HP Business Service Management

For the Windows, Linux operating systems

Software Version: 9.24

Hardening Guide

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2005-2014 Hewlett-Packard Development Company, L.P.

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.

Acknowledgements

This product includes software developed by the Apache Software Foundation (www.apache.org).

This product includes software developed by the JDOM Project (www.jdom.org).

This product includes software developed by the MX4J project (mx4j.sourceforge.net).

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services

- Enter into discussions with other software customers
- Research and register for software training

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

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

To find more information about access levels, go to:

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

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

Contents

Chapter 1: Introduction to Hardening

This chapter introduces the concept of a secure BSM platform and discusses the planning and architecture required to implement a secure platform. It is strongly recommended that you read this chapter before proceeding to the following chapters, which describe the actual hardening procedures.

The BSM platform is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it could potentially be exposed.

The hardening guidelines deal with the configuration required to implement a more secure (hardened) BSM platform. The hardening guidelines relate to both single machine (where all BSM components are installed on the same machine) and distributed (where all BSM components are installed on separate machines) deployments of BSM. You can also invoke dedicated Gateway deployment, in which several Gateway servers are assigned different tasks.

The hardening information provided is intended primarily for BSM administrators, and for the technical operator of each component that is involved in the implementation of a secure BSM platform (for example, the Web Server). These people should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

> **Note:** In this document, the term *reverse proxy* also refers to *load balancing* in Layer 7 load balancing except for BBC channel reverse proxy configuration (see *Configuring BBC Port 383 Connection on Reverse Proxy* in the BSM Installation Guide).

Deploying BSM in a Secure Architecture

Several measures are recommended to securely deploy your BSM servers:

- **DMZ architecture using a firewall**

  The secure architecture referred to in this document is a typical DMZ architecture using a device as a firewall. The basic concept of such an architecture is to create a complete separation, and to avoid direct access between the BSM clients and the BSM servers.

- **Secure browser**

  - **Firefox**

    Firefox in a Linux environment must be configured to securely handle Java scripts, applets, and cookies. SSL communication protocol Secure Sockets Layer protocol secures the connection between the client and the server. URLs that require an SSL connection start with HTTPS instead of HTTP.

  - **Autocomplete**

    The 3 major browsers have each decided to ignore autocomplete=off in web forms.

IE: http://blogs.msdn.com/b/ieinternals/archive/2013/09/24/internet-explorer-11-changelist-change-log.aspx

Chrome: http://googlechromereleases.blogspot.com/2014/04/stable-channel-update.html

Firefox: https://bugzilla.mozilla.org/show_bug.cgi?id=956906

As a result, when logging in to BSM you may, depending on your browser configuration, be prompted to remember your login credentials.

If you are an end user of the BSM and do not wish to have your login credentials remembered, they need not be; indicate when prompted by your browser that you do not wish to have your login or password information saved by the browser. Often you can instruct your browser not to prompt you in the future for this site.

It is often possible to configure your browser to not prompt you to remember passwords at all, if you wish to disable this ability entirely. This can often be configured either in the browser itself or via corporate IT policy. Refer to your browser documentation or contact your System Administrator for more details.

- **Secure browser**

  Internet Explorer in a Windows environment and Firefox in a Linux environment must be configured to securely handle Java scripts, applets, and cookies. SSL communication protocol Secure Sockets Layer protocol secures the connection between the client and the server. URLs that require an SSL connection start with HTTPS instead of HTTP.

- **Reverse proxy architecture**

  One of the more secure and recommended solutions is to deploy BSM using a reverse proxy. BSM fully supports reverse proxy architecture as well as secure reverse proxy architecture.

The following security objectives can be achieved by using a reverse proxy in DMZ proxy HTTP/HTTPS communication with BSM:

- No BSM logic or data resides on the DMZ.

- No direct communication between BSM clients and servers is permitted.

- No direct connection from the DMZ to the BSM database is required.

- The protocol used to communicate with the reverse proxy can be HTTP or HTTPS. HTTP can be statefully inspected by firewalls if required.

- A static, restricted set of redirect requests can be defined on the reverse proxy.

- Most of the Web server security features are available on the reverse proxy (authentication methods, encryption, and others).

- The reverse proxy screens the IP addresses of the real BSM servers as well as the architecture of the internal network.

- The only accessible client of the Web server is the reverse proxy.

- This configuration supports NAT firewalls.

- The reverse proxy requires a minimal number of open ports in the firewall.

The reverse proxy provides good performance compared to other bastion host solutions. It is strongly recommended that you use a reverse proxy with BSM to achieve a secure architecture. For details on configuring a reverse proxy for use with BSM, see "Configuring Secure Access to BSM Reverse Proxy" on page 25.

If you must use another type of secure architecture with your BSM platform, contact HP Software Support to determine which architecture is the best one for you to use.

Notes and Recommendations

Notes:

- **Prerequisites.** To best use the hardening guidelines given here for your particular organization, do the following before starting the hardening procedures:

  - Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate the BSM platform into your network.

  - Review the entire guide, especially Chapter 2, "Hardening Workflow" on page 10.

- **Log management**. BSM uses the log4j framework for managing log files. If you wish to change the locations of log files, these can be set in the log4j appenders, which are located in **<HPBSM root directory>\conf\core\Tools\log4j**. There is a separate directory for each process, for example **EJB** for the JBoss application server.

- **Security officer.** The security officer is a user who has security privileges to view sensitive information in the system. The security officer is typically not a regular BSM user and receives access to configure certain sensitive reporting information, such as which RUM transaction parameters to include or exclude from certain reports (For example Session Details or Session Analyzer). For details, see "Security Officer" in the BSM Platform Administration Guide.

  The Security Officer can see the parameters and decide to expose them in the reports, but once they are exposed in the reports, anyone with access to these reports will be able to see this data, so it is imperative that the application being monitored encrypts sensitive data, such as passwords, credit card numbers, and identity numbers.

- **Changing the encryption algorithm**. You can change the encryption algorithm used by BSM, but only before running the configuration wizard. Open the encryption properties file, **<HPBSM root directory>\conf\encryption.properties**, and choose one of the predefined

crypt configuration entries (**crypt.conf.x**) by setting **crypt.conf.active.id** to the appropriate index. If you want to add another entry, follow the standard Java Cryptography Extension (JCE) format.

- The hardening procedures are based on the assumption that you are implementing only the instructions provided in this guide, and not performing other hardening steps not documented here.

- Where the hardening procedures focus on a particular distributed architecture, this does not imply that this is the best architecture to fit your organization's needs.

- It is assumed that the procedures included in the hardening guide will be performed on machines dedicated to the BSM platform. Using the machines for other purposes in addition to BSM may yield problematic results.

Recommendations:

- Isolate BSM servers in their own internal segment behind a firewall since the traffic between the various BSM servers is not encrypted.

- Follow all security guidelines for LDAP servers and Oracle databases.

- Run SNMP and SMTP servers with low permissions.

> **Note:** SNMP and mail traffic may not be secure.

Chapter 2: Hardening Workflow

This section describes the overall workflow needed to harden the HP Business Service Management environment. The procedures in this book should not be performed outside of the context of this workflow.

1. **Hardening prerequisites**

   - **Verify BSM functionality.** Verify that the BSM environment is fully functioning before starting the hardening procedures. This includes the basic data flow into and out of BSM.

   - **Define security requirements.** Before starting the hardening process, define what areas of your environment you want to secure (with SSL).

   - **Review recommendations and notes.** For details, see "Notes and Recommendations" on page 8.

2. **Obtain server certificates for the BSM virtual gateway server URLs**

   Obtain a server certificate for each of the following front-end URLs that you want to secure: one for users to access BSM, and one for data collectors to access BSM. For details, see "Issuing SSL Certificates" on page 16.

   > **Note:** If your SSL termination points are not the front-end URLs (BSM virtual gateway server URLs), you need to issue server certificates for these termination points as well.

   The server certificates must be issued into the exact FQDNs. Later, these same FQDNs must be entered into the **BSM Console > Admin > Setup and Maintenance > Infrastructure Settings** page in the following rows:

   - Default Virtual Gateway Server for Application Users URL

   - Default Virtual Gateway Server for Data Collectors URL

   For example: If your URL is **https://bsmUsers.mycompany.com:443**, you would issue a certificate to **bsmUsers.mycompany.com**.

3. **Obtain root CA certificate(s)**

   Obtain the root CA certificates from the root, and any intermediate, authorities that issued the server certificates above.

4. **Configure SSL connection using the server certificates**

   Install the server certificates on the termination points of SSL. This may be a load balancer, a reverse proxy, or a BSM Gateway server.

    a. **Load Balancer.** Install the certificates on the termination points of SSL (this is usually the load balancer).

    b. **Reverse Proxy.** Perform the procedure to configure the reverse proxy to work with SSL.

       i. **IIS.** See *Configure IIS Reverse Proxy to Work with SSL* in the BSM Installation Guide.

       ii. **Apache.** See *Configuring a Reverse Proxy - Apache* in the BSM Installation Guide.

    c. **BSM Gateway servers.** Refer to the following information:

      ○ For IIS web server. The Microsoft Web site (http://www.iis.net).

