unknown]:  New York
   What is the name of your State or Province?
   [Unknown]:  USA
   What is the two-letter country code for this unit?
   [Unknown]:  US
   Is CN=domain.name, OU=dept, O=XYZ Ltd, L=New York, ST=USA, C=US correct?
   [no]:  yes
   Enter key password for <BSM Connector>
   Press Enter to use the same password as the keystore password.
   ```

b. Create a certificate request for this keystore by running the following command from the **<BSM Connector root directory>/java/bin** directory:

   ```
   keytool -certreq -alias bsmc -file c:\bsmc.csr -keystore <BSM Connector root directory>\templates.certificates\.ks -storepass <your_keystore_password>
   ```

   Example:

   ```
   keytool -certreq -alias bsmc -file c:\bsmc.csr -keystore
   C:\BSMConnector\templates.certificates\.ks -storepass changeit
   ```

c. Have your certificate authority sign the certificate request. Copy and paste the contents of the .csr file into your Certificate Authority Web form.

d. Download the signed Client Authentication certificate in BASE-64 format to **<BSM**

Connector root directory>/templates.certificates/clientcert.cer.

e. Download the certificate authority certificate in BASE-64 format to **c:**.

f. Import the certificate authority certificate into the JKS keystore by running the following command:

```
keytool -import -alias ca -file c:\ca.cer -keystore <BSM Connector root
directory>/templates.certificates/.ks -storepass <your_keystore_password>
```

Example:

```
keytool -import -alias ca -file c:\ca.cer -keystore
C:\BSMConnector\templates.certificates\.ks -storepass changeit
Owner: CN=dept-CA, DC=domain.name
Issuer: CN=dept-CA, DC=domain.name
Serial number: 2c2721eb293d60b4424fe82e37794d2c
Valid from: Tue Jun 17 11:49:31 IDT 2008 until: Mon Jun 17 11:57:06 IDT
2013
Certificate fingerprints:
MD5:  14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
SHA1: 17:2F:4E:76:83:5F:03:BB:A4:B9:96:D4:80:E3:08:94:8C:D5:4A:D5
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

g. Import the Client Authentication certificate into the keystore by running the following command:

```
keytool -import -alias bsmc -file <BSM Connector root
directory>/templates.certificates/certnew.cer -keystore <BSM Connector root
directory>/templates.certificates/.ks -storepass <your_keystore_password>
```

Example:

```
keytool -import -alias bsmc -file
c:\BSMConnector\templates.certificates\certnew.cer -keystore
C:\BSMConnector\templates.certificates\.ks -storepass changeit
```

The certificate reply is installed in the keystore **<BSM Connector root directory>/java/bin** directory.

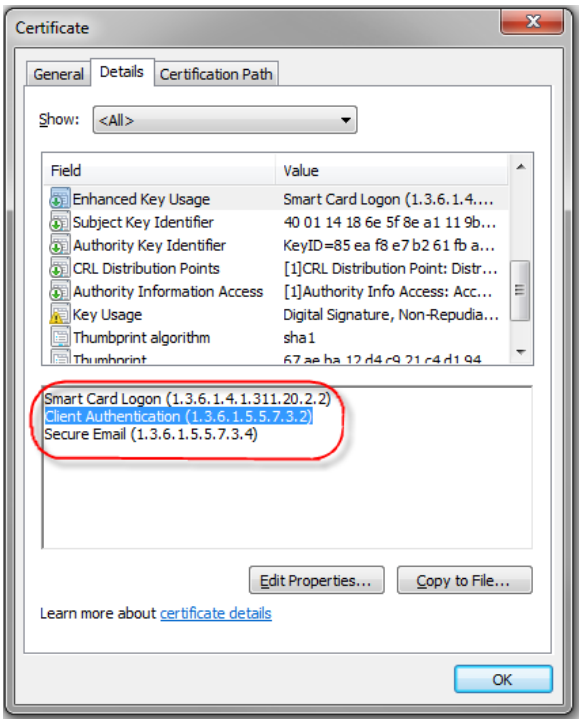
2. Verify that the Client Authentication certificate is correct.

a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

b. Click the **Details** tab.

c. Click **Enhanced Key Usage**.

d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



3. Check the keystore contents.

   Run the following command from the **<BSM Connector root directory>/java/bin** directory, and enter the keystore password:

   ```
   keytool -list -keystore <BSM Connector root
   directory>/templates.certificates/.ks
   ```

   Example:

   ```
   keytool -list -keystore C:\BSMConnector\templates.certificates\.ks
   Enter keystore password:  changeit

   Keystore type: jks
   Keystore provider: SUN

   Your keystore contains 2 entries

   ca, Mar 8, 2012, trustedCertEntry,
   Certificate fingerprint (MD5):
   14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
   bsmc, Mar 8, 2012, keyEntry,
   ```

```
Certificate fingerprint (MD5):
C7:70:8B:3C:2D:A9:48:EB:24:8A:46:77:B0:A3:42:E1
```

4. To use this keystore for Client Authentication certificate, add the following lines to the **<BSM Connector root directory>/groups/master.config** file:

   ```
   _urlClientCert=<keystoreName>
   _urlClientCertPassword=<keystorePassword>
   ```

   Example:

   ```
   _urlClientCert=.ks
   _urlClientCertPassword=changeit
   ```

5. Save the changes to the file.

6. Restart the BSM Connector server:

   Windows: Restart the **HP BSM Connector** service in the **Administrative Tools > Services**.

   Linux: Restart the BSM Connector main process, type `/opt/HP/BSMConnector/stop` followed by `/opt/HP/BSMConnector/start`.

7. In BSM, select **Admin > Integrations > BSM Connector Integrations**, and click the **New BSM Connector** button to add the BSM Connector instance.

Troubleshooting

If the connection between BSM Connector and BSM fails, check the following log files for errors:

- BSM Connector system:

  <BSM Connector root directory>/log/bac_integration.log

- BSM Gateway Server:

  <HPBSM root directory>/log/topaz_all.ejb.log

  Check for the following error:

  ```
  javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException:
  PKIX path building failed:
  sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
  certification path to requested target
  ```

  Possible solutions: The error indicates one of the following:

- The CA root certificate was not imported into the BSM JVM.
- The BSM server was not restarted after the import. (A server restart is always required after a certificate import.)

How to Prepare BSM Connector for Using SSL

BSM Connector is shipped with a self-signed certificate. You must replace the certificate with a certificate issued by your Certificate Authority (CA) as described below.

