HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.13

Hardening Guide

Document Release Date: May 2012
Software Release Date: May 2012

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 Notices

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 (**http://www.apache.org**).

This product includes software developed by the JDOM Project (**http://www.jdom.org**).

This product includes software developed by the MX4J project (**http://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 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

Table of Contents

Welcome to This Guide 9
Who Should Read This Guide 9
How Do I Find the Information That I Need? 9
Additional Online Resources...11
Documentation Updates 12

Chapter 1: Hardening Workflow...13

Chapter 2: Introduction to Hardening the BSM Platform 19
Introduction to Hardening..19
Deploying BSM in a Secure Architecture 20
Tracking Login Attempts and Logged In Users......................................21
Recommendations and Notes 22

Chapter 3: Using a Reverse Proxy in BSM 25
Overview of Reverse Proxies..26
Security Aspects of Using Reverse Proxies..26
BSM and Reverse Proxies...27
Specific and Generic Reverse Proxy Mode Support for BSM...............28
Using a Reverse Proxy 29

Chapter 4: Using SSL in BSM 45
Introducing SSL Deployment in BSM 46
Issuing SSL Certificates...48
SSL-Supported Topologies in BSM 51
Configuring BSM to Work with SSL...51
Configuring SSL from Application Users to the Gateway Server........53
Handling Security Certificate Expiration 55
Creating a Keystore 55
Configuring Tomcat to Support HTTPS 58
Configuring JBOSS to work with SSL 60
Configuring the JMX Console to Work with
SSL in Other Processes 63
Securing JMX-RMI Channel Used for Internal
BSM Communications..64
Using SSL Offloader..69

Chapter 5: Using SSL with TransactionVision.....................................71
About SSL and TransactionVision...72
Configuring SSL Between a TransactionVision Processing
Server and the BSM Gateway Server 73

Chapter 6: Using Basic Authentication in BSM 79
Introducing Basic Authentication Deployment in BSM.....................80
Configuring Basic Authentication Between the Gateway
Server and Application Users...83
Configuring Basic Authentication Between the Gateway
Server and the Data Collectors 86
Auto Upgrading Data Collectors Remotely when Using
Basic Authentication..90

Chapter 7: Troubleshooting and Limitations 93

Index...97

Welcome to This Guide

This chapter includes:

- Who Should Read This Guide on page 9
- How Do I Find the Information That I Need? on page 9
- Additional Online Resources on page 11
- Documentation Updates on page 12

Who Should Read This Guide

This guide is intended for the following users of BSM:

- BSM administrators
- Security administrators

Readers of this guide should be highly knowledgeable about enterprise system security.

How Do I Find the Information That I Need?

This guide is part of the HP Business Service Management Documentation Library. This Documentation Library provides a single point of access for all Business Service Management documentation.

You can access the Documentation Library by doing the following:

- In Business Service Management, select **Help** > **Documentation Library**.
- From a Business Service Management Gateway Server machine, select **Start** > **Programs** > **HP Business Service Management** > **Documentation**.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport user ID, go to:

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

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

1

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 "Recommendations and Notes" on page 22.

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 48.

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 two 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 balancers, a reverse proxy, or BSM Gateway servers. Use the web server documentation depending on your web server type and version:

- **For IIS web server.** The Microsoft Web site (http://www.microsoft.com).
- **For Apache web server.** The Apache Jakarta Web site (http://httpd.apache.org).

5 Establish trust to the Certificate Authority

On all BSM Gateway servers, establish trust to the Certificate Authority that issued the BSM server certificates above.

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 every data collector 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 on page 14 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	See the *HP Business Process Monitor Administrator's Guide*.
SIS	See *the HP SiteScope Deployment Guide* PDF
RUM	See the *Real User Monitor Administration* PDF
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 *RTSM Data Flow Management Guide*.
Transaction Vision	See the *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 applications servers (port 8080) are not secured. We recommend securing them as well. For details, see "Configuring JBOSS to work with SSL" on page 60.

10 Configure mutual SSL

If the connection to BSM requires a client certificate, perform the appropriate procedures:

Data Collector / Server type	Relevant Documentation
BSM front-end server (could be a web server on the Gateway server, a load balancer, or a reverse proxy)	Follow the standard procedures for requiring client certificates on the front end of your choice. (could be a web server on the Gateway server, a load balancer, or a reverse proxy). For details, see "How to Secure User Access to BSM Using Client-Side Authentication Certificates" in the *Platform Administration* guide
BPM	See the *HP Business Process Monitor Administrator's Guide*.
SIS	"Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.
RUM	See the *Real User Monitor Administration* PDF.
Data Flow Probe	See the *RTSM Data Flow Management Guide*.

11 (Recommended) Secure data collectors admin consoles with SSL

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 Tomcat to Support HTTPS" on page 58
SIS	"Configuring Tomcat to Support HTTPS" on page 58
RUM	"Configuring Tomcat to Support HTTPS" on page 58
Transaction Vision	"Enable SSL on the TransactionVision Processing Servers" on page 75

12 (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 only be performed if there is a specific reason to do so. For details, see "Securing JMX-RMI Channel Used for Internal BSM Communications" on page 64.

13 (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 the JMX Console to Work with SSL in Other Processes" on page 63.

2

Introduction to Hardening the BSM Platform

This chapter includes:

➤ Introduction to Hardening on page 19

➤ Deploying BSM in a Secure Architecture on page 20

➤ Tracking Login Attempts and Logged In Users on page 21

➤ Recommendations and Notes on page 22

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 servers are installed on the same machine) and distributed (where all servers 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.

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**

  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 "Using a Reverse Proxy in BSM" 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.

Tracking Login Attempts and Logged In Users

To track who has attempted to log in to the system:

See **<HPBSM root directory>\log\EJBContainer\UserActions.servlets.log**.

The appender for this file is located in **<HPBSM root directory>\conf\core\Tools\log4j\EJB\topaz.properties**.

To display a list of users currently logged in to the system:

1. Open the JMX console on this machine. For detailed instructions, see "Using the JMX Console" in the *Platform Administration* guide.
2. Under the **Topaz** section, select **service=Active Topaz Sessions**.
3. Invoke the java.lang.String showActiveSessions() operation.

Recommendations and Notes

- **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 1, "Hardening Workflow".
  - **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 (Session Details, Session Analyzer, etc.). For details, see "Security Officer" in the *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.

3

Using a Reverse Proxy in BSM

This chapter includes:

- Overview of Reverse Proxies on page 26
- Security Aspects of Using Reverse Proxies on page 26
- BSM and Reverse Proxies on page 27
- Specific and Generic Reverse Proxy Mode Support for BSM on page 28
- Using a Reverse Proxy on page 29

Overview of Reverse Proxies

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.

Security Aspects of Using Reverse Proxies

A reverse proxy functions as a bastion host. It is configured as the only machine to be addressed directly by external clients, and thus obscures the rest of the internal network. Use of a reverse proxy enables the application server to be placed on a separate machine in the internal network, which is a significant security objective.

This chapter discusses the use of a reverse proxy in DMZ architecture, the more common security architecture available today.

DMZ (Demilitarized Zone) is a network architecture in which an additional network is implemented, enabling you to isolate the internal network from the external one. Although there are a few common implementations of DMZs, this chapter discusses the use of a DMZ and reverse proxy in a back-to-back topology environment.

The following are the main security advantages of using a reverse proxy in such an environment:

- No DMZ protocol translation occurs. The incoming protocol and outgoing protocol are identical (only a header change occurs).
- Only HTTP or HTTPS access to the reverse proxy is allowed, which means that stateful packet inspection firewalls can better protect the communication.
- 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 more).
- The reverse proxy screens the IP addresses of the real 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 (as opposed to other solutions).
- The reverse proxy requires a minimal number of open ports in the firewall.
- The reverse proxy provides good performance compared to other bastion solutions.

BSM and Reverse Proxies

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.

BSM must be configured to recognize use of a reverse proxy.

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. To configure a reverse proxy for either of these architectures, see "Using a Reverse Proxy" on page 29.

Specific and Generic Reverse Proxy Mode Support for BSM

BSM servers reply to application users by sending a base URL that is used to calculate the correct references in the HTML requested by the user. When a reverse proxy is used, BSM must be configured to return the reverse proxy base URL, instead of the BSM base URL, in the HTML with which it responds to the user.