      ○ For Apache web server. See "Configuring Secure Access to Apache" on page 23.

5. **Establish trust to the Certificate Authority**

   On all BSM Gateway servers, establish trust to the Certificate Authority that issued the server certificates above. If you have Service Health Analyzer or an SHA PA/NNM Data Collector, this procedure must be performed on the BSM Data Processing servers and the SHA PA/NNM Data Collector as well.

   > **Note:** The same procedure must be performed in both the JRE and JRE64 directories.

   > **Example:**
   >
   > ```
   > cd <BSM root directory>/JRE64/bin
   > > keytool -import -alias <myCA> -file c:\myCArootcert.cer -keystore
   > ..\lib\security\cacerts -trustcacerts -storepass changeit
   > cd <BSM root directory>/JRE/bin
   > > keytool -import -alias <myCA> -file c:\myCArootcert.cer -keystore
   > ..\lib\security\cacerts -trustcacerts -storepass changeit
   > ```

6. **Verify secure connection works**

   From a client browser, open the **Default Virtual Gateway Server for Application Users** and **Default Virtual Gateway Server for Data Collectors** URLs that you secured. If the login page appears, this verifies that the secure connection is configured.

7. **Update BSM Virtual URLs to use https**

   Log in to BSM and enter the secured URLs in **BSM Console > Admin > Setup and Maintenance > Infrastructure Settings** page in the following two rows:

  ▪ Default Virtual Gateway Server for Application Users URL

  ▪ Default Virtual Gateway Server for Data Collectors URL

Enable and disable all BSM Gateway servers, and verify (again) that a client can log in using those URLs.

8. **Connect data collectors to secure BSM**

Now that the BSM servers are secured, you configure other servers to communicate securely with BSM.

The basic flow for any data collector connecting to secure BSM is as follows:

a. Import root CA certificate(s) obtained in step 3 into the JVM used by the data collector.

b. Configure the connection to BSM using https.

c. Make sure data flows over the secure connection.

Follow the appropriate procedures for more detailed descriptions for each of the data collectors:

Data Collector / Server type	Relevant Documentation
BPM	HP Business Process Monitor Administrator's Guide.
SiteScope	HP SiteScope Deployment Guide
Service Health Analyzer	Installation Guide for Service Health Analyzer Data Collector
System Health	Using System Health
RUM	Real User Monitor Administration
Data Flow Probe	The default UCMDB SSL port, 8443, must be changed to the BSM SSL port, 443, in the DiscoveryProbe.properties file. For more information, see the Data Flow Probe Installation Guide.
BSM Connector	BSM Connector User Guide
TransactionVision	HP TransactionVision Deployment Guide PDF

9. **Secure JBOSS Management API (http JMX) on BSM servers**

Up to this point in the procedure, you secured access to BSM from web servers (port 80). However, the application servers (port 8080) are not secured. We recommend securing them

as well. For details, see "Configuring Secure Access to the JBoss HTML JMX Console" on page 28.

10. **Configure mutual SSL**

    If you want to configure BSM to require a client certificate, perform this procedure:

    a. Follow the standard procedures for requiring client certificates on the front end BSM server (could be a web server on the Gateway server, a load balancer, or a reverse proxy). For details, see the documentation of the load balancer, reverse proxy, or web server.

       For examples for reverse proxies

       IIS. See *Configure IIS to Require Client Authentication - Optional* in the BSM Installation Guide.

       Apache. "Configuring Secure Apache Reverse Proxy to Require Client Authentication - Optional" on page 27

    b. If users are required to log in to BSM with a digital certificate, see "How to Secure User Access to BSM Using Client-Side Authentication Certificates" in the BSM Platform Administration Guide.

    c. If users are required to log in to BSM using smart cards, see the Smart Card Authentication Configuration Guide.

    d. To enable data collectors to connect to the BSM front end server that now requires a client certificate, refer to the following documentation:

Data Collector / Server type	Relevant Documentation
BSM Connector	See the BSM Connector User Guide
BPM	See the HP Business Process Monitor Administrator's Guide.
SiteScope	"Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the HP SiteScope Deployment Guide.
System Health	"Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the HP SiteScope Deployment Guide.
RUM	See the Real User Monitor Administration PDF.
Data Flow Probe	See the RTSM Data Flow Management Guide.
Service Health Analyzer	Installation Guide for Service Health Analyzer Data Collector

11. **(Optional) Secure JBOSS Management API (JMX-RMI channel)**

     In certain cases, you may need to secure the JMX-RMI channel used for internal BSM communications. This procedure should be performed only if there is a specific reason to do so. For details, see "Configuring Secure Access to the JMX-RMI Channel Used for Internal BSM Communications" on page 31.

12. **(Optional) Secure JMX console for other processes**

     You can also secure the JMX console to work with SSL in other processes. For details, see "Configuring Secure Access to the HTML JMX Console in other BSM processes" on page 30.

13. **(Optional) Secure BSM installation directory**

     We recommend that you restrict access to the BSM installation directory to privileged users. We recommend only allowing the **SYSTEM** account and **Administrators** groups to access this directory.

14. **(Optional) Configure Firewall**

     We recommend configuring a firewall on the BSM Gateway and DPS Servers. However, in order to this you must ensure that the BSM servers can still communicate freely. To do this, you must set up a host-to-host tunnel (or VPN) between all BSM Gateway and DPS servers.

15. **(Recommended) Configuring Secure Access to Data Collectors**

     This section describes how to secure access to the data collector admin consoles (UI). Follow the appropriate procedures depending on your data collectors:

Data Collector / Server type	Relevant Documentation
BPM	"Configuring Secure Access to Data Collectors" on page 36
SiteScope	"Configuring Secure Access to Data Collectors" on page 36
System Health	"Configuring Secure Access to Data Collectors" on page 36
RUM	"Configuring Secure Access to Data Collectors" on page 36
Transaction Vision	See the HP TransactionVision Deployment Guide PDF

Chapter 3: Using SSL in BSM

Secure Sockets Layer (SSL) technology secures communication by encrypting data and providing authentication. Without SSL encryption, packets of information travel over networks in full view.

SSL encryption uses two keys:

- **Public key.** The public key is used to encrypt data.

- **Private key.** The private key is used to decipher data.

Both keys together are called a **certificate**. Every SSL certificate is created for a particular server in a specific domain by a Certificate Authority (CA). When an application user or data collector accesses a BSM server, SSL authenticates the server, and can also be configured to authenticate the client. Additionally, BSM establishes an encryption method and a unique key for the communication session.

The BSM platform fully supports the SSL 3.0 protocol. The SSL channel is configured on the BSM servers/clients as required.

> **Note:** We recommend using the strongest currently available cryptographic algorithms when obtaining server or client certificates, as well as the largest key size (not less than 2048-bit RSA keys). To see the latest NIST approved cryptographic algorithms and key lengths, go to http://csrc.nist.gov/publications/PubsFIPS.html.

Overview of SSL and BSM

SSL provides BSM with the following:

- **Server authentication.** Provides authentication of the BSM server used for communication.

- **Client authentication (optional).** Provides authentication of the client communicating with the BSM server. The client could be an application user or a data collector such as Business Process Monitor.

- **Encrypted channel.** Encrypts the communication between the client and the server using a variety of ciphers.

- **Data integrity.** Helps ensure that the information sent by one side over SSL is the same information received by the other side.

Creating SSL Certificates

Server certificates can be obtained in various formats. Java uses a proprietary format (JKS) to store certificates in what is called a Keystore. This format is compatible with Java applications. Certificates can also be stored in other language-neutral formats such as PKCS#12.

Different components support different server certificate formats. For example, web-servers such as IIS and Apache work with PKCS#12 format and do not work with JKS format. Depending on the components included on your BSM server, you may need to use either the JKS or PKCS#12 format.

Issuing SSL Certificates

Secure communication via https can terminate either at the load balancer/ reverse proxy or on the BSM Gateway.

If it terminates on the BSM Gateway, the web server on the Gateway is configured to support/require SSL. Otherwise, if SSL terminates on the load balancer/reverse proxy, then only the load balancer/reverse proxy needs to be configured for secure communication.

Generally, server certificates must be issued to the name of the external access point (FQDN) that is configured in **Default Virtual Gateway Server for Application Users/Data Collectors URL**. This is the name that users and data collectors use to access BSM.

> **Note:** When using aliases (for example, one name for users, one for data) on the same BSM Gateway Server, you can obtain a Subject Alternative Name (SAN) certificate with a predefined set of DNS names.

If there is a load balancer/reverse proxy in front of a BSM gateway, it is recommended to have SSL terminate on the load balancer/reverse proxy.

As usual with SSL, you will need to have a CA root certificate present in your browser's **Trusted Certification Authorities** list and in the trustcacerts of the JVM on each data collector installation.

The following table addresses SSL termination in the High Availability environment:

SSL Termination On	SSL on Load Balancer	SSL on Gateway	Advantages/ Disadvantages
Load Balancer	Yes	No	This is a recommended configuration. It allows: • Maintenance of certificates in one place (on load balancer/reverse proxy) • Reduced processing of load on BSM Gateways On each load balancer/reverse proxy, use server certificates issued to the name of the external access point (FQDN) that users/data collectors are using to access BSM. If multiple load balancers/reverse proxies share the load, each one must have these certificates imported.