1. Obtain a server certificate from your CA issued to the BSM Connector server. Typically this certificate is issued in PKCS12 format with a password-protected private key.
2. Change the Tomcat configuration to use the PKCS12 certificate instead of the default self-signed Java certificate. Locate the following lines in the **<BSM Connector root directory>/Tomcat/conf/server.xml** configuration file:

   ```
   keystore="../groups/serverKeystore" keystoreType="JKS"
   keystorePass="changeit"/>
   ```

   Change them to:

   ```
   keystore="path to server certificate in PKCS12 format"
   keystoreType="PKCS12"
   keystorePass="password for the private key"
   ```

   Restart Tomcat.

If you cannot obtain a server certificate from a CA in PKCS12 format, manually generate a server certificate using a Java Keystore (JKS) and have it signed by your CA. See the section "Creating a Keystore" in the BSM Hardening Guide.

Note: The private key password must be at least six characters, and the password for the private key and password for the keystore must be the same.

How to Configure the Topology Discovery Agent in BSM Connector when the BSM Server Requires a Client Authentication Certificate

After configuring BSM Connector to connect to the BSM Gateway Server using a Client Authentication certificate (see "How to Configure BSM Connector to Connect to a BSM Server that Requires a Client Authentication Certificate" on page 39), you need to perform the following steps for discovery to report topology to the BSM server.

1. Import the Certificate Authority (CA) certificate (or BSM server certificate) into the discovery truststore (**<BSM Connector root directory>/WEBINF/classes/security/MAMTrustStoreExp.jks**) with the password **logomania**, which encrypted, is: **[22,-8,116,-119,-107,64,49,93,-69,57,-13,-123,-32,-114,-88,-61]**):

   ```
   keytool -import -alias <your_CA> -file <certificate file> -keystore <BSM
   Connector root directory>/WEB-INF/classes/security/MAMTrustStoreExp.jks
   -storepass logomania
   ```

   Example:

   ```
   keytool -import -alias AMQA_CA -file c:\ca.cer -keystore
   C:\BSMConnector\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass
   logomania
   ```

   Note:

   - The default discovery keystore password is logomania. We highly recommend that you do not change the default password.
   - The private key password must be at least six characters, and the password for the private key and password for the keystore must be the same.

2. Check the contents of the truststore using the following command:

   ```
   keytool -list -keystore <BSM Connector root directory>/WEB-
   INF/classes/security/MAMTrustStoreExp.jks -storepass logomania

   Keystore type: <Keystore_type>
   Keystore provider: <Keystore_provider>

   Your keystore contains 2 entries

   mam, Nov 4, 2004, trustedCertEntry,Certificate fingerprint (MD5):
   <Certificate_fingerprint>
   amqa_ca, Dec 30, 2010, trustedCertEntry,Certificate fingerprint (MD5):
   <Certificate_fingerprint>
   ```

   Example:

   ```
   keytool -list -keystore C:\BSMConnector\WEB-INF\classes\security\
   MAMTrustStoreExp.jks -storepass logomania

   Keystore type: JKS
   Keystore provider: SUN

   Your keystore contains 2 entries
   ```

```
mam, Nov 4, 2004, trustedCertEntry,
Certificate fingerprint (MD5):
C6:78:0F:58:32:04:DF:87:5C:8C:60:BC:58:75:6E:F7
amqa_ca, Dec 30, 2010, trustedCertEntry,
Certificate fingerprint (MD5):
5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB
```

3. Copy the BSM Connector client keystore (.ks) from **<BSM Connector root directory>/templates.certificates** to **<BSM Connector root directory>/WEB-INF/classes/security/**.

4. In the **ssl.properties** file, update the **javax.net.ssl.keyStore** property to the keystore name. For example, `javax.net.ssl.keyStore=.ks`.

5. Change the BSM Connector client keystore password to match the discovery keystore password (logomania).

   ```
   keytool -storepasswd -new logomania -keystore <BSM Connector root
   directory>/WEB-INF/classes/security/.ks -storepass <your_keystore_password>
   ```

   Example:

   ```
   keytool -storepasswd -new logomania -keystore C:\BSMConnector\WEB-
   INF\classes\security\.ks -storepass changeit
   ```

6. Change the private key password to match the discovery keystore password:

   ```
   keytool -keypasswd -alias bsmc -keypass <your_keystore_password> -new logomania
   -keystore <BSM Connector root directory>/WEB-INF/classes/security/.ks
   -storepass logomania
   ```

   Example:

   ```
   keytool -keypasswd -alias bsmc -keypass changeit -new logomania -keystore
   C:\BSMConnector\WEB-INF\classes\security\.ks -storepass logomania
   ```

7. Verify keystore using the new password:

   ```
   keytool -list -v -keystore <BSM Connector root directory>/WEB-
   INF/classes/security/.ks -storepass logomania
   ```

   Example:

   ```
   keytool -list -v -keystore C:\BSMConnector\WEB-INF\classes\security\.ks
   -storepass logomania
   ```

8. Restart the BSM Connector server:

   Windows: Restart the **HP BSM Connector** service in the **Administrative Tools > Services**.

   Linux: Restart the BSM Connector main process, type `/opt/HP/BSMConnector/stop` followed by `/opt/HP/BSMConnector/start`.

9. In BSM, select **Admin > Integrations > BSM Connector Integrations**, and click the **New BSM Connector** button to add the BSM Connector instance. In the **Profile Settings** pane, make sure to select the **Web Server Use SSL** checkbox.

Troubleshooting

Check the bac-integration.log located in **<BSM Connector root directory>/logs/bac_integration/** for the following errors:

```
2010-12-30 11:03:06,399 [TopologyReporterSender] (TopologyReporterSender.java:364)
ERROR - failed to run main topology agent. topologyCommand=TopologyCommand
{commandType
=RUN_SCRIPT, …
java.lang.IllegalArgumentException: cannot find script with
name=create_monitor.py at com.mercury.sitescope.integrations
.bac.topology.dependencies.DependenciesCrawler
.findDependencies(DependenciesCrawler.java:60)
at com.mercury.sitescope.integrations.bac.topology.
dependencies.ScriptDependenciesFinder
.find(ScriptDependenciesFinder.java:80)
at com.mercury.sitescope.integrations.bac.topology.
TopologyReporterSender.getDependencies(TopologyReporterSender.java:552)
at com.mercury.sitescope.integrations.bac.topology.
TopologyReporterSender.send(TopologyReporterSender.java:347)
at com.mercury.sitescope.integrations.bac.topology.
TopologyReporterSender.run(TopologyReporterSender.java:304)
at java.lang.Thread.run(Thread.java:619)
```

Verify that the certificate and keystore passwords are identical.