If the reverse proxy is being used for data collectors only, configuration is required only on the data collectors and reverse proxy, and not on the BSM server(s).

There are two proxy modes that control user access to BSM servers:

➤ "Specific Mode" on page 28

➤ "Generic Mode" on page 29

Specific Mode

This mode should be used if you want to concurrently access BSM servers through specific reverse proxies and by direct access. Accessing the server directly means that you are bypassing the firewall and proxy because you are working within your intranet.

If you are working in this mode, each time an application user's HTTP/S request causes BSM to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Server URL** or the **Local Server URL** (when defined), if the HTTP/S request came through one of the IP addresses defined for the **HTTP** or **HTTPS Reverse Proxy IPs** parameter. If the HTTP/S request did not come through one of these IP addresses, the base URL that BSM receives in the HTTP/S request is the base URL that is returned to the client.

Generic Mode

This mode is used when you try to access the Gateway server via the reverse proxy. Any URLs requested are rewritten and sent back with the virtual IP of the Gateway server.

If you are working in this mode, each time an HTTP/S request causes the BSM application to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Server URL** or the **Local Virtual Server URL** (when defined).

Note that when using this mode, you must ensure that all BSM clients are accessing the BSM servers via the URL defined for the **Default Virtual Server URL** or the **Local Virtual Server URL** parameters.

Using a Reverse Proxy

This section includes the following topics:

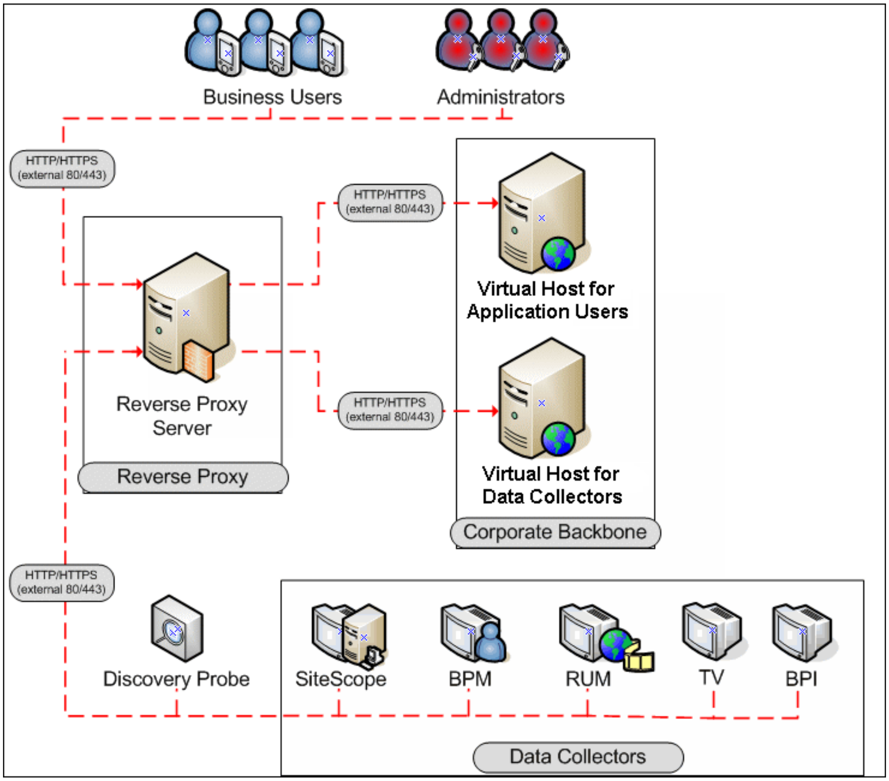
- "Reverse Proxy Configuration" on page 29
- "Configuring BBC Port 383 Connection on Reverse Proxy" on page 36
- "HP BSM Specific Configuration" on page 38
- "Limitations" on page 41
- "Apache 2.x – Distributed Configuration Example" on page 41

Reverse Proxy Configuration

In this topology, the reverse proxy context is divided into two sections:

- Communication that is redirected to the Virtual Host for Data Collectors.
- Communication that is redirected to the Virtual Host for Application Users.

The use of a reverse proxy is illustrated in the diagram below. 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.


Business Users
Administrators
HTTP/HTTPS (external 80/443)
HTTP/HTTPS (external 80/443)
Virtual Host for Application Users
Reverse Proxy Server
Reverse Proxy
HTTP/HTTPS (external 80/443)
Virtual Host for Data Collectors
Corporate Backbone
HTTP/HTTPS (external 80/443)
Discovery Probe
SiteScope
BPM
RUM
TV
BPI
Data Collectors

Reverse proxy BSM support should be configured differently in each of the following cases:

Scenario #	BSM Components Behind the Reverse Proxy
1	Data collectors (Business Process Monitor, Real User Monitor, SiteScope, Data Flow Probe)

Scenario #	BSM Components Behind the Reverse Proxy
2	Application users
3	Data collectors and application users

Note:

- Different reverse proxies may require different configuration syntaxes. For an example of an Apache 2.x reverse proxy distributed configuration, see "Apache 2.x – Distributed Configuration Example" on page 41.
- When configuring a Reverse Proxy with TransactionVision, only one instance of the TransactionVision UI/Job Server exists, even if there are multiple Gateway Servers in your environment.

Support for BSM Data Collectors

The following configuration is required on the reverse proxy for data collectors to connect via the reverse proxy to the Virtual Host for Data Collectors:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/topaz_api/*	http://[Virtual Host for Data Collectors]/topaz/topaz_api/* https://[Virtual Host for Data Collectors]/topaz/topaz_api/*
/topaz/sitescope/*	http://[Virtual Host for Data Collectors]/topaz/sitescope/* https://[Virtual Host for Data Collectors]/topaz/sitescope/*
/ext/*	http://[Virtual Host for Data Collectors]/ext/* https://[Virtual Host for Data Collectors]/ext/*
/cm/*	http://[Virtual Host for Data Collectors]/cm/* https://[Virtual Host for Data Collectors]/cm/*

Requests for... on the Reverse Proxy Server	**Proxy Request to be Served by:**
/axis2/*	http://[Virtual Host for Data Collectors]/axis2/* https://[Virtual Host for Data Collectors]/axis2/*
/mam-collectors/*	http://[Virtual Host for Data Collectors]/mam-collectors/* https://[Virtual Host for Data Collectors]/mam-collectors/*
/tv/*	http://[HP TransactionVision UI/Job Server]: 21000/tv/* https://[HP TransactionVision UI/Job Server]: 21001/tv/* **Note:** If you want to use AJP to enable the Reverse Proxy server to communicate with the HP TransactionVision UI/Job Server, use the following: http://[HP TransactionVision UI/Job Server]: 21002/tv/*
/axis2/*	http://[Virtual Host for Data Collectors]/axis2/* https://[Virtual Host for Data Collectors]/axis2/* **Note:** Required if SOAP adaptor is used with embedded Run-time Service Model (RTSM) for replication into secure BSM via reverse proxy.

Note: Make sure your reverse proxy supports priority handling logic, which enables a specific expression to be handled before a more generic one, if required. For example, the **/topaz/topaz_api/*** expression must be handled before the **/topaz/*** expression.

For some reverse proxies, a reverse pass is also required. The reverse pass changes the HTTP or HTTPS headers returned from the server to relative headers. For an example of a reverse pass, see "Apache 2.x – Distributed Configuration Example" on page 41.