SSL Termination On	SSL on Load Balancer	SSL on Gateway	Advantages/ Disadvantages
Gateway	Yes	Yes	This is a less ideal configuration, especially where load balancers are concerned. It requires: ● Maintenance of certificates in multiple places (load balancer/reverse proxy and Gateways) ● Expensive SSL renegotiation in load balanced environment for data collectors (see note below) In this configuration, in addition to installing certificates on the load balancer, also install server certificates on the Gateway, using a server certificate issued to the FQDN name of the Gateway. **In a high availability environment with multiple Gateways:** Traffic from the same data collector will be load-balanced between different Gateways using a round-robin mechanism. If you have a different certificate on each Gateway issued to a different name, in the worst case scenario, switching between Gateways will require an SSL renegotiation process to run each time there is a switch between Gateways. This is very expensive in terms of CPU use and network traffic, on both the server and client sides. For this reason, SSL termination is typically done on the load balancer.
Gateway	No	Yes	Not a recommended scenario.

Creating a Java Keystore

Option 1: Convert a PKCS#12 certificate provided by your Certificate Authority.

1. Request a client or server certificate from CA in the name of your server.

2. Export private key with a password that is at least six characters long. Example: **changeit**.

3. Convert the certificate from PFX/PKCS#12 to JKS format. For example: **keytool.exe -importkeystore -srckeystore c:\certificate.pfx -destkeystore c:\certificate.jks -srcstoretype PKCS12**

4. Import CA root certificate into the keystore just created, as in the following example.

    Download CA root certificate in BASE-64 format, for example, **c:\ca_root.cer**.

Import CA root certificate into the keystore:
keytool -import -alias ca -file c:\ca_root.cer -keystore C:\certificate.jks -storepass changeit

Option 2: Create a keystore in JKS format manually and have it signed by your certificate authority as follows:

1. Generate a keystore with a private key

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

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

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

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

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

4. Obtain the root authority certificate (and any intermediate authority certificates if applicable).

5. 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 changei
t -alias  myRootCA -file c:\ca_root.cer
```

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

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

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

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

Note: Make sure that your private key password and keystore password are the same.

Configuring Secure Access to BSM Front Ends

This section contains the following topics:

- "Supported Topologies in BSM" below

- "Configuring Secure Access to BSM Gateways" on the next page

- "Configuring Secure Access to BSM Reverse Proxy" on page 25

Supported Topologies in BSM

SSL supports the following topologies:

- Application users / data collectors that communicate with BSM Gateway Servers directly.
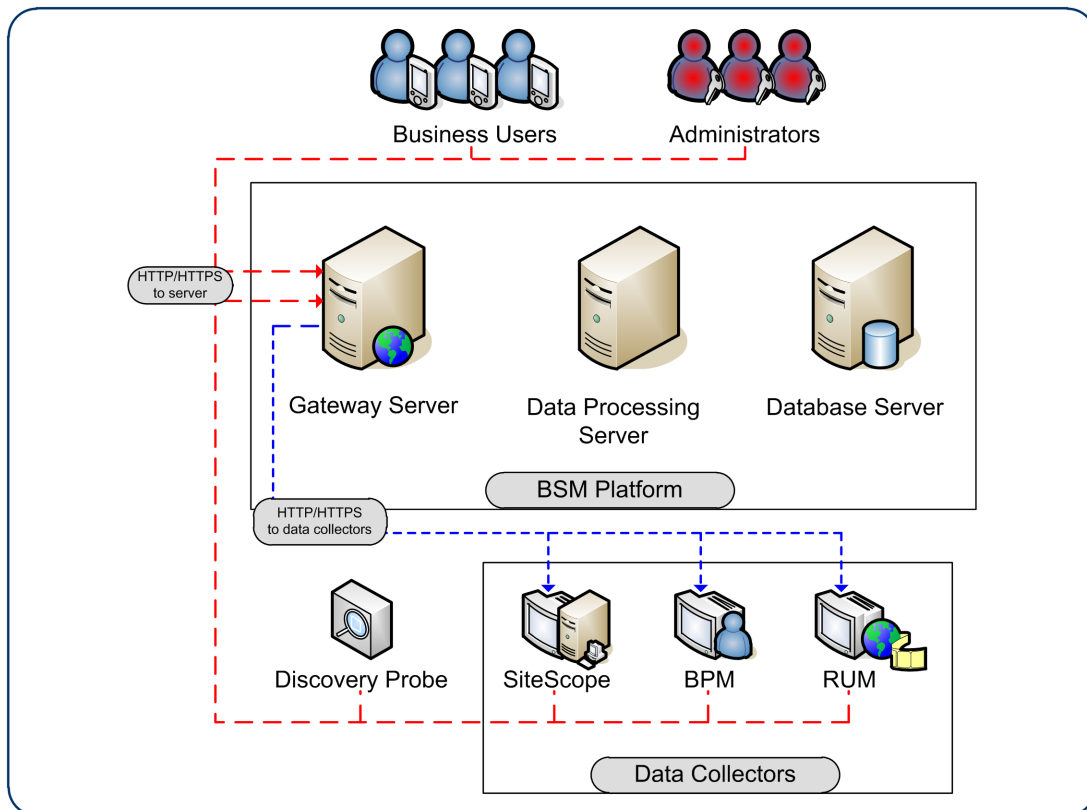
- Application users / data collectors that communicate with BSM Gateway Servers using Reverse

Proxy.
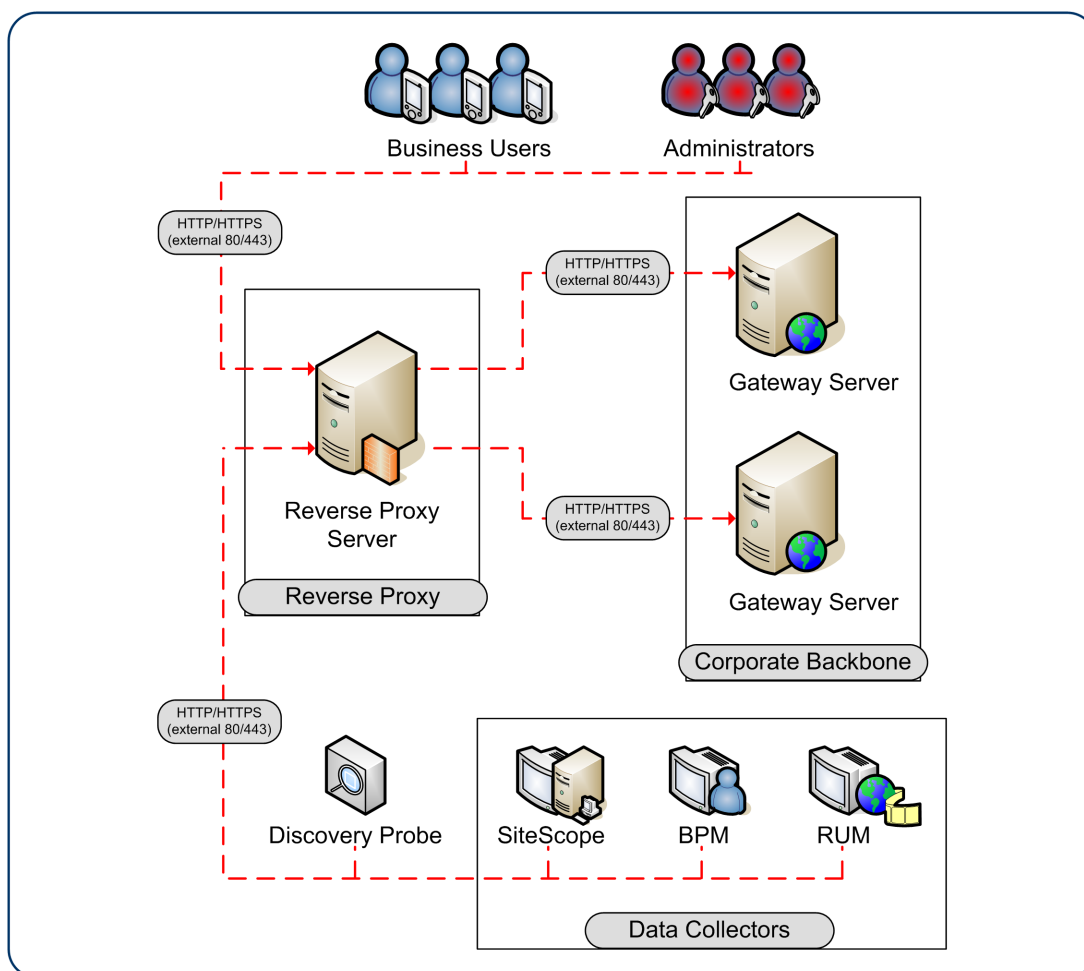
Client authentication using a client-side certificate is optional with BSM clients.

Configuring Secure Access to BSM Gateways

To configure secure access to the BSM Gateway (or a BSM machine, in the case of a single machine installation) , you must enable SSL support on the Web server used by the Gateway Server.

To enable SSL support on the Web Server:

- **Microsoft Internet Information Server (IIS).** See Microsoft's site http://www.iis.net/ for information on enabling SSL for all interaction with the Web server. Note that SSL should be enabled for the entire IIS Web Site under which you installed the BSM applications.

- **Apache HTTP Server 2.2.x**. The Apache web server is included in BSM. For details about configuring SSL, see "Configuring Secure Access to Apache" on page 23.

If you are not using a publicly known Certificate Authority for your server certificate, you need to set the Java truststore to trust the Certificate Authority that issued the server certificate. For details, see step 5 in the "Hardening Workflow" on page 10.

After performing the above procedures, the Web server installed on the Gateway Server machine is configured to support HTTPS communication.

Additional Security Recommendations

To provide additional security for access to the BSM Gateway or BSM machine, we recommend the following:

- **Disable Weak Ciphers on IIS.** See http://support.microsoft.com/default.aspx?scid=kb;EN-US;245030.

- **Disable HTTP Methods for IIS.** HTTP provides several methods that can be used to perform actions on the web server. Some of these methods pose a security risk for BSM. To avoid this security threat, the following methods should be disabled:

  - PUT

  - DELETE

  - TRACE

  - OPTIONS

  - CONNECT

  To disable an HTTP method from the command line:

  a. Open a CMD window.

  b. Type `cd C:\Windows\System32\inetsrv`.

  c. Type the following command:

  ```
  appcmd.exe set config "Default Web Site" -section:system.webServer/security/requestFiltering /+"verbs.[verb='<HTTP command>',allowed='False']"
  ```

  where `<HTTP command>` is the name of the HTTP command you want to disable.

  > For example, if you want to disable the PUT command, enter
  >
  > ```
  > appcmd.exe set config "Default Web Site" -section:system.webServer/security/requestFiltering /+"verbs.[verb='<PUT>',allowed='False']"
  > ```

  To disable an HTTP method from the user interface:

a. Open the Internet Information Services (IIS) Manager.

   In Windows 2008/2008 R2/2012/2012 R2, from the taskbar, click **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**.

b. In the Connections pane, click **Default Web Site**.

c. In the Home pane, double-click **Request Filtering**.

d. In the Request Filtering pane, click the **HTTP Verbs** tab.

e. In the Actions Pane, click **Deny Verb**.

f. In the Deny Verb dialog box, type the HTTP verb you wish to block, and click **OK**.

   For example, to prevent HTTP TRACE requests to your server, type **TRACE** in the Deny Verb dialog box.

- **Filter IIS File Extensions.** In the IIS Manager, in the File Name Extensions page, create a list of file name extensions for which the request-filtering module will allow or deny access. This will help restrict certain file types and increase security on your Web server.

- **Remove Server Header.** By default, Microsoft adds a server response header with content looking like this `Server: Microsoft-IIS/7.5`. It is recommended to remove this header.

  a. Download and install URL Rewrite (if it is not already installed). See http://www.iis.net/downloads/microsoft/url-rewrite.

  b. Click **Add Rule(s)** and create a new blank outbound rule. Complete the following information:

     ○ **Name:** Remove response server

     ○ **Matching scope:** Server variable

     ○ **Variable name:** RESPONSE_SERVER

     ○ **Variable value:** Matches the Pattern

     ○ **Using:** Regular Expressions

     ○ **Pattern:** .+

     ○ **Action type:** Rewrite

     ○ **Value:** type bogus server name. For example, nginx, apache etc.

     ○ **Replace existing server variable value:** Select this option.

  c. Apply and use a header sniffer to check the results.

Configure URL for Accessing BSM with SSL

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. Click **Foundations** and select **Platform Administration**.

2. In the Host Configuration pane, set the following parameters:

   - Default Virtual Gateway Server for Application Users URL and Default Virtual Gateway Server for Data Collectors URL. You must enter the server URL with the SSL protocol https and the SSL port (default is 443). For example: https://my_server.example.com:443

   - Local Virtual Gateway Server for Application Users URL and Local Virtual Gateway Server for Data Collectors URL (optional). If you must use more than one URL (the one defined for the Default Virtual Core Server URL parameter) to access the Gateway Server machine, define a Local Core Centers Server URL for each machine through which you want to access the Gateway Server machine. For example:

   https://my_specific_virtual_server.example.com:443

   > **Note:** If the Local Virtual Core Services Server URL parameter is defined for a specific machine, this URL is used instead of the Default Virtual Core Services URL for the specifically-defined machine. If the Local Virtual Server URL parameter is defined for a specific machine, this URL is used instead of the Default Virtual Server URL for the specifically-defined machine.

3. **Direct Gateway Server for Application Users Server URL**. Click the **Edit** button and delete the URL in the **Value** field.

4. **Direct Gateway Server for Data Collectors URL**. Click the **Edit** button and delete the URL in the **Value** field.

5. Restart the HP BSM service on all BSM machines.

> **Note:** Once you change the BSM base URL, it is assumed that the client is initiating HTTP or HTTPS sessions using the new base URL. You must therefore ensure that the HTTP or HTTPS channel from the client to the new URL is enabled.

Configuring Secure Access to Apache

If you are using an Apache web server on the BSM Gateway server, and you decide to use SSL, you must configure the web server as described in this section. For more information, see http://httpd.apache.org/docs/2.2/ssl/.

1. Prepare the server certificate

    a. Obtain a signed server certificate from your certificate authority to the name of the BSM Gateway server. Typically this certificate comes in PKCS#12 format with a password protected private key.

    b. Separate the private key and the server public key using the openssl utility.

        For example: Go to **HPBSM\WebServer\bin**, run openssl, and use the following commands:

        ```
        pkcs12 -in c:\bsmcert.pfx -clcerts -nokeys -out c:\bsm_server_cert.pem
        pkcs12 -in c:\bsmcert.pfx -nocerts -nodes -out c:\bsm_server_key.pem
        ```

2. Update the Apache SSL configuration file

    a. Go to **<BSM Gateway Installation Directory>\WebServer\conf\extra**

    b. Open **httpd-ssl.conf** in a text editor.

    c. Look for the following lines and replace the file name in quotation marks with the path to the files produced in the previous step.

        ```
        SSLCertificateFile "c:/bsm_server_cert.pem"
        SSLCertificateKeyFile "c:/bsm_server_key.pem"
        ```

    d. Locate the line starting with **ServerName** and verify that this is the name that you issued the server certificate to.

    e. Close and save file.

3. Enable SSL

    a. Go to **<BSM Gateway Installation Directory>\WebServer\conf**

    b. Open **httpd.conf** in a text editor.

    c. Search the file for the string ssl to locate and uncomment the following lines (they are not consecutive):

        ```
        LoadModule ssl_module modules/mod_ssl.so

        Include conf/extra/httpd-ssl.conf
        ```

    d. Close and save the file.

4. Restart the Apache web service

   a. In Windows, go to **Start > Run** and type **services.msc**.

   b. Locate **HP Business Service Management Web Server**.

   c. Restart the Service.

   d. Test your https connection to the BSM Server to make sure you can log in. For example: **https://<BSM Gateway Server>/topaz**.

   e. When you have verified that the https connection works, close the http port by commenting out the line **Listen 80** in the **<BSM Gateway Installation Directory>\WebServer\conf\httpd.conf** file.

Configuring Secure Access to BSM Reverse Proxy

This chapter describes the security ramifications of reverse proxies and contains instructions for using a reverse proxy with BSM.

This chapter discusses only the security aspects of a reverse proxy. It does not discuss other aspects of reverse proxies, such as caching and load balancing.

A reverse proxy is an intermediate server that is positioned between the client machine and the Web server(s). To the client machine, the reverse proxy seems like a standard Web server that serves the client machine's HTTP or HTTPS protocol requests with no dedicated client configuration required.

The client machine sends ordinary requests for Web content, using the name of the reverse proxy instead of the name of a Web server. The reverse proxy then sends the request to one of the Web servers. Although the response is sent back to the client machine by the Web server through the reverse proxy, it appears to the client machine as if it is being sent by the reverse proxy.

BSM supports a reverse proxy in DMZ architecture. The reverse proxy is an HTTP or HTTPS mediator between the BSM data collectors/application users and the BSM servers.

Your data collectors may access BSM through the same virtual host or a different virtual host as your application users. For example, your environment may use one load balancer for application users and one load balancer for data collectors.

Configuring Secure Access to Apache Reverse Proxy

This procedure should be performed as part of the Hardening Workflow. For details, see "Hardening Workflow" on page 10.

1. Convert the root CA certificate obtained earlier to base 64 format.

   Openssl > x509 -in c:\ca_64.cer -out c:\ca.pem

2. Split certificate and private key.

    If the server certificate is in PFX format, split the certificate. In OpenSSL run the following commands to generate both certificate and private key in PEM format:

    pkcs12 -in C:\<server_certificate>.pfx -clcerts -nokeys -out C:\mycert.pem

    Enter Import Password: <your_password>

    MAC verified OK

    pkcs12 -in C:\<server_certificate>.pfx -nocerts -nodes -out C:\mykey.pem

    Enter Import Password: <your_password>

    MAC verified OK

3. Configure Apache to use the certificates.

    a. Edit **<Apache Installation Directory>/WebServer/conf/httpd.conf**

        uncomment these lines (remove #):

        LoadModule ssl_module modules/mod_ssl.so

        Include conf/extra/httpd-ssl.conf

    b. Edit **<Apache Installation Directory>/WebServer/conf/extra/httpd-ssl.conf**

        ○ Update SSLCertificateFile with path to <mycert.pem >

        ○ Update SSLCertificateKeyFile with path to <mykey.pem>

        ○ Insert the following lines in the virtual host section in httpd-ssl.conf with the path to the certificate authority key in PEM format:

            VirtualHost <Reverse Proxy FQDN>

            ProxyRequests Off

            SSLProxyEngine On

            SSLProxyCACertificateFile <path to file of ca who issued the proxy certificate, for example c:\ca.pem>

            SSLProxyVerify require

            # General setup for the virtual host

4. Close port 80

Open **<Apache installation directory>\Webserver\conf\httpd.conf** and comment out **listen 80** by adding # as a prefix.

5. Verify that Apache runs using SSL

   a. Restart Apache

   b. Go to https://<Reverse Proxy FQDN>.

      Do not use localhost, use the full server name that matches the name on the certificate. You should see the message "it works!"

   c. Go to http://<Reverse Proxy FQDN>.

      It should not work.

Configuring Secure Apache Reverse Proxy to Require Client Authentication - Optional

Configuring a secure reverse proxy to require client authentication involves manual procedures

1. Make the following changes in **<Apache installation directory>/conf/extra/httpd-ssl.conf**:

   a. Uncomment (remove the #) the following lines:

      SSLVerifyClient require

      SSLVerifyDepth 10

   b. Search for **SSLCACertificateFile**, uncomment it and update the path to the client CA root certificate for the authority that issued your client certificate.

      SSLCACertificateFile "C:\CA.pem"

   c. Locate the line **#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire**

      Add the following line right below it: **SSLOptions +ExportCertData**

   d. Add the following line before </VirtualHost>:

      RequestHeader set CLIENT_CERT_HEADER "%{SSL_CLIENT_CERT}s"

2. Edit the **<Apache installation directory>/conf/httpd.conf** file

   Uncomment (remove the #) from the following lines:

   LoadModule headers_module modules/mod_headers.so

   LoadModule rewrite_module modules/mod_rewrite.so

3. Restart Apache.

    Go to https://<Reverse Proxy FQDN>/topaz

    Verify that you see a prompt for a client certificate.

Configuring the URL for Accessing BSM with SSL

See "Configure URL for Accessing BSM with SSL" on page 23.

Configuring Secure Access to the JBoss HTML JMX Console

This task describes how to configure secure access to the JBoss HTML JMX console.

This procedure should be repeated for every BSM Gateway, DPS, and one-machine server.

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

    - **Option 1 - PKCS12 Format:** Obtain the server certificate from your corporate Certificate Authority in .pfx (PKCS12) format and skip to step 2.

    - **Option 2 - JKS Format:** Create a java keystore with the server certificate. For details, see "Creating a Java Keystore" on page 17.

2. Modify the file server.xml.

    a. Open the file
        <HPBSM root directory>\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml

    b. Locate the following section and replace the value of address with **127.0.0.1**.

        ```
        <Connector port="8080" address="${jboss.bind.address}" maxThreads="25
        0"
        maxHttpHeaderSize="8192" emptySessionPath="false" protocol="HTTP/1.1"
        enableLookups="false" redirectPort="29443" acceptCount="100"
        connectionTimeout="20000" disableUploadTimeout="true"
        URIEncoding="UTF-8" />
        ```

    c. Uncomment the section with Connector port="**29443**":

        ```
        <--!
        ```