Chapter 8: Configuring Data Flow Probe for Smart Card Authentication

This chapter contains the following topics:

Connect the Data Flow Probe to BSM Using SSL

When a session is started between the Data Flow Probe and the Gateway Server, the Gateway Server sends the Probe a server-side certificate that was issued by a Certification Authority (CA) recognized by the Gateway Server. The Data Flow Probe engine should be configured to trust the certificate or the CA that issued it, and to communicate via SSL.

1. Establish trust with the CA which issued the BSM virtual server certificate.

   a. Obtain the root certificate of the issuing authority and save it to a file, for example, **C:\ca.cer**.

   b. Import this certificate into the Data Flow Probe JVM: **C:\hp\UCMDB\DataFlowProbe\bin\jre\bin** with the following values:

   ```
   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\keytool -import -trustcacerts -alias
   <your alias> -keystore ..\lib\security\cacerts -file C:\ca.cer
   ```

   c. Enter the password (default: **changeit**) and click **Yes** to confirm.

2. Set the connection parameters in the Data Flow Probe.

   a. Open the file **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties**.

   b. Configure the URL of the BSM server:

   ```
   serverName = <BSM virtual server fully qualified domain name>
   ```

   Note: The SSL connection may fail if an IP address is used instead of domain name.

   c. Configure the port number to use for HTTPS:

```
# Ports used for HTTP/s traffic

#serverPort = 80

serverPortHttps = 443
```

d. Set the schema to be used by the Agent to HTTPS:

```
# Can be either HTTP or HTTPS

appilog.agent.probe.protocol = HTTPS
```

3. Restart the Data Flow Probe.

Connect the Data Flow Probe to BSM Using Reverse Proxy

Perform the following procedure to connect the Data Flow Probe to BSM through the reverse proxy.

1. Edit the **discoveryProbe.properties** file (located in **C:\hp\UCMDB\DataFlowProbe\conf**).
2. Set the **serverName** property to the reverse proxy server's IP or DNS name.
3. Set the **serverPort** and **serverPortHttps** properties to the reverse proxy server's ports.
4. Save the file.

The following proxy server configuration is required if Data Flow Probes only are connected via a reverse proxy to BSM.

Note: In the URLs in this table, you can use either https or http.

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam/*	https://[BSM server]/mam /* or
/mam_images/*	https://[BSM server]/mam_images/*
/mam-collectors/*	https://[BSM server]/mam-collectors/*
/cm/*	https://[BSM server]/cm/* https://[BSM server]/cm/*
/axis2/*	https://[BSM server]/axis2/* **Note:** Required if SOAP adaptor is used with embedded RTSM for replication into secure BSM via reverse proxy.

Connect the Data Flow Probe to BSM Using Client Authentication Certificates

If the BSM front-end requires SSL and a Client Authentication certificate, you need to configure the Data Flow Probe to provide a certificate as described below.

Prerequisite: The Data Flow Probe must be configured with SSL, as described in "Connect the Data Flow Probe to BSM Using SSL" on page 48.

1. Obtain the Client Authentication certificate issued to the name of the Data Flow Probe server. The certificate can be in either PFX or JKS format. If you want to create your own keystore manually, see "SSL Certificates" in the BSM Hardening Guide.

   If the Client Authentication certificate is in PFX format, you must convert it to JKS format. For example:

   ```
   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin>keytool.exe -importkeystore -srckeystore
   C:\hp\UCMDB\DataFlowProbe\conf\security\certificate.pfx -destkeystore
   C:\hp\UCMDB\DataFlowProbe\conf\security\keystore.jks -srcstoretype PKCS12.
   ```

   Note: The keystore password must be the same as the private key password.The keystore password should already be configured in the **ssl.properties** file as **logomania** (the default password). If the keystore password is not **logomania**, you must re-encrypt the password and change it in the **ssl.properties** file. To re-encrypt the password, see step 4 below.

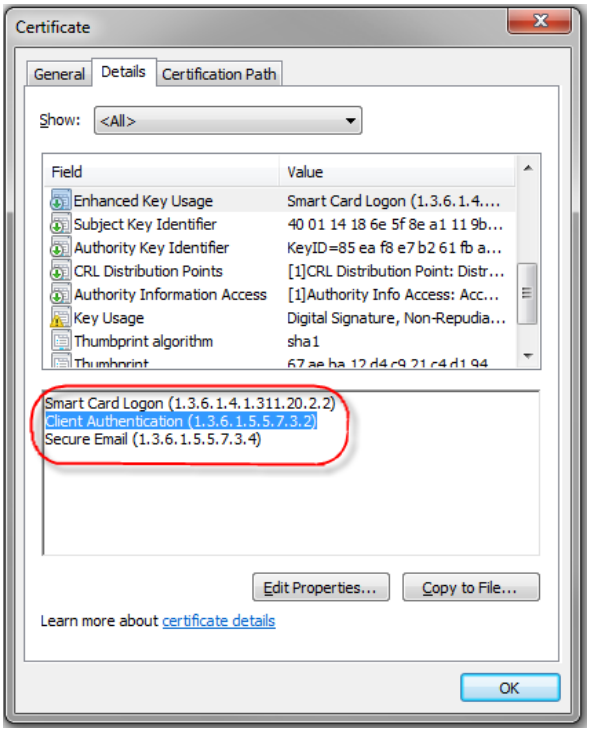
2. Verify that the Client Authentication certificate is correct.

   a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

   b. Click the **Details** tab.

   c. Click **Enhanced Key Usage**.

d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



3. Import the Certificate Authority certificate into the Data Flow Probe Java truststore by running the following command:

   ```
   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin>keytool.exe -import -trustcacerts -alias
   <your alias> -file C:\ca.cer -keystore
   C:\hp\UCMDB\DataFlowProbe\conf\security\MAMTrustStoreExp.jks
   ```

   Enter the keystore password (default: **logomania**). To change the password, see "Update the keystore and truststore passwords" below.