Support for BSM Application Users

The following configuration is required on the reverse proxy for application users to connect via the reverse proxy to the Virtual Host for Application Users:

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/hpbsm/*	http://[Virtual Host for Application Users] /hpbsm/* https://[Virtual Host for Application Users] /hpbsm/*
/bpi/*	http://[Virtual Host for Application Users] /bpi/* https://[Virtual Host for Application Users] /bpi/*
/filters/*	http://[Virtual Host for Application Users] /filters/* https://[Virtual Host for Application Users] /filters/*
/mam/*	http://[Virtual Host for Application Users] /mam/* https://[Virtual Host for Application Users] /mam/*
/mam_images/*	http://[Virtual Host for Application Users] /mam_images/* https://[Virtual Host for Application Users] /mam_images/*
/mcrs/*	http://[Virtual Host for Application Users] /mcrs/* https://[Virtual Host for Application Users] /mcrs/*

Requests for... on the Reverse Proxy Server	**Proxy Request to be Served by:**	
/mercuryam/*	http://[Virtual Host for Application Users]/mercuryam/* https://[Virtual Host for Application Users]/mercuryam/*	
/odb/*	http://[Virtual Host for Application Users]/odb/* https://[Virtual Host for Application users]/odb/*	
/opal/*	http://[Virtual Host for Application Users]/opal/* https://[Virtual Host for Application Users]/opal/*	
/opr-admin-server/messagebroker/amfpolling/*	http://[Virtual Host for Application Users]/opr-admin-server/messagebroker/amfpolling/* https://[Virtual Host for Application Users]/opr-admin-server/messagebroker/amfpolling**secure**/*	**Note:** Append the word **secure** to each resource URL when using https.
/opr-admin-server/messagebroker/amf/*	http://[Virtual Host for Application Users]/opr-admin-server/messagebroker/amf/* https://[Virtual Host for Application Users]/opr-admin-server/messagebroker/amf**secure**/*	
/opr-console/messagebroker/amf/*	http://[Virtual Host for Application Users]/opr-console/messagebroker/amf/* https://[Virtual Host for Application Users]/opr-console/messagebroker/amf**secure**/*	
/opr-admin-server/*	http://[Virtual Host for Application Users]/opr-admin-server/* https://[Virtual Host for Application Users]/opr-admin-server/*	

Requests for... on the Reverse Proxy Server	**Proxy Request to be Served by:**
/opr-console/*	http://[Virtual Host for Application Users]/opr-console/* https://[Virtual Host for Application Users]/opr-console/*
/opr-gateway/*	http://[Virtual Host for Application Users]/opr-gateway/* https://[Virtual Host for Application Users]/opr-gateway/*
/OVPM/*	http://[Virtual Host for Application Users]/OVPM/* https://[Virtual Host for Application Users]/OVPM/*
/rumproxy/*	http://[Virtual Host for Application Users] /rumproxy/* https://[Virtual Host for Application Users] /rumproxy/*
/topaz/*	http://[Virtual Host for Application Users] /topaz/* https://[Virtual Host for Application Users] /topaz/*
/TopazSettings/*	http://[Virtual Host for Application Users] /TopazSettings/* https://[Virtual Host for Application Users] /TopazSettings/*
/tv/*	http://[Virtual Host for Application Users] /tv/* https://[Virtual Host for Application Users] /tv/*
/tvb/*	http://[Virtual Host for Application Users] /tvb/* https://[Virtual Host for Application Users] /tvb/*
/ucmdb-api/*	http://[Virtual Host for Application Users] /ucmdb-api/* https://[Virtual Host for Application users] /ucmdb-api/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/ucmdb-ui/*	http://[Virtual Host for Application Users] /ucmdb-ui/* https://[Virtual Host for Application users] /ucmdb-ui/*
/uim/*	http://[Virtual Host for Application Users] /uim/* https://[Virtual Host for Application Users] /uim/*
/webinfra/*	http://[Virtual Host for Application Users] /webinfra/* https://[Virtual Host for Application Users] /webinfra/*

Configuring BBC Port 383 Connection on Reverse Proxy

For the HP OM server to be able to forward events to the HP BSM server in the reverse proxy environment, port 383 used by the BBC protocol must be configured on the reverse proxy.

The following general steps use Apache as an example:

1 Use the utility below to issue a certificate for the ReverseProxy node. This can be done from the BSM processing server or any OM server, but not from the BSM gateway server.

For example:

```
ovcm -issue -file <certificate_file> -name <FQDN (fully qualified domain name) of Reverse Proxy> [-pass <passphrase>]
```

2. Use openssl to convert it for use by Apache reverse proxy, as in the following:

   SSLCertificateFile:
   ```
   openssl pkcs12 -in <certificate_file> -out oprcl.crt
   ```

   SSLCertificateKeyFile:
   ```
   openssl rsa -in oprcl.crt -out oprcl.pem
   ```

   SSLProxyMachineCertificateFile:
   ```
   openssl pkcs12 -in <certificate_file> -out oprcl.p12 -nodes -clcerts
   ```

3. Copy SSLCertificateFile, SSLCertificateKeyFile and SSLProxyMachineCertificateFile to the reverse proxy machine (in this example, to the locations <Apache_Install_Dir>/Apache2.2/conf/oprcl.crt, <Apache_Install_Dir>/Apache2.2/conf/oprcl.pem, and <Apache_Install_Dir>/Apache2.2/conf/oprcl.p12, respectively).

4. Modify httpd-ssl.conf to:

   a Listen on port 383

b Add a virtual host section for port 383, for example:

```
<VirtualHost <FQDN of Reverse Proxy>:383>
ServerName <value of "friendlyName" in oprcl.crt>
ServerAlias <hostname of RP>
ServerAdmin <admin email>
DocumentRoot "<Apache_Install_Dir>/Apache2.2/htdocs"
ErrorLog "<Apache_Install_Dir>/Apache2.2/logs/<FQDN of Reverse Proxy>-error.log"
TransferLog "<Apache_Install_Dir>/Apache2.2/logs/<FQDN of Reverse Proxy>-
access.log"
ProxyRequests Off
SSLProxyEngine on
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile "<Apache_Install_Dir>/Apache2.2/conf/oprcl.crt"
SSLCertificateKeyFile "<Apache_Install_Dir>/Apache2.2/conf/oprcl.pem"
SSLProxyMachineCertificateFile "<Apache_Install_Dir>/Apache2.2/conf/oprcl.p12"
<Proxy *>
Order deny,allow
Allow from "<DomainName> e.g. .devlab.ad"
</Proxy>
ProxyPass / "https://<FQDN of BSM Gateway>:383/"
ProxyPassReverse / "https://<FQDN of BSM Gateway>:383/"
</VirtualHost>
```

HP BSM Specific Configuration

In addition to configuring the reverse proxy to work with BSM, you must configure BSM to work with the reverse proxy.

Note: BSM must be configured only if application users are connected via a reverse proxy to BSM. If the reverse proxy is being used for data collectors only, skip the instructions in this section.

To configure BSM to work with the reverse proxy:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings.** Click **Foundations** and select the **Platform Administration** context from the drop-down box.

2 In the Platform Administration - Host Configuration pane, set the following parameters:

- **Default Virtual Gateway Server for Application Users URL** and **Default Virtual Gateway Server for Data Collectors URL.** Verify that these parameters represent the URL of the machine (reverse proxy, load balancer, or other type of machine) used to access the Gateway server machine. For example, http://my_reverse_proxy.example.com:80.

  If you are using a NAT device to access the Gateway server, enter the full URL of the NAT device. For example, http://nat_device.example.com:80.

- **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 ones defined for the Default Virtual Server URLs, above) to access the Gateway server machine, define a Local Server URL for each machine through which you want to access the Gateway server machine. For example, http://my_specific_virtual_server.example.com:80.

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

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

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

3 In the Reverse Proxy Configuration pane, set the following parameters:

➤ **HTTP or HTTPS Reverse Proxy IPs** (optional). Configure the IP addresses of the reverse proxy or proxies used to communicate with the Gateway server machine. If a Load Balancer is in use, you must also add the IP addresses of the Load Balancers to this setting.

If the IP address of the reverse proxy sending the HTTP/S request is included in the list of IP addresses defined for this parameter, the URL returned to the client is either the **Default Virtual Server URL** or the **Local Virtual Server URL** (when defined). If the IP address of the reverse proxy sending the HTTP/S request is not included in the list of IP addresses defined for this parameter, the Gateway server machine returns the base URL that it receives in the HTTP/S request.

Note: If no IP addresses are defined for this parameter (the default option), BSM works in Generic Mode and the Gateway server machine returns the **Default Virtual Server URL** or the **Local Virtual Server URL** (when defined) to the client in all cases.

➤ **Enable Reverse Proxy**. Set this parameter to **true**. Note that this must be done after the above parameters have been configured.