```
<Connector port="29443" protocol="HTTP/1.1" SSLEnabled="true"
maxthreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

d. In the same section, 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="<path to keystore>" keystoreType="JKS"
keystorePass="<private key password>"
```

The section should now look similar to this:

```
<Connector port="29443" protocol="HTTP/1.1" SSLEnabled="true"
maxthreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="c:\mykeystore" keystoreType="JKS"
keystorePass="myprivatekeypassword" />
```

3. Modify the web.xml files in the following two locations:

- **<HPBSM root directory>\EJBContainer\server\mercury\ deploy\jmx-console.war\WEB-INF\web.xml**

- **<HPBSM root directory>\EJBContainer\server\mercury\ deploy\jboss-web.deployer\ROOT.war\WEB-INF\web.xml**

Add the **<user-data-constraint>** element as shown below immediately before the **</security-constraint>** element.

```
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>

</security-constraint>
```

4. Restart the BSM server.

Configuring Secure Access to the HTML JMX Console in other BSM processes

This task describes how to configure secure access to the HTML JMX console in other BSM processes.

To configure secure access to the JMX console in other BSM processes:

1. Open the following files:

   - <HPBSM root directory>\conf\spring\jmx-html-adaptor-spring.xml

   - <HPBSM root directory>\conf\supervisor\spring\jmx-html-adaptor-spring.xml

   and locate the following section in each:

   ```
   <bean id="jmx.html.adaptor" class="com.mercury.infra.utils.jmx.MX4JHtmlAd
   aptor"
          lazy-init="true">
   <property name="sslEnabled"><value>false</value></property>
   <property name="keyManagerAlgorithm"><value>SunX509</value></property>
   <property name="keyStorePassword"><value>changeit</value></property>
   <property name="keyManagerPassword"><value>changeit</value></property>
   <property name="keyStoreType"><value>JKS</value></property>
   <property name="sslProtocol"><value>TLS</value></property>
   <property name="keyStoreName"><value>file.keystore</value></property>
   </bean>
   ```

2. Update the relevant parameters, as indicated in the following table:

Parameter Name	Required Value
sslEnabled	true
keyStorePassword	The password you use to protect the keystore. This is the value of the keystore's **-storepass** parameter, if you created the keystore yourself.
keyManagerPassword	The password you use to protect the private key. This is the value of the keystore's **-keypass** parameter, if you created the keystore yourself.
keyStoreName	The name and path of the file where the keystore is located.

If you do not have a keystore available, you can create one. For details, see "Creating a Java Keystore" on page 17.

Configuring Secure Access to the JMX-RMI Channel Used for Internal BSM Communications

To secure access to the JMX-RMI channel used for internal BSM communications, you must configure JMX-RMI with basic authentication over SSL. This involves the following steps:

- Configuring user name/password authentication

- Configuring SSL for the JMX-RMI channel

Note:

- This procedure was written for Windows. Linux users should use Unix paths and commands as needed.

- If you are securing a JMX channel and using System Health, you must use the Encryption tool provided in the System Health installation to supply JMX monitor credentials to System Health. For details, see the HP System Health Guide.

- This procedure must be performed on every Gateway and Data Processing server in the BSM deployment.

Configuring User name/Password Authentication

1. Add user role.

   Add the user role to:
   <HPBSM root directory>\JRE64\lib\management\jmxremote.access.

   Example:

   ```
   adminUser readwrite \
        create javax.management.monitor.*,javax.management.timer.* \
        unregister
   ```

2. Create password file.

   a. Copy:
      <HPBSM root directory>\JRE64\lib\management\jmxremote.password.template
      to:
      jmxremote.password

b. Add the user role defined previously in jmxremote.access to the end of the jmxremote.password file, and set a clear text password. Remember this password so you can test it with the JMX console.

> Example:
>
> ```
> adminUser mypassword
> ```

3. Protect the password file.

   In Windows:

   a. Change the owner of the **jmxremote.password** file to be an administrator user or the SYSTEM user.

      If you change the owner to the SYSTEM user, you will not be able to view data on the BSM Status page.

      If you change the owner to an administrator user, you will need to change the default log on credentials to run the HP Business Service Management service. This procedure is performed in your operating system. In Windows Server 2008, the procedure is as follows:

      i. Run **services.msc**.

      ii. Right click **HP Business Service Management**.

      iii. In the **Log on** tab, select **This account** and enter the administrator credentials.

      Whatever user you select, you must use the same user for any other similar steps in this procedure.

      To change the owner of the files:

      i. Navigate to **Properties > Security > Advanced > Owner**.

      ii. Click Other Users or Groups, type "**<domain\admin user name>**" or "**SYSTEM**", and click **Check Names**.

      iii. Verify that you see that the value of Current Owner is updated.

   b. Change the permissions of jmxremote.password file to be **Full Control** for the owner defined above as follows:

      ○ For administrator user: **cmd: icacls jmxremote.password /P <domain\user name>:F**

      ○ For SYSTEM user: **cmd: icacls jmxremote.password /P SYSTEM:F**

In Linux:

Run the following command: **chmod 600 jmxremote.password**

4. Repeat the above steps for the **<HPBSM root directory>\JRE** directory.

5. Enable authentication on all BSM processes other than JBoss.

    Open **<HPBSM root directory>\bin\service_manager.bat** (in Linux, **service_manager.sh**) and set the authentication to **true**, as in the following example:

    -Dcom.sun.management.jmxremote.authenticate=true

6. Enable authentication on JBoss process.

    Open **<HPBSM root directory>\EJBContainer\bin\mercury_run.bat** (in Linux, **mercury_ run.sh**) and set the authentication to **true**, as in the following example:

    -Dcom.sun.management.jmxremote.authenticate=true

7. Enable authentication on nannyManager.

    Open **<HPBSM root directory>\conf\supervisor\manager\nannyManager.wrapper** and set the following:

    wrapper.java.additional.3=-Dcom.sun.management.jmxremote.authenticate=true

Configuring SSL for the JMX-RMI Channel

> **Note:** When creating a Java keystore password, make sure your private key password and the keystore password are the same.

1. Create Java keystore (JKS file). For details, see "Creating a Java Keystore" on page 17.

2. Create a JMX-RMI properties file with SSL parameters.

    Create **jmx-rmi.properties file in <HPBSM root directory>\conf** containing the following lines:

    ```
    com.sun.management.jmxremote.ssl=true

    javax.net.ssl.keyStore=<path to keystore file name with forward slashes>

    javax.net.ssl.keyStorePassword=<keystore password>
    ```

    > **Note:**

Use forward slashes only, not backslashes.

Example:

```
com.sun.management.jmxremote.ssl=true

javax.net.ssl.keyStore=c:/certificate.jks

javax.net.ssl.keyStorePassword=changeit
```

3. Protect the SSL parameters file.

    In Windows:

    a. Navigate to **Properties > Security > Advanced** and change the owner of the **jmx-rmi.properties** file to be an administrator user or the SYSTEM user.

        If you change the owner to the SYSTEM user, you will not be able to view data on the BSM Status page.

        If you change the owner to an administrator user, you will need to change the default log on credentials to run the HP Business Service Management service. This procedure is performed in your operating system. In Windows Server 2008, the procedure is as follows:

        i.   Run **services.msc**.

        ii. Right click **HP Business Service Management**.

        iii. In the **Log on** tab, select **This account** and enter the administrator credentials.

        Whatever user you select, you must use the same user for any other similar steps in this procedure.

        To change the owner of the files:

        i.   Navigate to **Properties > Security > Advanced > Owner**.

        ii. Click Other Users or Groups, type "**<domain\admin user name>**" or "**SYSTEM**", and click **Check Names**.

        iii. Verify that you see that the value of Current Owner is updated.

    b. Change the permissions of **jmx-rmi.properties** file to be **Full Control** for the file owner defined above as follows:

        ○ For administrator user: **cmd: icacls jmx-rmi.properties /P <domain\user name>:F**

        ○ For SYSTEM user: **cmd: icacls jmx-rmi.properties /P SYSTEM:F**

In Linux:

chmod 600 jmx-rmi.properties

4. Enable SSL on JMX-RMI for all BSM processes other than JBoss.

   Open **<HPBSM root directory>\bin\service_manager.bat** (in Linux, service_manager.sh) and make the following changes:

   a. Set the value of `-Dcom.sun.management.jmxremote.ssl=true` to **true**

   b. Add the following string immediately after the string you just modified:

   ```
   -Dcom.sun.management.jmxremote.ssl.config.file=<HPBSM root
   directory>/conf/jmx-rmi.properties
   ```

5. Enable SSL on JMX-RMI for JBoss process.

   Open **<HPBSM root directory>\EJBContainer\bin\mercury_run.bat** (in Linux, **mercury_ run.sh**) and make the following changes:

   a. Set the value of `-Dcom.sun.management.jmxremote.ssl=true`

   b. Add the following string immediately after the string you just modified:

   ```
   -Dcom.sun.management.jmxremote.ssl.config.file=<HPBSM root
   directory>/conf/ jmx-rmi.properties
   ```

6. Enable SSL on JMX-RMI for Nanny process.

   Open **<HPBSM root directory>\conf\supervisor\manager\nannyManager.wrapper** and set the following:

   a. Comment out the line with ssl:

   ```
   #wrapper.java.additional.4=-Dcom.sun.management.jmxremote.ssl=false
   ```

   b. Add this line instead:

   ```
   wrapper.java.additional.4=-Dcom.sun.management.jmxremote.ssl.config.file=
   <HPBSM root directory>/conf/jmx-rmi.properties
   ```

7. Make JVM trust the key defined in the keystore file.

   a. Export the public key from the keystore file (use regular keytool).

   > **Example:**

```
keytool -export -alias ca -keystore c:\certificate.jks -rfc -file ca_r
oot.cer
```

where **certificate.jks** is the keystore file, and **ca_root.cer** is the exported public key file.

b. Import the public key into **<HPBSM root directory>\JRE\lib\security\cacerts and <HPBSM root directory>\JRE64\lib\security\cacerts**.

Example:

```
<HPBSM installation directory>\JRE64\bin\keytool -import -alias ca -fi
le ca_root.cer -keystore <HPBSM installation directory>\JRE64\lib\secu
rity\cacerts
```