4. Change the **ssl.properties** file, located in the **C:\hp\UCMDB\DataFlowProbe\conf\security** folder. Update the keystore file name to point to the client keystore file you created previously:

   ```
   # Path to Keystore file

   javax.net.ssl.keyStore=keystore.jks
   ```

5. (Optional) Update the keystore and truststore passwords:

   a. You encrypt the password through the Probe's JMX console: Launch a Web browser and enter the following address: **http://<Data Flow Probe machine name or IP address>:1977**. If you are running the Data Flow Probe locally, enter **http://localhost:1977**.

      You may have to log in with a user name (default: **sysadmin**) and password (default: **sysadmin**).

b. Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.

c. Locate the **getEncryptedKeyPassword** operation.

d. Enter your keystore or truststore password in the **Key Password** field and click **getEncryptedKeyPassword**.

e. Open the **ssl.properties** file in the following folder: **C:\hp\UCMDB\DataFlowProbe\root\lib\security**.

f. Copy and paste the encrypted password (numbers separated by commas, for example, 1,2,3,4,5) into the relevant keystore or truststore line of the **ssl.properties** file.

g. Save the file.

6. Update the **C:\hp\UCMDB\DataFlowProbe\conf\DiscoveryProbe.properties** file:

   a. Change the **appilog.agent.probe.protocol** parameter to **HTTPS**.

   b. Make sure the **serverPortHttps** value is **443**.

7. Restart the Data Flow Probe.

Chapter 9: Configuring System Health for Smart Card Authentication

This chapter contains the following topics:

Installing System Health

Before installing System Health, you must ensure that the server and the database are up and running. System Health must be installed in the same domain as , and any firewalls must be open.

Note:

- For system requirements, see the BSM System Requirements and Support Matrixes Guide at http://support.openview.hp.com/selfsolve/document/KM00318731/binary/BSM_922_SysReqs_SupportMatrixes.pdf.
- If you plan to enable smart card enforcement in BSM, you should install System Health on the BSM Gateway server.

You install System Health in one of the following ways:

- On a standalone machine with access to (recommended so that System Health continues to run if servers are down).
- On the server (should be done only if a standalone machine is not available or if smart card enforcement is enabled in BSM).

How to install System Health

1. Uninstall the existing version of System Health from your machine.
2. Run the System Health installation according to your operating system from the System Health installation disk or access it from the Software Patches Site (support.openview.hp.com/selfsolve/patches).

   For Windows:

Enter the location from which you are installing System Health according to your operating system and architecture, followed by **SystemHealth_9.22_setup.exe**.

For Linux:

a. Log into the server as user **root**.

b. Move to the directory where the installation files can be found according to your operating system and architecture.

c. Run the script **./SystemHealth_9.22_setup.bin**.

> **Note:** Installation in console mode is not supported.

3. If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation. Read the warnings, if any, that appear in the **Application requirement check warnings** screen and follow the instructions as described in the screen.

   Click **Continue** to continue with the installation.

4. In the **Introduction (Install)** screen that opens, click **Next**.

5. To install System Health, you must accept the terms of the license agreement by clicking **Next**.

6. The **Install Checks** screen opens and runs verification checks. After the free disk space verification is complete, click **Next**.

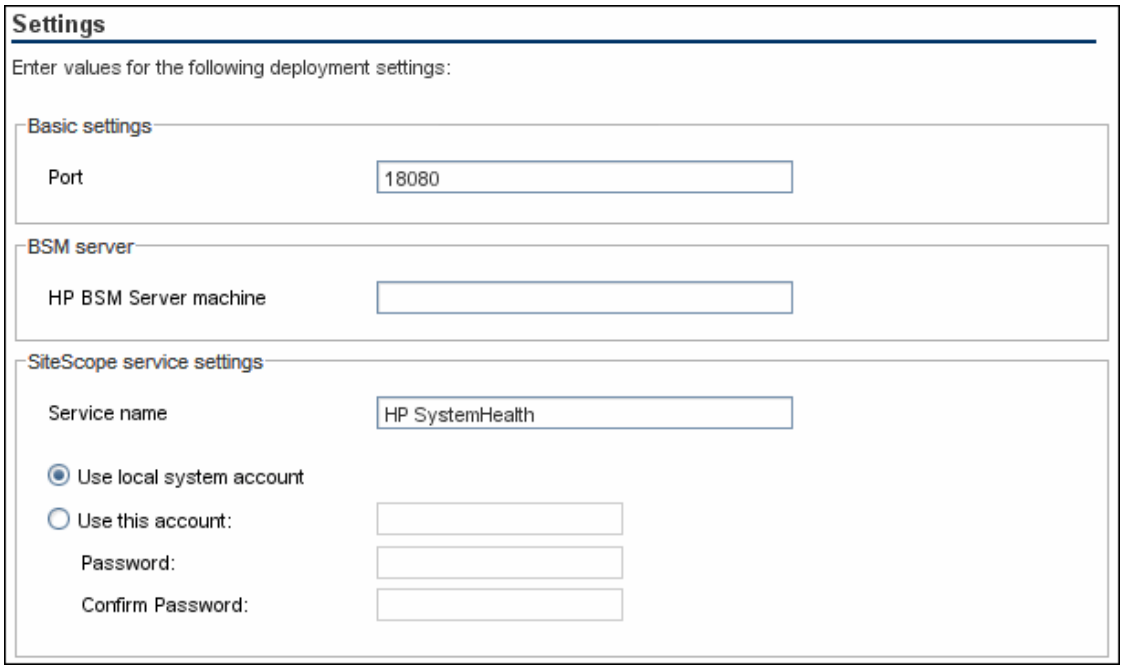
   If the free disk space verification is not successful, free up disk space (for example, by using the Windows Disk Cleanup utility) and repeat this step.

7. In the Pre-Install Summary screen, click **Install**.

   The Installer selects and installs the required System Health software components. The progress of each software component appears on your screen during installation.

8. After installing the System Health components, the Introduction screen of the System Health Configuration Wizard opens. Click **Next**.

9. The Settings page of the System Health Configuration Wizard opens.



Enter the required configuration information and click **Next**:

- **Port.** The System Health port number. Accept the default port number of 18080, or choose another port that is free. If the port number is already in use, an error message appears.
- **HP BSM Server machine.** The fully qualified domain name (FQDN) of the server. For example, **http://<server_name>.<domain_name>**.

  Note: If you are connecting System Health to an environment with a Load Balancer, enter the hostname of the BSM Gateway server, not the Load Balancer.