4 Restart the HP BSM service on the BSM Gateway and Data Processing servers.

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.

Limitations

If you configured BSM to work in Generic Mode, all the BSM clients must access the BSM machine via the reverse proxy.

Apache 2.x – Distributed Configuration Example

Below is a sample configuration file that supports the use of an Apache 2.x reverse proxy in a case where data collectors are connecting to the Virtual Host for Data Collectors and application users are connecting to the Virtual Host for Application Users through the same reverse proxy.

Note: In the example below, the Virtual Host for Data Collectors is **DATA** and the Virtual Host for Application Users is **USERS**.

1 Open the <**Apache machine root directory**>**\Webserver\conf\httpd.conf** file.

2 Enable the following modules:

- **LoadModule proxy_module modules/mod_proxy.so**
- **LoadModule proxy_http_module modules/mod_proxy_http.so**

3 Add the following lines:

```
ProxyRequests off

<Proxy *>

        Order deny,allow

        Deny from all

        Allow from all

</Proxy>

ProxyPass              /ext                 http://DATA/ext
ProxyPassReverse       /ext                 http://DATA/ext
ProxyPass              /topaz/topaz_api     http://DATA/topaz/topaz_api
ProxyPassReverse       /topaz/topaz_api     http://DATA/topaz/topaz_api
```

```
ProxyPass           /mam-collectors     http://DATA/mam-collectors
ProxyPassReverse    /mam-collectors     http://DATA/mam-collectors
ProxyPass           /mercuryam          http://USERS/mercuryam
ProxyPassReverse    /mercuryam          http://USERS/mercuryam
ProxyPass           /hpbsm              http://USERS/hpbsm
ProxyPassReverse    /hpbsm              http://USERS/hpbsm
ProxyPass           /topaz              http://USERS/topaz
ProxyPassReverse    /topaz              http://USERS/topaz
ProxyPass           /webinfra           http://USERS/webinfra
ProxyPassReverse    /webinfra           http://USERS/webinfra
ProxyPass           /filters            http://USERS/filters
ProxyPassReverse    /filters            http://USERS/filters
ProxyPass           /TopazSettings      http://USERS/TopazSettings
ProxyPassReverse    /TopazSettings      http://USERS/TopazSettings
ProxyPass           /opal               http://USERS/opal
ProxyPassReverse    /opal               http://USERS/opal
ProxyPass           /mam                http://USERS/mam
ProxyPassReverse    /mam                http://USERS/mam
ProxyPass           /mam_images         http://USERS/mam_images
ProxyPassReverse    /mam_images         http://USERS/mam_images
ProxyPass           /mcrs               http://USERS/mcrs
ProxyPassReverse    /mcrs               http://USERS/mcrs
ProxyPass           /rumproxy           http://USERS/rumproxy
ProxyPassReverse    /rumproxy           http://USERS/rumproxy
ProxyPass           /bpi                http://USERS/bpi
ProxyPassReverse    /bpi                http://USERS/bpi
ProxyPass           /odb                http://USERS/odb
ProxyPassReverse    /odb                http://USERS/odb
ProxyPass           /uim                http://USERS/uim
ProxyPassReverse    /uim                http://USERS/uim
ProxyPass           /ucmdb-api          http://USERS/ucmdb-api
ProxyPassReverse    /ucmdb-api          http://USERS/ucmdb-api
ProxyPass           /ucmdb-ui           http://USERS/ucmdb-ui
ProxyPassReverse    /ucmdb-ui           http://USERS/ucmdb-ui
ProxyPass           /tv                 http://USERS/tv
ProxyPassReverse    /tv                 http://USERS/tv
ProxyPass           /tvb                http://USERS/tvb
ProxyPassReverse    /tvb                http://USERS/tvb
```

```
ProxyPass /opr-admin-server/messagebroker/amfsecure http://USERS/opr-admin-
    server/messagebroker/amf
ProxyPassReverse /opr-admin-server/messagebroker/amfsecure http://USERS/opr-
    admin-server/messagebroker/amf
ProxyPass /opr-admin-server/messagebroker/amfpollingsecure http://USERS/opr-admin-
    server/messagebroker/amfpolling
ProxyPassReverse /opr-admin-server/messagebroker/amfpollingsecure
    http://USERS/opr-admin-server/messagebroker/amfpolling
ProxyPass /opr-console/messagebroker/amfsecure http://USERS/opr-
    console/messagebroker/amf
ProxyPassReverse /opr-console/messagebroker/amfsecure http://USERS/opr-
    console/messagebroker/amf
ProxyPass            /opr-admin-server      http://USERS/opr-admin-server
ProxyPassReverse     /opr-admin-server      http://USERS/opr-admin-server
ProxyPass            /opr-console           http://USERS/opr-console
ProxyPassReverse     /opr-console           http://USERS/opr-console
ProxyPass            /opr-gateway           http://USERS/opr-gateway
ProxyPassReverse     /opr-gateway           http://USERS/opr-gateway
ProxyPass            /OVPM                  http://USERS/OVPM
ProxyPassReverse     /OVPM                  http://USERS/OVPM
```

Note: If you are using IDM-SSO, you may need to add the following lines (replace siteminderagent in the syntax below with the name of your IDM-SSO vendor):

```
ProxyPass            /siteminderagent       http://USERS/siteminderagent
ProxyPassReverse     /siteminderagent       http://USERS/siteminderagent
```

4

Using SSL in BSM

This chapter includes:

- Introducing SSL Deployment in BSM on page 46
- Issuing SSL Certificates on page 48
- SSL-Supported Topologies in BSM on page 51
- Configuring BSM to Work with SSL on page 51
- Configuring SSL from Application Users to the Gateway Server on page 53
- Handling Security Certificate Expiration on page 55
- Creating a Keystore on page 55
- Configuring Tomcat to Support HTTPS on page 58
- Configuring JBOSS to work with SSL on page 60
- Configuring the JMX Console to Work with SSL in Other Processes on page 63
- Securing JMX-RMI Channel Used for Internal BSM Communications on page 64
- Using SSL Offloader on page 69

Introducing SSL Deployment in BSM

SSL must be configured to work with BSM servers and clients.

This section includes the following topics:

- "Overview of SSL" on page 46
- "Overview of SSL and BSM" on page 46

Overview of SSL

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.

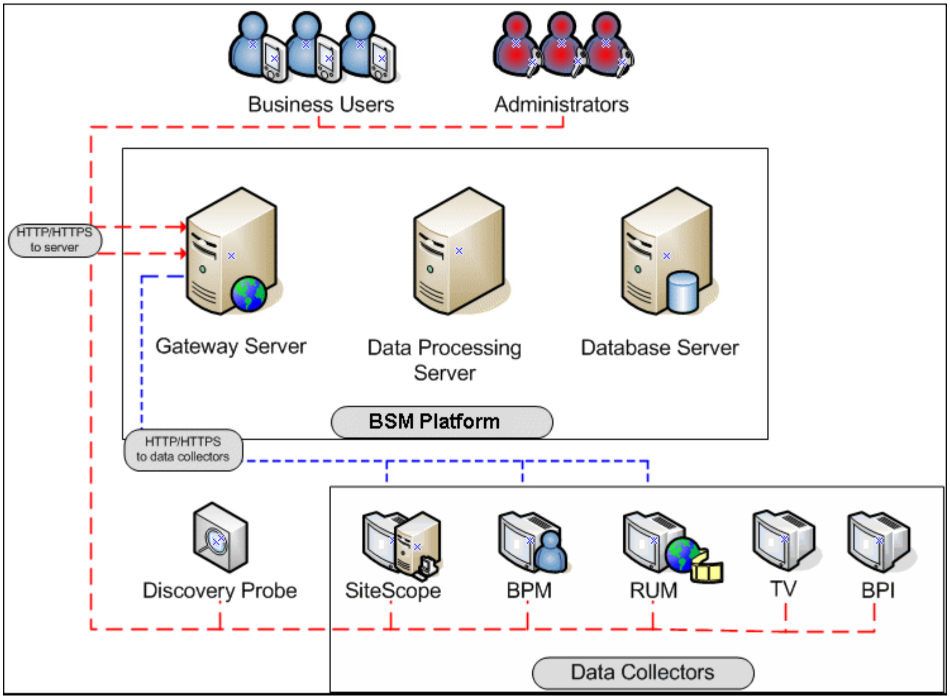
Overview of SSL and BSM

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.