```
<HPBSM installation directory>\JRE\bin\keytool -import -alias ca -file
ca_root.cer -keystore <HPBSM installation directory>\JRE\lib\security\
cacerts
```

where **ca_root.cer** is the public key file, and **cacerts** is the default truststore used by JVM.

c. Enable the BSM Server. If the BSM server cannot be enabled, see **<HPBSM installation directory>\log\supervisor\wrapper.log**.

Configuring Secure Access to Data Collectors

For information on configuring secure access to data collectors, see the relevant data collector documentation.
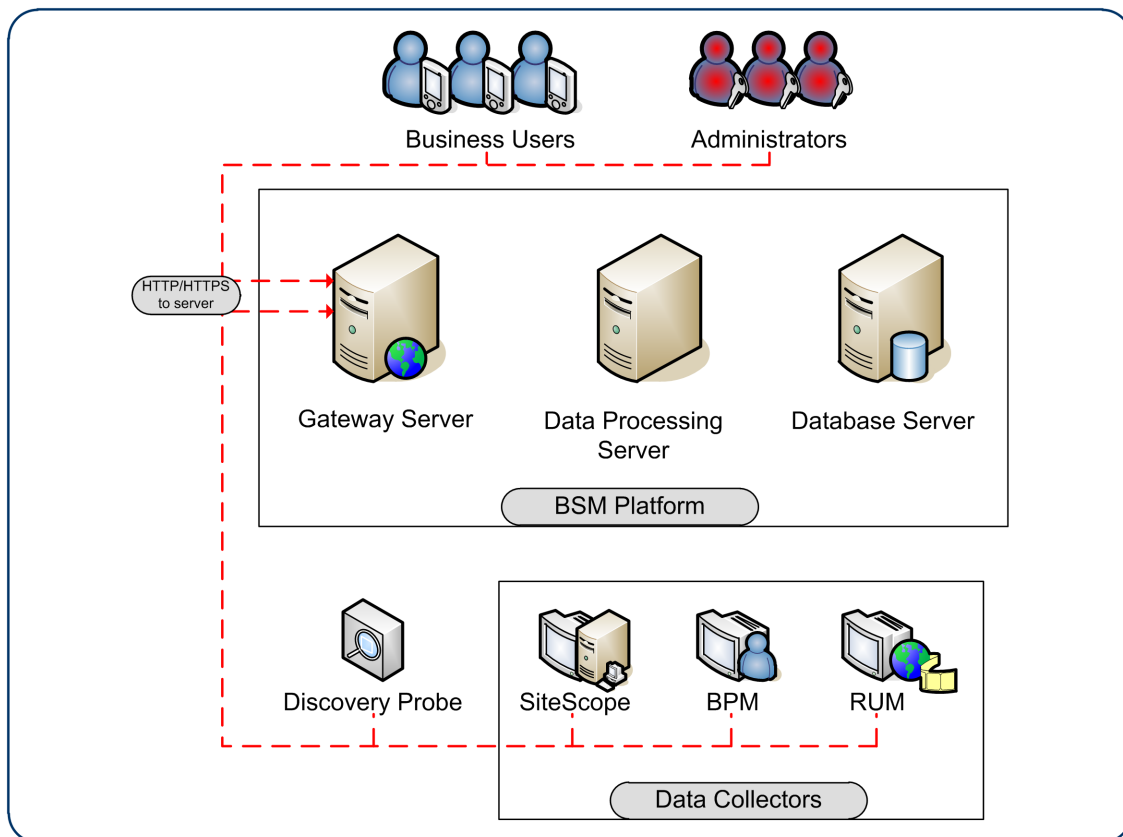
Chapter 4: Using Basic Authentication in BSM

The BSM platform fully supports the basic authentication schema, which provides BSM with the ability to authenticate a client communicating with a BSM server via HTTP or HTTPS.

The basic authentication schema is based on the client sending its credentials to the server so that the server can authenticate the client. The client's credentials are sent in a Base64 encoding format and are not encrypted in any way. If you are concerned that your network traffic may be monitored by a sniffer, it is recommended that you use basic authentication in conjunction with SSL. This sends the client's credentials over an encrypted wire (after the SSL handshake has been completed).

For information on configuring the BSM platform to support SSL communication, see "Using SSL in BSM" on page 15.

Possible basic authentication channels in BSM are illustrated in the following diagram:

Note: The BSM components do not support basic authentication with blank passwords. Do not use a blank password when setting basic authentication connection parameters

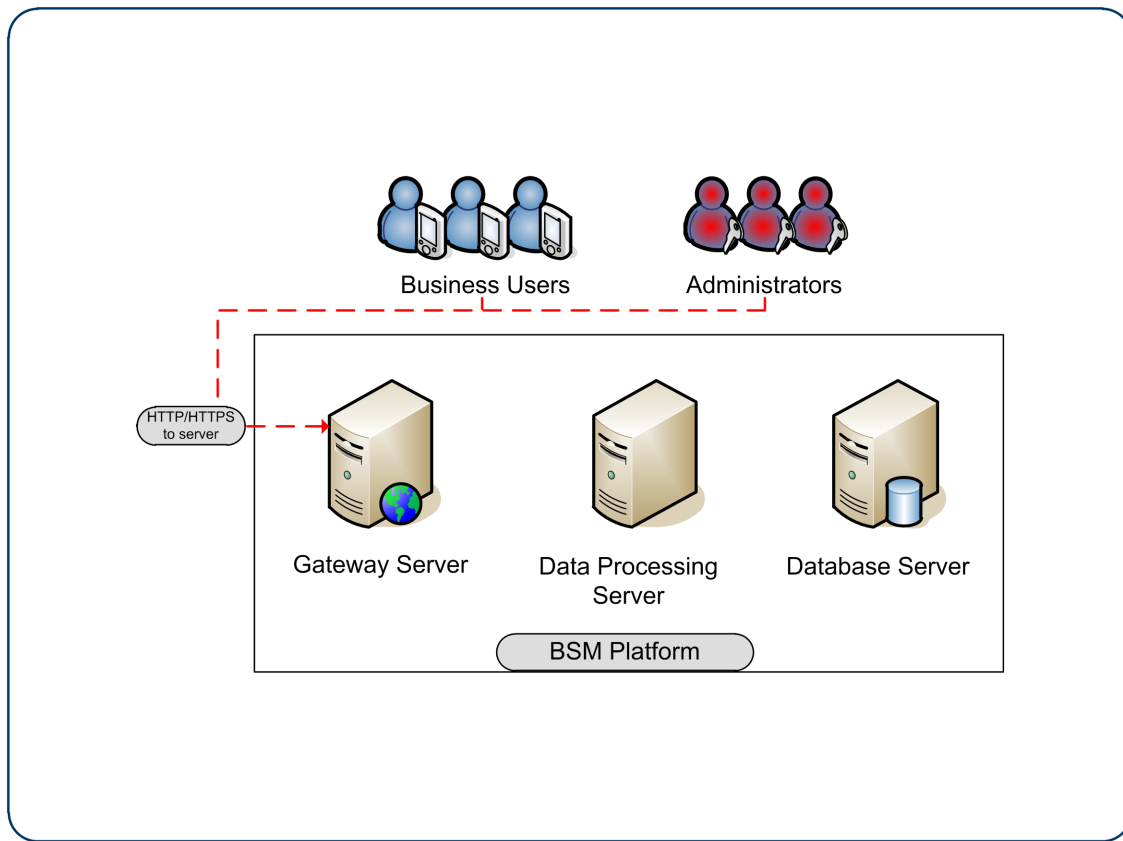# Overview of Configuring Basic Authentication in BSM

Before proceeding with the configuration steps, ensure that:

- The BSM platform is operating as it is supposed to without basic authentication.

- You read this chapter in its entirety before you begin performing the configuration.

- You define your authentication requirements and use basic authentication only where required.

Note: The configuration specified for each BSM server is also relevant for a single machine installation, in which the Gateway Server and Data Processing Server both reside on the same machine.

Configuring Basic Authentication Between the Gateway Server and Application Users

The instructions in this section describe how to configure the Gateway Server (or a BSM machine, in the case of a single machine installation) and its clients, and application users to support basic authentication.

Basic Authentication Configuration for the Gateway Server

This section provides instructions for configuring the Gateway Server (or a BSM machine, in the case of a single machine installation) to support basic authentication.

Caution: Some JREs request an additional username and password confirmation when accessing applets imbedded in BSM, such as the Service Health Topology Map, System Health, and IT Universe Manager.

Enable Basic Authentication Support on the Web Server

The first step in configuring the Gateway Server to support basic authentication is to configure the Web server used by the Gateway Server.

Note: On each Web server, make sure that you enable basic authentication only and disable anonymous access. Once you have enabled basic authentication, validate the settings by requesting a BSM resource and ensuring that you are prompted to insert basic authentication parameters.

- **Microsoft Internet Information Server (IIS) 5.0 and 6.0.** See http://support.microsoft.com/kb/324276/en-us for information on enabling basic authentication for all interaction with the Web server. Note that basic authentication should be enabled for the entire IIS Web Site under which you installed the BSM applications.

- **Apache HTTP Server 2.2.x**. See the http://httpd.apache.org/docs-2.0/howto/auth.html for information on enabling basic authentication for all interaction with the Web server, using **mod_auth**. Note that basic authentication should be enabled on all the directories used by the Web server.

Basic authentication can only be added in conjunction with enabling SSL on the web server.

Once you have performed the above configuration procedures, when you are using a Microsoft IIS 5.0 or 6.0 Web server, you must make sure that all the folders and files in use by BSM have the required NTFS permissions required for the users connecting to BSM.

Basic Authentication Configuration for the Application Users
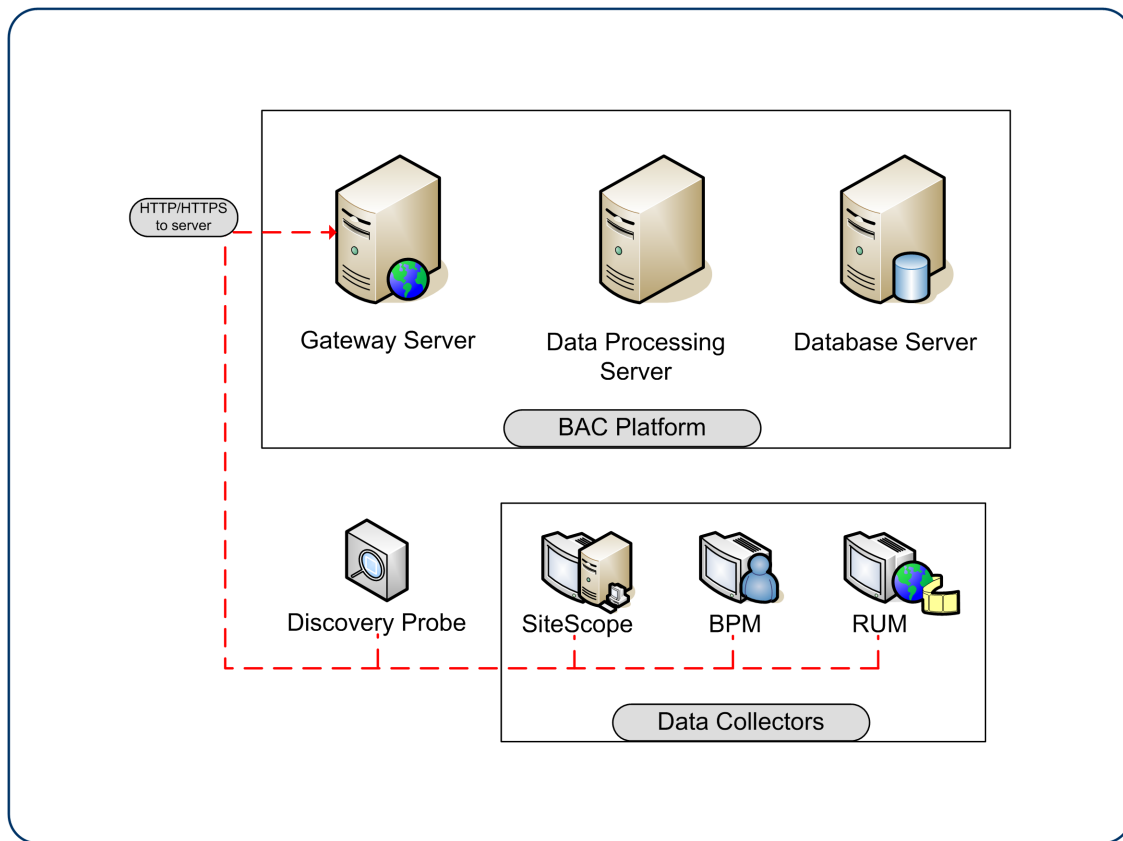
This section provides instructions for configuring the application users (Gateway Server clients) to support basic authentication.

To connect as an application user to a BSM server that requires basic authentication, it is only necessary for you to know the credentials of the user permitted to log in to the BSM Web server. When connecting to the Web server, you will be prompted to enter these credentials. The authentication is then performed automatically.

Configuring Basic Authentication Between the Gateway Server and Data Collectors

The instructions in this section describe how to configure the Gateway Server and the BSM data collectors to support basic authentication. To enable basic authentication support, you must make the required changes for the Gateway Server, as well as for all the BSM data collectors connecting to it using HTTP/S.

Basic Authentication Configuration for Gateway Servers

This section provides instructions for configuring the Gateway Server (or a BSM machine, in the case of a single machine installation) to support basic authentication.

Enable Basic Authentication Support on the Web Server

The first step in configuring the Gateway Server to support basic authentication is to configure the Web server used by the Gateway Server.

Note: On each Web server, make sure that you enable basic authentication only and disable anonymous access. Once you have enabled basic authentication, validate the settings by requesting a BSM resource and ensuring that you are prompted to insert basic authentication parameters.

- **Microsoft Internet Information Server (IIS) 5.0 and 6.0**. See http://support.microsoft.com/kb/324276/en-us for information on enabling basic authentication for all interaction with the Web server. Note that basic authentication should be enabled for the entire IIS Web Site under which you installed the BSM applications.

- **Apache HTTP Server 2.2.x**. See the http://httpd.apache.org/docs-2.2/howto/auth.html for information on enabling basic authentication for all interaction with the Web server, using mod_ auth. Note that basic authentication should be enabled on all the directories used by the Web server.

Once you have performed the above configuration procedures, when you are using a Microsoft IIS 5.0 or 6.0 Web server, you must make sure that all of the folders and files in use by BSM has the required NTFS permissions required for the users connecting to BSM.

After performing the above procedures, the Web server installed on the Gateway Server is configured to support basic authentication for HTTP/S communication.

Basic Authentication Configuration for Data Collectors

This section provides instructions for configuring the following BSM data collectors to support basic authentication.

> **Note:** The Staging Data Replicator (used during a staging upgrade) does not support basic authentication.

Business Process Monitor

If you configured the Gateway Server to require basic authentication, you must configure the Business Process Monitor to connect to the Gateway Server using basic authentication.

To configure the Business Process Monitor to use basic authentication:

1. Open the Business Process Monitor Admin (**http://<Business Process Monitor machine>:2696**).

2. In the Business Process Monitor page, identify the Business Process Monitor instance you want to configure from the **Instances** list and click the Edit button for the instance. The Edit Instance page opens.

3. In the **Authentication** section, enter the following parameter values:

   - **Authentication user name**. The user name to be used to log in to the Gateway Server.

   - **Authentication user password**. The user password to be used to log in to the Gateway Server.

   - **Authentication domain**. The domain name to be used to log in to the Gateway Server.

4. Click **Save Changes and Restart Instance**.