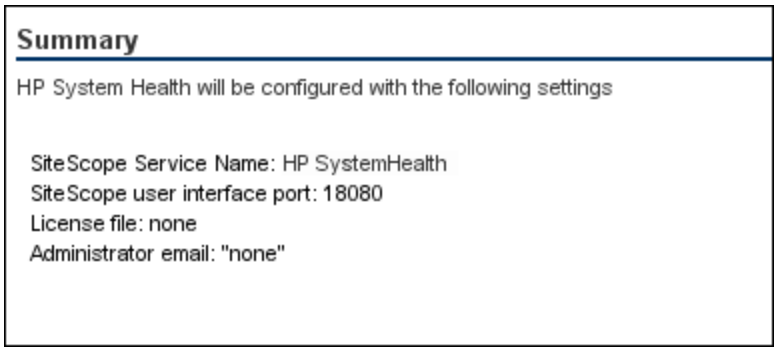
- **Service name.** The name of the System Health service. If the machine has a previous version of System Health installed, enter another name for the System Health service. The default service name is `HP SystemHealth`.
- **Use local system account.** By default, System Health is installed to run as a Local System account. This account has extensive privileges on the local computer, and has access to most system objects. When System Health is running under a Local System account, it attempts to connect to remote servers using the name of the server.
- **Use this account.** Select to change the user account of the System Health service. You can set the System Health service to log on as a user with domain administration privileges. This gives System Health access privileges to monitor server data within the domain. Enter an account and password (and confirm the password) that can access the remote servers. If System Health is installed to run as a custom user account, the account used must have **Log on as a service** rights.

The JMX Encryption data settings page opens.

10. On the JMX Encryption data settings page, you can enter the login and password for the JMX Server, the JMX HTTP Server, and the URL Server. To enable System Health to communicate with a BSM system in which smart card enforcement is enabled, select the **Smart Card** check box.

    If you do not enable smart card enforcement when installing System Health, you can enable it later. For details, see "Enabling Smart Card Enforcement in System Health" on the next page.

11. The Summary screen opens.



    Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

12. In the Done screen, click **Finish** to close the System Health Configuration Wizard.

13. When the installation finishes, the Installation Complete window opens displaying a summary of the installation paths used and the installation status.

    If the installation was not successful, review the installation log file for any errors by clicking the **View log file** link in the **Installation Complete** window to view the log file in a web browser.

    For more information about the installed packages, click the **Details** tab.

    Click **Done** to close the installation program.

    If the installation program determines that the server must be restarted, it prompts you to restart the server.

How to install System Health in a secured environment

To connect System Health to BSM in a secured environment, you must connect directly to the BSM Gateway server, not the reverse proxy. You must then:

1. Click the SiteScope link at the top left corner of the System Health interface. SiteScope opens.
2. Configure SiteScope to connect to the BSM server. For details, see "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the HP SiteScope Deployment Guide.
3. Configure the topology discovery agent in SiteScope to report topology to the BSM server. For details, see "Configuring the Topology Discovery Agent in SiteScope When BSM Server Requires a Client" in the HP SiteScope Deployment Guide.

Note: The HP SiteScope Deployment Guide is available from the HP Software Support site at https://softwaresupport.hp.com.

When installing System Health in a secured environment, note the following:

- If you connect System Health to BSM using the secured Gateway server, the following URL-based monitors do not work because their URLs use the HTTP protocol, not the HTTPS protocol:
  - Web Data Entry Availability
  - BSM Application Server Response

  To enable these monitors to work:

  a. Click the SiteScope link at the top left corner of the System Health interface. SiteScope opens.

  b. In the monitor tree in the left pane of the SiteScope interface, click the monitor name.

  c. Open the URL Monitor Settings panel in the Properties tab.

  d. In the URL field under Main Settings, replace **http** with **https** and save the change. For example, replace the monitor URL `http://ourcompany.com/SiteScope/services` with `https://ourcompany.com/SiteScope/services`.

Enabling Smart Card Enforcement in System Health

If smart card enforcement is enabled in System Health, you can access System Health only from the localhost machine. Access requests from other machines are rejected. Therefore, if smart card enforcement is enabled in System Health, to enable communication between BSM and System Health, System Health must be on the same server as BSM.

You can enable smart card enforcement in System Health either while installing System Health or after installation. For details, see the System Health Guide.

To enable smart card enforcement after installing System Health:

1. Run the System Health Configuration Wizard:

   For Windows:

   Run **Start** > **HP System Health** > **Configuration Wizard**.

   For Linux:

   Run the **sh_config.sh** file in the **%SYSH_HOME%/bin** directory.

2. In the System Health Configuration Wizard, skip to the JMX Encryption data settings page.
3. On the JMX Encryption data settings page, select the **Smart Card** check box.
4. Click **Next**.
5. Click **Finish**. Smart card enforcement is enabled.

Chapter 10: Configuring TransactionVision to Connect to BSM with Client Authentication Certificates

TransactionVision can be configured to communicate with BSM servers that have enabled smart card authentication. This configuration can be achieved in three main steps:

"Step 1: Obtain a CA Root Certificate and Establish Trust" below

"Step 2: Obtain and Configure the CA Issued Client Authentication Certificate" on page 61

"Step 3: Configure TransactionVision to Use the BSM Front-End Server" on page 62

Step 1: Obtain a CA Root Certificate and Establish Trust

This procedure involves obtaining the root CA certificate that signs the server certificate used by BSM and importing it into the JREs used by a TransactionVision Processing Server. This allows TransactionVision server components to trust certificates coming from this authority.

To obtain a CA root certificate:

You must obtain the root certificate from the CA that signed the BSM server certificate.

If you do not have the root certificate of the CA that signed the BSM server certificate:

1. Obtain the CA root certificates for the BSM virtual gateway (front end) server URLs.
    a. In Internet Explorer, open a secured BSM web console (https://<BSM-GW-Server>/topaz).
    b. Click the **Security Report** button (located on the right side of URL field in the Internet Explorer browser) and click the **Viewcertificates** link.

> **Note:** If you do not see the **Security Report** button, press **Alt** on your keyboard (to expand the upper toolbar options) and click **File > Properties** and click the **Certificates** button.

c. Click the **General** tab and check that the following certificate fields are defined correctly:

- **issued to:** BSM's host name
- **issued by:** SomeRoot-CA

d. Verify that the certificate did not expire.

e. Click the **Certificate Path** tab and click the root node of the certificate path.