Possible SSL channels in BSM are illustrated in the following diagram:



Communication channels between BSM servers, data collectors, application users, and BSM platform components use various protocols on specific ports. For details, see "Port Usage" in the *Platform Administration* guide, found in the HP BSM Documentation Library.

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. **Note:** When SSL termination is not on a BSM gateway, but on a load balancer/reverse proxy, you must perform an additional procedure on the BSM Gateways. For details, see "Using SSL Offloader" on page 69".

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.

SSL-Supported Topologies in BSM

SSL optional topologies in BSM are divided into two main categories:

- Application users that communicate with BSM Gateway Servers using SSL.
- Data collectors that communicate with BSM Gateway Servers using SSL.

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

Configuring BSM to Work with SSL

To configure a BSM Gateway Server (or a BSM machine, in the case of a single machine installation) to support SSL, 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 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.** See http://httpd.apache.org/docs/2.2/ssl/ for information on enabling SSL for all interaction with the Web server, using mod_ssl. SSL should be enabled for all the directories in use by BSM, as configured in the Apache configuration files (**httpd.conf** and **httpd-ssl.conf**).

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 on page 14 in the Hardening Workflow.

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

To disable weak ciphers on IIS, refer to http://support.microsoft.com/kb/187498/en-us.

To configure the 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.

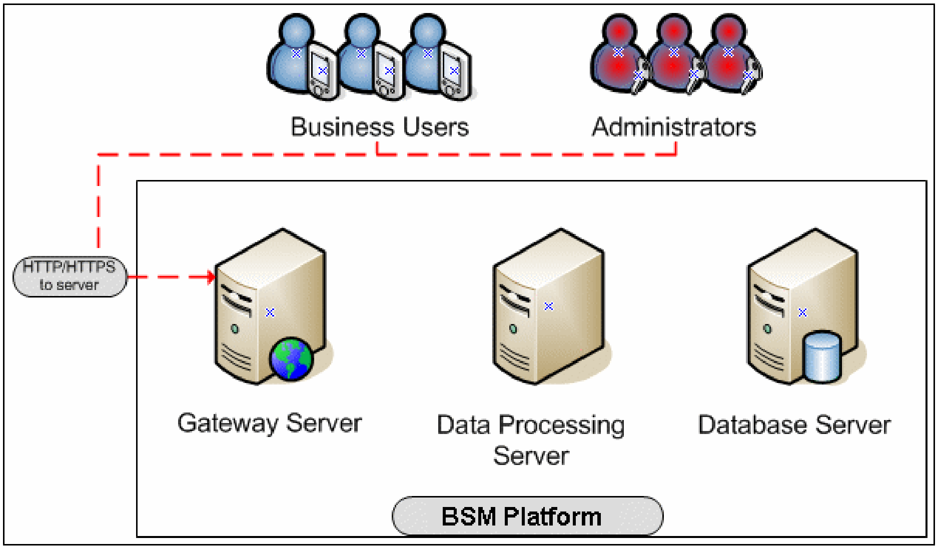
4 **Direct Gateway Server for Data Collectors URL.** Click the **Edit** button and delete the URL in the **value** field.

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 SSL from Application Users to the Gateway Server

The instructions in this section describe how to enable SSL from the application users to the Gateway Server.



SSL Configuration for the Application Users

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 6.0 or 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.

Creating a Keystore

There are several places in BSM where you may need to point to a Java keystore containing a client or server certificate.

Example use cases:

- ➤ A Java keystore with a client certificate is used when configuring mutual SSL.
- ➤ A Java keystore with a server certificate is used when securing the JMX console as well as the JMX-RMI channel.

Option 1: Use a Certificate Authority.

- ➤ Request a client or server certificate from CA in the name of your server.
- ➤ Export private key with a password that is at least six characters long. Example: changeit.
- ➤ 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**

➤ 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_64.cer.

Import CA root certificate into the keystore:
keytool -import -alias ca -file c:\ca_64.cer -keystore C:\certificate.jks -
storepass changeit

List contents of the keystore, for example:

C:\<HPBSM root directory>\JRE\bin>keytool -list -keystore C:\certificate.jks -
storepass changeit

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

ca, Jan 20, 2011, trustedCertEntry,
Certificate fingerprint (MD5):
5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB

bsm, Jan 20, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5):
99:D5:B3:4B:63:08:49:9D:83:4F:CB:5B:C6:FB:6B:AD
```

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

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 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
```

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

Configuring Tomcat to Support HTTPS

This section describes the procedure for configuring Apache Tomcat 5.x to support HTTPS on SiteScope, RUM, and BPM servers. **This procedure should not be perfored on BSM Gateway or Data Processing servers.**

This section includes the following topics:

- "Configuring Tomcat to Support HTTPS" on page 58
- "Configuring Tomcat to Require Client-Side Certificates" on page 59

Configuring Tomcat to Support HTTPS

This section describes how to secure Tomcat using HTTPS. The procedure below is based on Tomcat 5.x.

To configure Tomcat 5.x to support HTTPS:

1. Locate the server.xml file used by your Tomcat. Search for a connector with port 8443 in server.xml file, such as <!--<Connector port="8443" ....scheme="https" ..../>-->, and uncomment it.

2. Add the following attribute to the connector element:

   keystoreFile="myKeyStore"

   where myKeyStore is the JKS or PFX/PKCS#12 file that contains the Web server certificate and a corresponding private key.

3. Change the keystore type and password accordingly in the connector element:

   keystorePass="your password"

   keystoreType="jks" or "pkcs12"

   For example: keystoreFile="c:\myserver.pfx" keystorePass="password for the private key" keystoreType="PKCS12"

4. Restart Tomcat.

5. Test the SSL connection. If it is satisfactory, close the **default port**, leaving only the SSL connection open. To do this:

   Locate the XML Connector with **redirectPort** 8443, and comment it out. For example, change:

   ```
   <Connector className="org.apache.catalina.connector.http.HttpConnector"
   port=<default_port> minProcessors="5" maxProcessors="75"
   enableLookups="true" redirectPort="8443" acceptCount="10" debug="0"
   connectionTimeout="60000"/>
   ```

   to:

   ```
   <!--<Connector
   className="org.apache.catalina.connector.http.HttpConnector"
   port=<default_port> minProcessors="5" maxProcessors="75"
   enableLookups="true" redirectPort="8443" acceptCount="10" debug="0"
   connectionTimeout="60000"/>-->
   ```

   where <**default_port**> has the following values:

   - **For SiteScope:** 8080
   - **For Business Process Monitor:** 2696
   - **For Real User Monitor:** 8180

Configuring Tomcat to Require Client-Side Certificates

Tomcat requires that the keystore containing client certificate be in .jks format. If your keystore is not in .jks format, convert your .pfx certificate to .jks.

Set **keystoreType**="**JKS**" and **clientAuth**="**true**", as in the following example:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="true" sslProtocol="TLS"
keystoreType="JKS"  keystoreFile="C:\Certificates\server_with_changeit_key.jks"
keystorePass="changeit"
truststoreFile="D:\Program Files\HP\BPM\JRE6\lib\security\cacerts"
truststorePass="changeit"/>
```

Set Apache Tomcat to Trust the Client-side Certificate

You may need to set Apache Tomcat to trust the client-side certificate sent by BSM.

Add the following attributes to the Tomcat HTTPS connector element:

- truststoreFile="my_truststore"
- truststorePass="truststore_password" (if different than the keystore password)

so that the element appears as follows:

<Connector className="org.apache.coyote.tomcat5.CoyoteConnector" port="8443" minProcessors="5" maxProcessors="75" enableLookups="true" disableUploadTimeout="true" acceptCount="100" debug="0" scheme="https" secure="true" clientAuth="true" **truststoreFile**="my_truststore" **truststorePass**="truststore_password"/>

The default truststore used by Tomcat is <**Tomcat root directory**>**\java\lib\security\cacerts**. You can set a different truststore, or import the client-side certificate used by BSM into this **cacerts** file.

Configuring JBOSS to work with SSL

This task describes how to configure the application server (JBOSS) to work with SSL.

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

Option 2: Create a java keystore with the server certificate. For details, see "Creating a Keystore" on page 55.

2 Modify the file **server.xml**.

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

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 Reassign the connector port value to 29443. This resolves a conflict with HP Universal CMDB.

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

e Locate the section that begins Connector port="8080":