SiteScope

If you configured the Gateway Server to require basic authentication, you must configure the SiteScope machine to connect to the Gateway Server using basic authentication.

To configure the SiteScope machine to use basic authentication:

1. If you are configuring SiteScope using System Availability Management Administration, right-click the SiteScope you want to instruct to use basic authentication, and select **Edit**.

    a. In the Profile Settings section of the Edit SiteScope page, enter the following parameter values:

        ○ **Web server authentication user name**. The user name and domain of the Gateway Server (in the format domain\user name).

        ○ **Web server authentication password**. The password of the Gateway Server.

    b. Click OK at the bottom of the page and restart the SiteScope instance.

2. If you are configuring SiteScope using the SiteScope interface, select **Preferences > Integration Preferences**.

    a. In the Optional Settings section of the BSM Server Registration page, enter the following parameter values:

        ○ **Authentication username**. The user name and domain of the Gateway Server (in the format domain\user name).

        ○ **Authentication password**. The password of the Gateway Server.

    b. Click the Update button at the bottom of the page and restart the SiteScope instance.

BSM Connector

If you configured the Gateway Server to require basic authentication, you must configure the BSM Connector machine to connect to the Gateway Server using basic authentication.

To configure the BSM Connector machine to use basic authentication:

1. Go to **Admin > Integrations > BSM Connector Integrations**

2. Right-click the BSM Connector you want to instruct to use basic authentication, and select Edit.

    a. In the **Profile Settings** section of the Edit BSM Connector page, enter the following parameter values:

        ○ **Web server authentication user name**. The user name and domain of the Gateway Server (in the format domain\user name).

○ **Web server authentication password**. The password of the Gateway Server.

b. Click **OK** at the bottom of the page and restart the BSM Connector instance.

Real User Monitor

If you configured the Gateway Server to require basic authentication, you must configure the Real User Monitor engine machine to connect to the Gateway Server using basic authentication.

To configure the Real User Monitor engine machine to use basic authentication:

1. Open the Real User Monitor Web Console (**http://<Real User Monitor engine name>:8180/rumconsole**).

2. Click the **Configuration** tab.

3. Under **Basic Authentication**, select the **Use basic authentication** check box and enter the following parameter values:

   ▪ **Authentication user name**. The user name to be used to log in to the Gateway Server.

   ▪ **Authentication user password**. The user password to be used to log in to the Gateway Server.

   ▪ **Authentication domain**. The domain name to be used to log in to the Gateway Server.

4. Click **Save Configuration**.

Chapter 5: Troubleshooting and Limitations

Login Problems

Issue	Resolution
Login page does not load when using SSL	Check that server certificate was generated correctly. All fields must be filled in properly, including email, city, state, etc. For example, in IIS6, go to **Default WebSite > Directory Security > Certificates > View > Details**. Subject should be filled in completely. Enhanced Key Usage must be "Server Authentication".
Cannot log in through Reverse Proxy; login page not fully displayed	Try to log in directly to BSM Gateway, bypassing the proxy. Make sure that the port (even if it is default port) is specified in Platform Administration infrastructure settings (**Default Virtual Gateway Server for Application Users URL**) for the virtual URLs. If you change virtual server URLs, restart BSM.
Cannot log in through Reverse Proxy	A firewall in the environment may be blocking BSM server from resolving Reverse Proxy IP address. **Solution:** Remove Reverse Proxy IP address from the settings, restart BSM servers, and try again.
Cannot log in; blank page or error in login.jsp - permission denied	• This is typically a result of inconsistency in Host Configuration infrastructure settings. **Solution:** Try to log in directly to the BSM Gateway (bypassing Reverse Proxy) and verify that the virtual host URL for application server is correct. Copy/paste it into the browser and check that the page will load. • The virtual URLs may reference the reverse proxy, or vice versa, when reverse proxy is not used. **Solution:** Fix the settings, restart BSM server, and try again. To restore to clean, set these to empty string using JMX console (context = platform): ▪ default.centers.server.url = empty or original (with port) ▪ default.core.server.url ▪ Enable.reverse.proxy = false ▪ Http.reverse.proxy.ip = empty

Issue	Resolution
Internal error when trying to load BSM url; FileNotFound error in topaz_all.ejb.log for lwssofmconf.xml	Most likely, the path to the keystore is incorrect after upgrade or new lines were introduced into the setting when manually updated. **Solution:** 1. Fix configuration: http://<BSM_SERVER>:<JBOSS_PORT>/jmx-console/ (Domain: Foundations, Service: Infrastructure Settings Manager) To retrieve configuration in a string format, use **getGlobalSettingValue()** with: contextName=**SingleSignOn** settingName=**lw.sso.configuration.xml**. Make sure that the new configuration is stored in a single-lined string! No newlines are expected. You can use any text editor to change the configuration as desired. To store configuration, use **setGlobalSettingValue()** with contextName=**SingleSignOn** settingName=**lw.sso.configuration.xml** newValue=**<NEW_VALUE_STRING>** 2. Reload configuration: go to service = **SSO** invoke **Start()**

Establishing Trust in a Browser for Self Signed Certificates

BSM application users (Gateway Server clients) use Web browsers to communicate with the Gateway Server. The Web browsers can be configured to support SSL.

When a session is started between the browser and the Gateway Server, the Gateway Server's Web server sends the browser a server-side certificate that was issued by a Certification Authority (CA). If the certificate used by the Web server is issued by a known CA, the certificate can generally be validated by the browser and no configuration is required. However, if the CA is not trusted by the browser, the browser machine must be configured to validate the server-side certificate that is sent. For instructions on setting CA certificate recognition in the browser and configuring browser certificate validation, refer to your browser vendor documentation.

For example, if you are working with Internet Explorer 7.0, you can import a certificate to the truststore used by the browser.

To import a certificate to the truststore used by the browser:

1. Select **Tools > Internet Options** and click the **Content** tab.

2. Click the **Certificates** button.

3. In the **Trusted Root Certification Authorities** tab, click **Import**.

4. Link to the certificate you want to trust and import it.

> **Note:** You can import one of the following to the truststore:
>
> ● The Gateway Server's certificate.
>
> ● The certificate of the Certificate Authority (CA) that issued the Gateway Server's certificate.
>
> If you do not import the CA's certificate, you must import the certificate of each individual Gateway Server that you are working with.

If you are not using a publicly known Certificate Authority (CA), you must import your own CA root certificate into the truststore of BSM's JVM for communicating with the data collectors over SSL.

Handling Security Certificate Expiration

If the webserver on BSM Gateway is configured for SSL and the server certificate expires, perform the following steps:

1. Change the webserver configuration files to use a new certificate:

   ▪ **IIS:** Import the new certificate.

   ▪ **Apache**: Update **httpd-ssl.conf** to use new certificate files.

2. Restart the webserver (IIS or Apache service).

3. Make sure you get no certificate errors when accessing the BSM user interface through the https protocol.

We appreciate your 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 Hardening Guide (Business Service Management 9.24)

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.