> **Note:** The certificate path may contain a chain of certificates. You will need to obtain each of the certificates in the chain.

f. Click **View Certificate**.

g. Click the **Details** tab and click **Copy to File**.

h. Click **Next** and select **Base 64 encoded binary**.

> **Note: Base 64 encoded** supports both Apache and IIS. **DER encoded** works only with IIS).

i. Specify the certificate file name and path (for example, C:\BSM_Root).

j. Click **Next**.

k. Click **Finish**.

l. Click **OK** and exit the Certificate wizard. Make sure that the server certificate file was created in the requested path (for example, C:\BSM_Root.cer).

m. Copy the created certificate and save it on the local machine (for example, under C:\).

n. Repeat steps e - m for each CA root certificate in the chain of certificates.

2. Import the root CA certificate into the JREs used by the TransactionVision Processing Server. This needs to be done for both 32- and 64-bit versions of the JRE shipped with TransactionVision Processing Server. Below is an example for each version:

   cd C:\Program Files\HP\TransactionVision\jre\bin

   keytool -importcert -trustcacerts -file C:\myCArootcert.cer -keystore ..\lib\security\cacerts -storepass changeit

   cd C:\Program Files\HP\TransactionVision\jre64\bin

   keytool -importcert -trustcacerts -file C:\myCArootcert.cer -keystore ..\lib\security\cacerts -storepass changeit

Step 2: Obtain and Configure the CA Issued Client Authentication Certificate

This procedure involves obtaining a Client Authentication certificate from your certificate authority and configuring the TransactionVision server components to use the Client Authentication certificate when they communicate with the BSM servers.

1. Request a Client Authentication certificate from your CA with keys marked as exportable, then export the certificate in PFX or PKCS#12 format with a password protected private key.

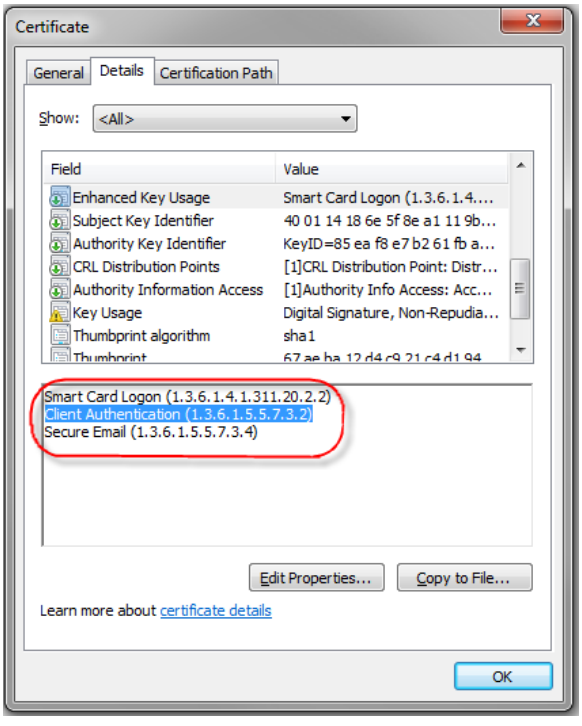
2. Verify that the Client Authentication certificate is correct.

   a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

   b. Click the **Details** tab.

   c. Click **Enhanced Key Usage**.

   d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



3. Import the Client Authentication certificate and private key into a Java keystore. Below is an

example.

keytool -importkeystore -srckeystore myClientCert.pfx -destkeystore C:\ClientKeystore.jks -srcstoretype PKCS12

4. Configure TransactionVision server components to use the Client Authentication certificate.

   Edit the following script files: bin\start_processmanager.bat, bin\start_jobmanager.bat, and bin\start_analyzer.bat

   Add a line like the following below the set JVMOPTS line:

   set JVMOPTS=%JVMOPTS% -Djavax.net.ssl.keyStore=C:\ClientKeystore.jks -Djavax.net.ssl.keyStorePassword=<keystore_password>

5. Restart TransactionVision as follows:

   cd C:\Program Files\HP\TransactionVision\bin

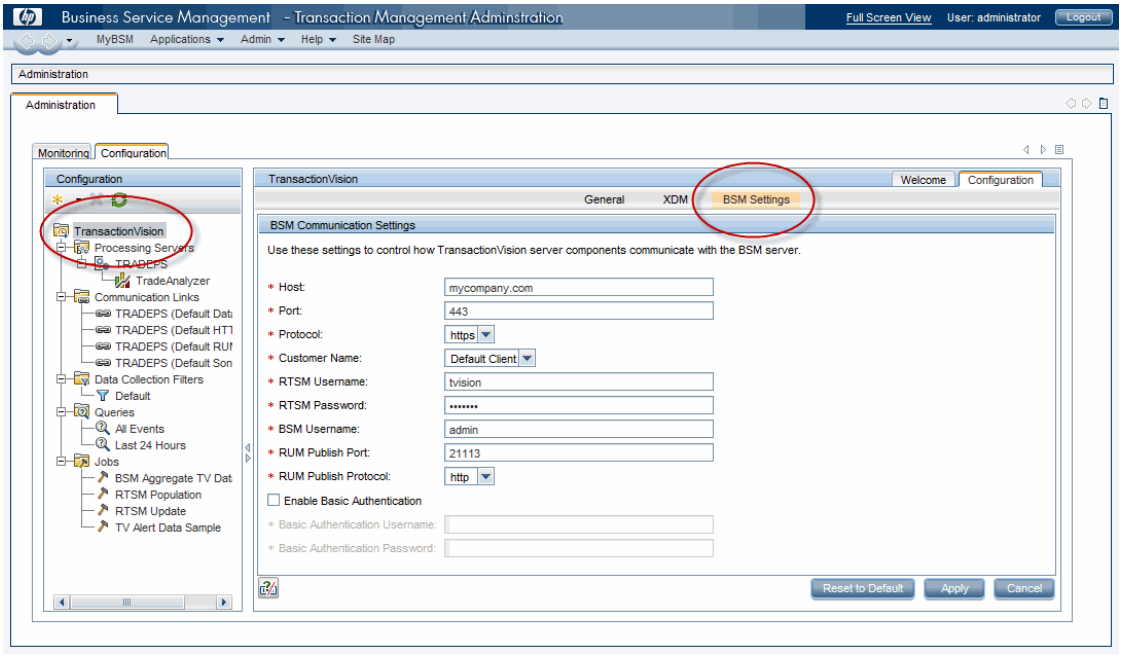
   SupervisorStop.bat

   SupervisorStart.bat

Step 3: Configure TransactionVision to Use the BSM Front-End Server

In a hardened BSM deployment, the BSM front-end server is either a reverse proxy or a BSM Gateway server. You should review and configure the BSM settings used by the TransactionVision server components to make sure that they are set properly according to your BSM deployment. Below is the procedure.