```
<Connector port="8080" address="$(jboss.bind.address)"
maxthreads="250" maxHttpHeaderSize="8192"
emptySessionPatch="false" protocol="HTTP/1.1"
enableLookup="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"
="UTF-8" />
```

f Change the value of **redirect port** to 29433, and change the value of **address** to "127.0.0.1".

g The section should now look like this:

```
<Connector port="8080" address="127.0.0.1"
maxthreads="250" maxHttpHeaderSize="8192"
emptySessionPatch="false" protocol="HTTP/1.1"
enableLookup="false" redirectPort="29433" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"
URIEncoding="UTF-8" />
```

h In the section with **Connector port**="**8009**" change the value of redirectPort from 8443 to **29443**.

3 Modify the file <**HPBSM root directory**>**\EJBContainer\server\mercury\deploy\jmxconsole.war\WEB-INF\web.xml** to add user-data-constraint with CONFIDENTIAL transport-guarantee into:

```
</web-resource-collection>
        <auth-constraint>
          <role-name>JBossAdmin</role-name>
        </auth-constraint>
         <user-data-constraint>
         <transport-guarantee>CONFIDENTIAL</transport-guarantee>
           </user-data-constraint>

      </security-constraint>
```

4 Back up the file **C:\HPBSM\AppServer\webapps\myStatus.war\myStatus.html**

5 Modify **myStatus.html** to use https and port 29433 for HacInfo as follows:

```
        if (_mercuryAsStarted) {
              getStatus("HacInfo", "https://" + getHostName() + ":29443/jmx-
console/HtmlAdaptor?action=invokeOpByName&name=Topaz:service=hac-
manager&methodName=listMyStatus", "hacinternal");
              checkHacStatus();
```

6 Restart the BSM server.

Configuring the JMX Console to Work with SSL in Other Processes

This task describes how to configure the JMX console to work with SSL in other BSM processes.

To configure the JMX console to work with SSL 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.MX4JHtmlAdaptor" 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.

Parameter Name	Required Value
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 Keystore" on page 55.

Securing JMX-RMI Channel Used for Internal BSM Communications

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

- Configuring user name/password authentication and
- Configuring SSL

Notes:

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

For 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.

For 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 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:

- ➤ Run **services.msc.**
- ➤ Right click **HP Business Service Management.**
- ➤ 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, navigate to **Properties** > **Security** > **Advanced** > **Owner.** Click **Other Users or Groups**, type "<**domain\admin user name**>" or "**SYSTEM**", and click **Check Names**. Verify that you see that the value of **Current Owner** is updated.

b Change the permissions of **jmxremote.password** file to be **Read Only By The Owner**.

For administrator user: cmd: cacls jmxremote.password /P <domain\user name>:R)

For SYSTEM user: cmd: cacls jmxremote.password /P SYSTEM:R)

In Linux:

a **chmod 600 jmxremote.password**

b Try to open the password file. You should now be denied access to it.

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

1 Create Java keystore (JKS file). For details, see "Creating a Keystore" on page 55.

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:/Certificates/Server_Keystore
javax.net.ssl.keyStorePassword=changeit
```

---

3 Protect the SSL parameters file.

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 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:

- Run **services.msc.**
- Right click **HP Business Service Management.**
- In the **log on** tab, select **This account** and enter the administrator credentials.

To change the owner of the files, navigate to **Properties** > **Security** > **Advanced** > **Owner.** Click **Other Users or Groups**, type "<**domain****admin user name**>" or "**SYSTEM**", and click **Check Names**. Verify that you see that the value of **Current Owner** is updated.

b Change the permissions of **jmx-rmi.properties** file to be **Read Only By The Owner.**

For administrator user: cmd: cacls jmx-rmi.properties /P <domain\user name>:R)

For SYSTEM user: cmd: cacls jmx-rmi.properties /P SYSTEM:R)

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 set the following:

```
-Dcom.sun.management.jmxremote.ssl=true
```

```
-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 set the following:

```
-Dcom.sun.management.jmxremote.ssl=true
```

```
-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 SecureServer -keystore Server_Keystore -rfc -file
Server.cer
```

where **Server_Keystore** is the keystore file, and **Server.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
SecureServer -file Server.cer -keystore <HPBSM installation
directory>\JRE64\lib\security\cacerts
```

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

where **Server.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**.

Using SSL Offloader

If your environment contains an SSL Offloader such as reverse proxy or load balancer where SSL is terminated and traffic is forwarded unencrypted to the BSM webserver, you may see errors when loading pages with Adobe Flex components (for example, Application Status Report in End User Management or 360 View page in MyBSM).

The error in topaz_all.ejb.log would look like this:

flex.messaging.security.SecurityException: Secure endpoint '/messagebroker/amfsecure' must be contacted via a secure protocol

In this case, you must do the following:

1. Replace the file: **<HPBSM root directory>\AppServer\webapps\site.war\WEBINF\flex\services-config.xml** with the following file found in the same directory: **services-config_for_reverse_proxy_env.xml**.
2. Use this new **services-config.xml** to replace the **services-config.xml** files found in each of the following directories on the BSM Gateway Server:
   <HPBSM root directory>\AppServer\webapps\tvb.war\WEB-INF\flex
   <HPBSM root directory>\AppServer\webapps\bpi.war\WEB-INF\flex
3. Replace the file: **<HPBSM root directory>\AppServer\webapps\opr-admin-server.war\WEBINF\flex\services-config.xml** with the following file found in the same directory: **services-config_for_reverse_proxy_env.xml**
4. Replace the file: **<HPBSM root directory>\AppServer\webapps\OVPM.war\WEBINF\flex\services-config.xml** with the following file found in the same directory: **services-config_for_reverse_proxy_env.xml**
5. Replace the file: **<HPBSM root directory>\AppServer\webapps\opr-console.war\WEBINF\flex\services-config.xml** with the following file found in the same directory: **services-config_for_reverse_proxy_env.xml**
6. After replacing **services-config.xml** in all locations, restart BSM.

5

Using SSL with TransactionVision

This chapter describes how to configure a BSM platform that includes TransactionVision components to support communication using the Secure Sockets Layer (SSL) channel.

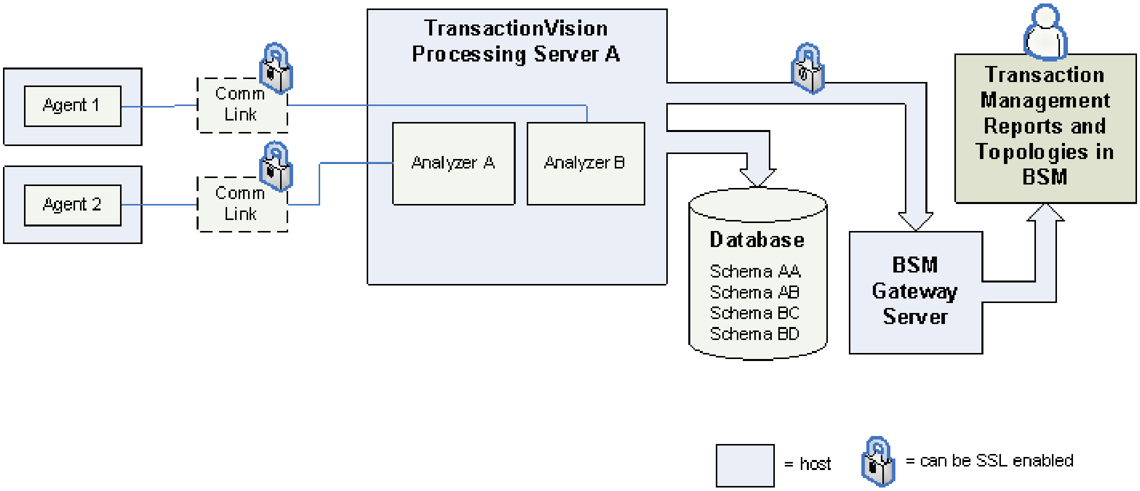
This chapter includes:

- About SSL and TransactionVision on page 72
- Configuring SSL Between a TransactionVision Processing Server and the BSM Gateway Server on page 73

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 45.