1. Log on to BSM and go to **Admin > Transaction Management**.
2. Click the Configuration tab (at the left) and select TransactionVision from the top of the trees at the left, then click the Configuration tab (at the right) and the BSM Settings tab (in the middle).



3. Update the BSM front-end server host name, port number, and protocol, and click **Apply**.

Note: If your TransactionVision Processing Server cannot directly connect to a BSM Gateway (e.g., there is a firewall in between), your analyzers may not be able to get the time skew information from the BSM server. You can work around the issue by configuring the Time Skew Web URL setting of the Processing Server to use the BSM front-end server instead.

Chapter 11: Configuring SHA for Smart Card Authentication

The following procedure describes how to configure SHA to connect with BSM when BSM requires smart card authentication.

1. Obtain a Client Authentication certificate (certificate.jks) and place it on all BSM Gateway and Data Processing servers. This certificate must be in jks format.

2. If you have an SHA PA/NNM Data Collector, copy the Client Authentication certificate to the SHA Data Collector server.

3. Open **<BSM installation directory>\bin\service_manager.bat** on **all** BSM Gateway and Data Processing servers and all SHA PA/NNM Data Collector servers and make the following changes on each server:

   a. Locate the line that begins **set JVM_OPTS=....**

      Add the following lines immediately before it (or uncomment them out if they are already there)

      set SECURITY_OPTS=-Djavax.net.ssl.keyStore=<path to certificate.jks> -Djavax.net.ssl.keyStorePassword=<keystore password> -Djavax.net.ssl.keyStoreType=JKS

   b. Add the following line after the line **set JVM_OPTS=...**

      set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%

   c. Add **%SECURITY_OPTS%** to the string **SET JVM_OPTS=...** as seen in the following example:

      set JVM_OPTS=%JVM_OPTS% %JVM_64_BIT_OPTS% %SECURITY_OPTS%

4. On all BSM DPS servers, establish trust to the Certificate Authority that issued the BSM server certificates. For details, see the BSM Hardening Guide.

5. Restart all BSM Gateway, Data Processing, and SHA PA/NNM Data Collector servers.

Chapter 12: Configure RUM to Connect to BSM when Smart Card Authentication is Enabled

Configuring RUM to connect to a smart card authentication enabled BSM mainly involves establishing trust to the certificate authority, taking a Client Authentication certificate from the certificate authority, configuring it properly, and saving it on the RUM machine. This is done in two main steps:

"Step 1: Obtain a CA Root Certificate and Establish Trust" below

"Step 2: Obtain and Configure the CA Issued Client Authentication Certificate" on page 67

Prerequisite

Before securing the connection from RUM to a secured BSM, prepare a secured BSM environment.

Step 1: Obtain a CA Root Certificate and Establish Trust

This procedure involves obtaining the root CA certificate that signs the server certificate used by BSM, converting it to the proper format, and saving it on the RUM machine. This allows RUM to trust certificates coming from this authority.

To obtain a CA root certificate:

You must obtain the root certificate from the CA that signed the BSM server certificate.

If you do not have the root certificate of the CA that signed the BSM server certificate:

1. Obtain the CA root certificates for the BSM virtual gateway (front end) server URLs.

    a. In Internet Explorer, open a secured BSM web console (https://<BSM-GW-Server>/topaz).

    b. Click the **Security Report** button (located on the right side of URL field in the Internet Explorer browser) and click the **Viewcertificates** link.

    > **Note:** If you do not see the **Security Report** button, press **Alt** on your keyboard (to expand the upper toolbar options) and click **File > Properties** and click the **Certificates** button.

c. Click the **General** tab and check that the following certificate fields are defined correctly:

- **issued to:** BSM's host name
- **issued by:** SomeRoot-CA

d. Verify that the certificate did not expire.

e. Click the **Certificate Path** tab and click the root node of the certificate path.

> **Note:** The certificate path may contain a chain of certificates. You will need to obtain each of the certificates in the chain.

f. Click **View Certificate**.

g. Click the **Details** tab and click **Copy to File**.

h. Click **Next** and select **Base 64 encoded binary**.

> **Note: Base 64 encoded** supports both Apache and IIS. **DER encoded** works only with IIS).

i. Specify the certificate file name and path (for example, C:\BSM_Root).

j. Click **Next**.

k. Click **Finish**.

l. Click **OK** and exit the Certificate wizard. Make sure that the server certificate file was created in the requested path (for example, C:\BSM_Root.cer).

m. Copy the created certificate and save it on the local machine (for example, under C:\).

n. Repeat steps e - m for each CA root certificate in the chain of certificates.

2. After obtaining the CA root certificate(s), establish trust by importing the root CA certificate(s) for the authority that issues BSM's virtual gateway (front end) server.

a. Open a cmd window on the RUM Engine machine.

b. Connect to `<productDir>\JRE\bin` and execute:

keytool -import -alias SomeRoot-CA -file <server certificate file and path> -keystore <keystore path> -trustcacerts -storepass <password>

c. When asked about trusting this certificate, enter **y**. A **certificate was added to keystore** message appears

3. After obtaining the CA root certificate and establishing trust, configure the connection to BSM using HTTPS.

    a. Open the RUM Engine web console and click **Configuration > BSM Connection Settings**.

    b. In the **Connection to Business Service Management** pane, change the **protocol** to **https**, and make sure that the **port** changes to **443**.

    c. In the **SSL** pane, make sure that the **Truststore type** is **JKS** (mandatory).

    d. If you used the default truststore/keystore (..\lib\security\cacerts), the **Truststore path** and **Truststore password** fields should remain empty.

Step 2: Obtain and Configure the CA Issued Client Authentication Certificate

To work with a CA Client Authentication certificate:

1. Obtain a Client Authentication certificate.

2. Convert the Client Authentication certificate to .pfx format.

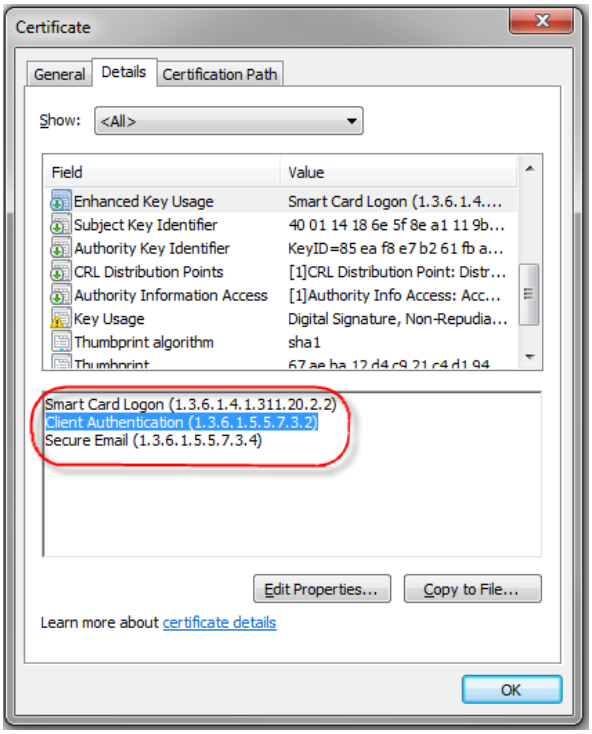
3. Verify that the Client Authentication certificate is correct.

    a. Double-click the Client Authentication certificate that is installed on your machine. The Certificate dialog box opens.

    b. Click the **Details** tab.

    c. Click **Enhanced Key Usage**.

d. Verify that the Client Authentication object identifier (OID) is **1.3.6.1.5.5.7.3.2**.



4. Copy the created .pfx file to the RUM Engine machine.
5. Configure the certificate information in the RUM Engine web console.
   a. Open the RUM Engine web console.
   b. Navigate to **Configuration > BSM connection Settings**.
   c. In the **SSL** pane, enter the following:
      - **keystore path** = Client Authentication certificate path (for example: "C:\client_certificate.pfx")
      - **keystore type** = PKSC12" (.pfx file is of PKSC12 type)
      - **keystore password** and **private key password** = Password for Client Authentication certificate.
   d. Click **Save Configuration** and test the connection with BSM by clicking the **Test RTSM Password** button.

Note: If you already retrieved the client.pfx file with another password from BSM, make sure to put the file in the proper path on RUM and use the relevant password in the configuration connection.

Chapter 13: Troubleshooting

Frequent Requests to Re-enter Your Smart Card PIN Code when Accessing BSM Components

Problem: Each time you click in the BSM Console to start a new Java process, you are asked for the PIN code of your smart card .

Solution: The reason you are asked for your PIN code each time you start another application, is that the smart card software does not allow caching the pin code for the BSM session, only per process. To resolve this problem:

- Set the Smart Card Authentication Configuration mode to **Custom** or **Users only login** in the Smart Card Authentication Configuration Wizard (see Smart Card Authentication in the BSM Platform Administration Guide).
- If you have an Apache reverse proxy configuration, constrain the URL list that is client-cert authenticated. This list is in the configuration file of the Apache Reverse Proxy / Load Balancer (or the Apache web server, if you don't have the Apache Load Balancer in front to terminate the user's incoming SSL connection). This method is relevant for reverse proxy configurations. For instructions, see "To constrain the URL list that is client-cert authenticated" below.

> **Note:** If you rerun the Smart Card Authentication Configuration Wizard for any reason, you need to repeat this procedure.

To constrain the URL list that is client-cert authenticated

1. In the file **httpd-ssl.conf**, locate the following section:

```
SSLVerifyClient require

SSLVerifyDepth  10

SSLCACertificateFile /opt/HP/BSM/WebServer/conf/ssl/client_ca_root.pem

SSLOptions +ExportCertData
```

2. Wrap this section with a URL constraint as follows. This enables this particular URL to do the smart card authentication (and thus the PIN prompt), while the remainder of the application session will be server-authenticated https after a valid application session is established.

```
<LocationMatch
"^/topaz/login.jsp|.*/topaz.*/bsmservices.*|.*/opr.*/rest.*|.*/topaz.*/servicehealth.*|.*/topaz.*/slm.*|.*/topaz.*/eumopenapi.*|.*/topaz.*/eumappapi.*|.*/topaz.*/eumreportsapi.*">

SSLVerifyClient require

SSLVerifyDepth  10

SSLCACertificateFile /opt/HP/BSM/WebServer/conf/ssl/client_ca_root.pem

SSLOptions +ExportCertData

</LocationMatch>
```

3. Restart the Apache web server to ensure that the configuration is activated.

Smart Card Authentication Configuration Timeout Failure

Problem: When configuring Smart Card Authentication using the Configuration Wizard, BSM fails during setup with a timeout failure.

Solution: Increase the value of the **process.launcher.time.out** parameter. The default is 60 seconds.

1. In a text editor, open **HPBSM\conf\settings\security.xml**.
2. Locate the parameter **process.launcher.time.out**.

```
<setting

name="process.launcher.time.out"

sectionResource="security.login"

nameResource="process.launcher.time.out.name"

descResource="process.launcher.time.out.desc"

refreshRate="Reboot"

displayInUI="false"

settingType="global">

<value type="number">60</value>

</setting>
```

3. In the line `<value type="number">60</value>`, increase the value .

Unable to Disable Smart Card Authentication

Problem: If you manually change the IIS and then try to disable Smart Card Authentication by running the Smart Card Authentication wizard or RevertHardening.bat, the BSM system may enter an unstable state. Although Smart Card Authentication seems to be disabled, you can continue to access BSM using Smart Card Authentication as well as entering a user name and password.

Solution: Remove SSL binding and rerun the post-installation wizard.

1. Open a cmd window and run **netsh http show ssl**.
2. Locate the IP:port line and copy the address.

   For example, locate the line: `IP:port : 0.0.0.0:443` and copy `0.0.0.0.443`

3. Run the command **netsh http delete sslcert ipport=<IP port address>** where <IP port address> is the address you copied in the previous step.

   For example, **netsh http delete sslcert ipport=0.0.0.0.443**

4. Run **<HPBSM root directory>\bin\postinstall.bat**.

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 Smart Card Authentication Configuration Guide (Business Service Management 9.25)

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!