About SSL and TransactionVision

TransactionVision Processing Servers communicate both with the BSM Gateway Server and with the agents collecting events. Each of these data pathways are eligible for SSL. The following diagram shows the SSL eligible pathways in an example deployment environment:



Enabling SSL on the communication link data pathway (left side of the diagram) is dependent on the type of agent and message middleware provider. For more information about enabling SSL on this data pathway, see "Securing with SSL" in the *HP TransactionVision Deployment Guide* PDF.

Enabling SSL on the TransactionVision Processing Server to the Gateway Server pathway (right side of the diagram) is described in the sections that follow.

Configuring SSL Between a TransactionVision Processing Server and the BSM Gateway Server

To enable SSL between a Processing Server and BSM Gateway Server pathway, perform the tasks that follow:

1. "Import the Certificate from an SSL Enabled BSM Gateway Server to the TransactionVision Processing Servers" on page 73
2. "Generate a Certificate" on page 74
3. "Import the Certificate to the BSM Truststore" on page 75
4. "Enable SSL on the TransactionVision Processing Servers" on page 75
5. "Set the BSM Communication Protocol and Port" on page 77
6. "Synchronize the Processing Server" on page 78

Import the Certificate from an SSL Enabled BSM Gateway Server to the TransactionVision Processing Servers

The BSM Gateway Server host must be enabled for SSL. A certificate obtained from the BSM Gateway Server needs to be imported into the cacerts file on each Processing Server host.

The TransactionVision Processing Server cacerts file is located in the following location: **<TVISION_HOME>/jre/lib/security/cacerts**.

Following import of the certificate, the Processing Server components must be restarted.

One way to restart the Processing Server components is to use the nanny utility on the host on which the Processing Server is running:

➤ For Windows run:

```
<TVISION_HOME>\bin\nanny.bat stopAllServices
<TVISION_HOME>\bin\nanny.bat startAllServices
```

➤ For Linux run:

```
<TVISION_HOME>/bin/nanny.sh stopAllServices
<TVISION_HOME>/bin/nanny.sh startAllServices
```

For more information about restarting these components, see *Using Transaction Management*.

Generate a Certificate

To generate a certificate in the default keystore:

1 On the Processing Server host, generate a certificate with the following command:

```
keytool -genkey -keystore <TVISION_HOME>\jre\lib\security\cacerts -alias
tvserverkey -keyalg RSA
```

Replace <TVISION_HOME> with the absolute path of the TransactionVision Processing Server installation directory. The default installation path on Linux is **/opt/HP/TransactionVision**; on Windows it is **C:\Program Files\HP\TransactionVision**.

TransactionVision requires a JKS keystore type. To import certificates from a PKCS12 keystore into the default TransactionVision keystore, use the following command:

```
keytool -importkeystore -srckeystore C:\mykeystore.p12 -srcstoretype pkcs12
-destkeystore <TVISION_HOME>\jre\lib\security\cacerts
```

The keytool command prompts you for information regarding the creation of the key. Note the following when using this command:

- If you specify a password other than the default "changeit", be sure to record it as it will be needed to access this key in a later task.
- If you plan to use the keystore with SonicMQ, specify a 1 or 2 character country code. Longer country codes are not supported.
- When keytool prompts for "your first and last name", the fully-qualified Processing Server hostname should be used. For example:

```
What is your first and last name?
[Unknown]: tvhost.my.domain.com
```

2 Export the certificate's public key with the following command:

```
keytool -export -alias tvserverkey -file serverkey.cer -keystore
<TVISION_HOME>\jre\lib\security\cacerts
```

This exports the key to a file called **serverkey.cer**.

Import the Certificate to the BSM Truststore

The certificate generated in Generate a Certificate, must be incorporated into the BSM truststore.

This task requires the BSM Gateway Server to be restarted.

Enable SSL on the TransactionVision Processing Servers

If the deployment environment has multiple Processing Servers, each one must be separately enabled for SSL.

To enable SSL on a Processing Server:

1 Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers** > <processing server>.

2 Select **Configuration** > **Advanced,** then set the **Enable SSL** check box.

Enter the Keystore Password and Location, and the Key password. These values were provided as result of Generate a Certificate.

Note: The keystore location is relative to <TVISION_HOME> unless an absolute path is specified. The default location is <TVISION_HOME>/jre/lib/security/cacerts. Forward slashes can be used regardless of the Processing Server’s host operating system.

---

3 (optional) By default, the SSL port on the Processing Server is used for SSL communication. If you have a port conflict, you can modify the SSL port for the Processing Server. Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers** > <processing server> > **Configuration** > **General** > **SSL Port** field.

4 Click **Apply**.

When a Processing Server becomes enabled for SSL, any Analyzer, Job Manager or Query Engine running on that Processing Server is also set to run in SSL. By default, the SSL dedicated ports are used for each of them. If you have a port conflict, you can modify the SSL ports.

To modify the SSL port for the Job Manager

1 Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers.**

2 On the **Job Manager** tab, locate and select the processing server for which you want to enable the SSL setting.

3 Click the **Edit** button to modify the SSL port as well as any other Job Manager properties.

To modify the SSL port for the Query Engine

1 Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers.**

2 On the **Query Engine** tab, locate and select the processing server for which you want to enable the SSL setting.

3 Click the **Edit** button to modify the SSL port as well as any other Query Engine properties.

To modify the SSL port for the Analyzer

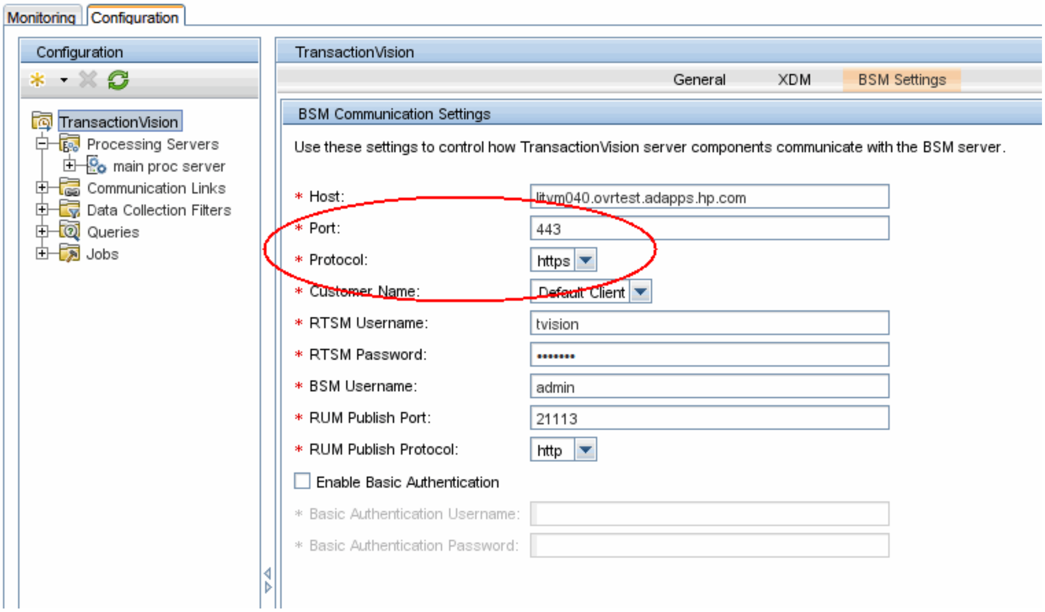
1 Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers** > <processing server> > <analyzer>.

2 On the **Configuration** > **General** tab, modify the **SSL Port** setting.

Set the BSM Communication Protocol and Port

By default, the protocol for the Processing Server to communicate with the BSM Gateway Server is http. To enable SSL, the protocol must be https and the SSL port of 443 must be specified.

To specify these settings, choose **Admin** > **Transaction Management** > **Configuration** > **TransactionVision** (root level node) > **Configuration tab** > **BSM Settings**, and set the **Protocol** to https and **Port** to 443.



BSM Communication Settings

Use these settings to control how TransactionVision server components communicate with the BSM server.

* Host:	litvm040.ovrtest.adapps.hp.com
* Port:	443
* Protocol:	https
* Customer Name:	Default Client
* RTSM Username:	tvision
* RTSM Password:	•••••••
* BSM Username:	admin
* RUM Publish Port:	21113
* RUM Publish Protocol:	http

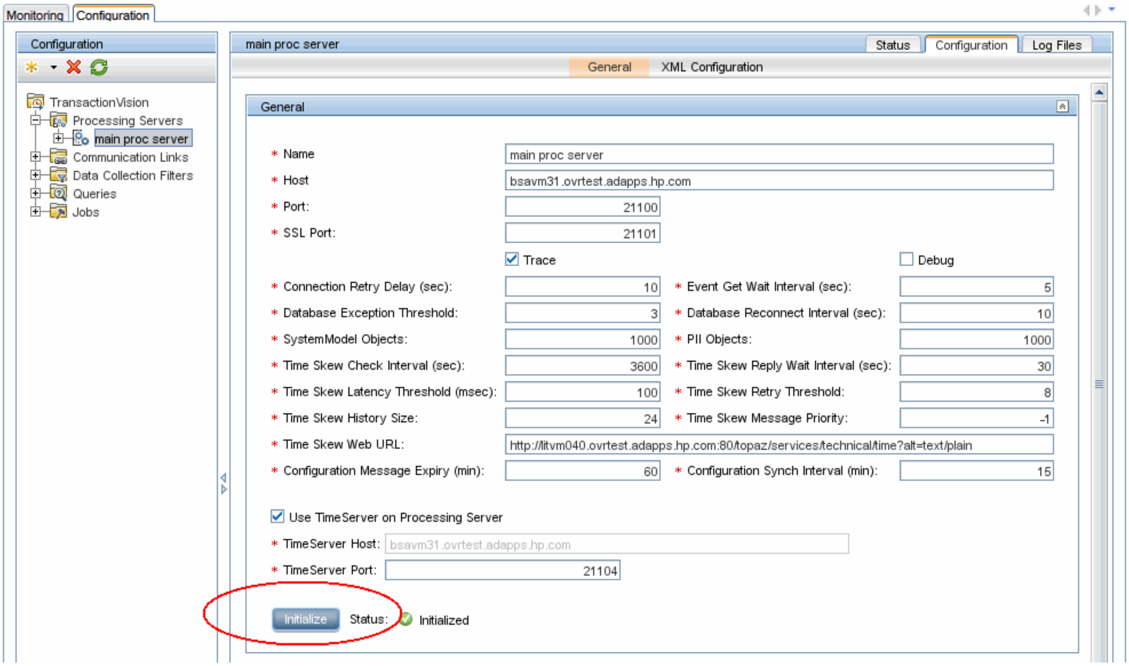
□ Enable Basic Authentication

* Basic Authentication Username:	
* Basic Authentication Password:	

Synchronize the Processing Server

To synchronize the Processing Server configuration settings with the changes to the BSM Settings page:

1. Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers** > <processing server>.
2. On the **Configuration** tab, click the **Initialize** button.



* Name: main proc server

* Host: bsavm31.ovrtest.adapps.hp.com

* Port: 21100

* SSL Port: 21101

☑ Trace

□ Debug

* Connection Retry Delay (sec):	10	* Event Get Wait Interval (sec):	5
* Database Exception Threshold:	3	* Database Reconnect Interval (sec):	10
* SystemModel Objects:	1000	* PII Objects:	1000
* Time Skew Check Interval (sec):	3600	* Time Skew Reply Wait Interval (sec):	30
* Time Skew Latency Threshold (msec):	100	* Time Skew Retry Threshold:	8
* Time Skew History Size:	24	* Time Skew Message Priority:	-1
* Time Skew Web URL:	http://litvm040.ovrtest.adapps.hp.com:80/topaz/services/technical/time?alt=text/plain		
* Configuration Message Expiry (min):	60	* Configuration Synch Interval (min):	15

☑ Use TimeServer on Processing Server

* TimeServer Host: bsavm31.ovrtest.adapps.hp.com

* TimeServer Port: 21104

Status: ✓ Initialized

6

Using Basic Authentication in BSM

This chapter includes:

- Introducing Basic Authentication Deployment in BSM on page 80
- Configuring Basic Authentication Between the Gateway Server and Application Users on page 83
- Configuring Basic Authentication Between the Gateway Server and the Data Collectors on page 86
- Auto Upgrading Data Collectors Remotely when Using Basic Authentication on page 90

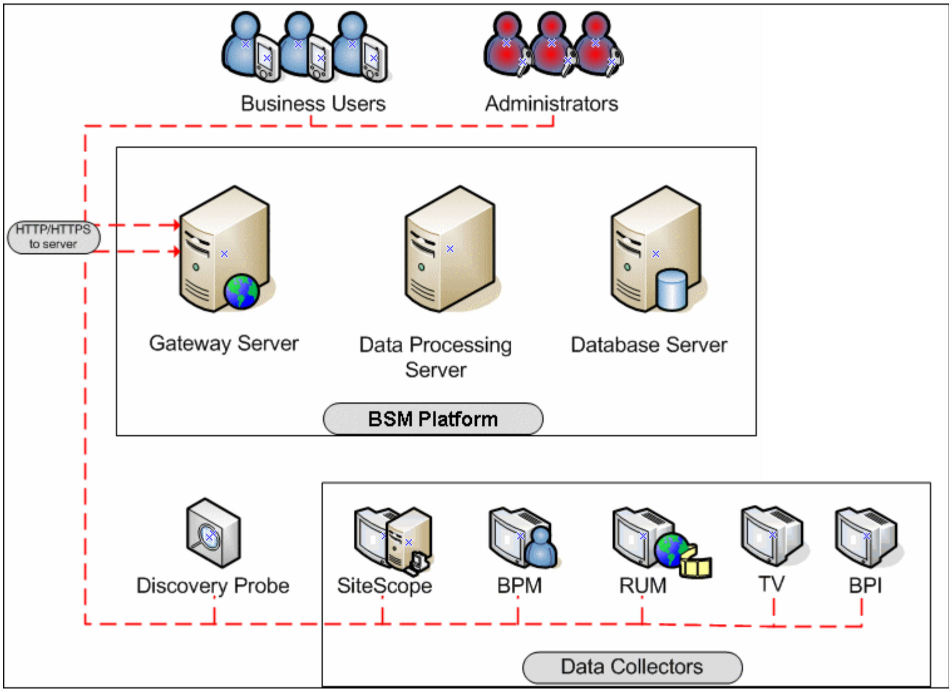
Introducing Basic Authentication Deployment in BSM

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 45.

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

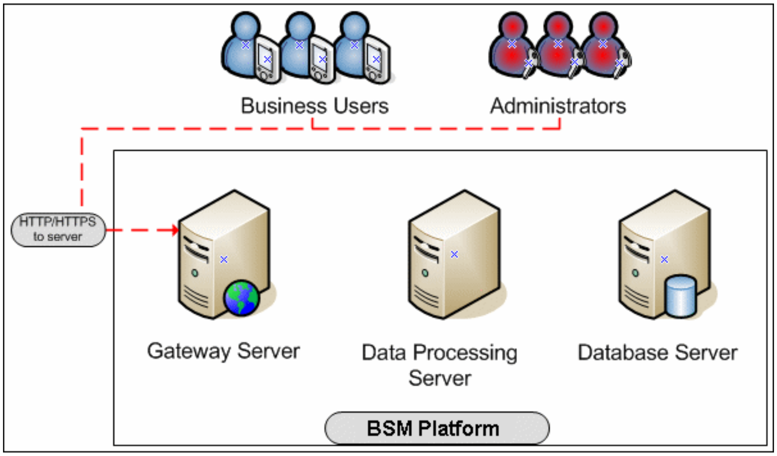
Before proceeding with the configuration steps, ensure that:

- 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.



This section includes the following topics:

- "Basic Authentication Configuration for the Gateway Server" on page 84
- "Basic Authentication Configuration for the Application Users" on page 85

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 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 webserver.

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.

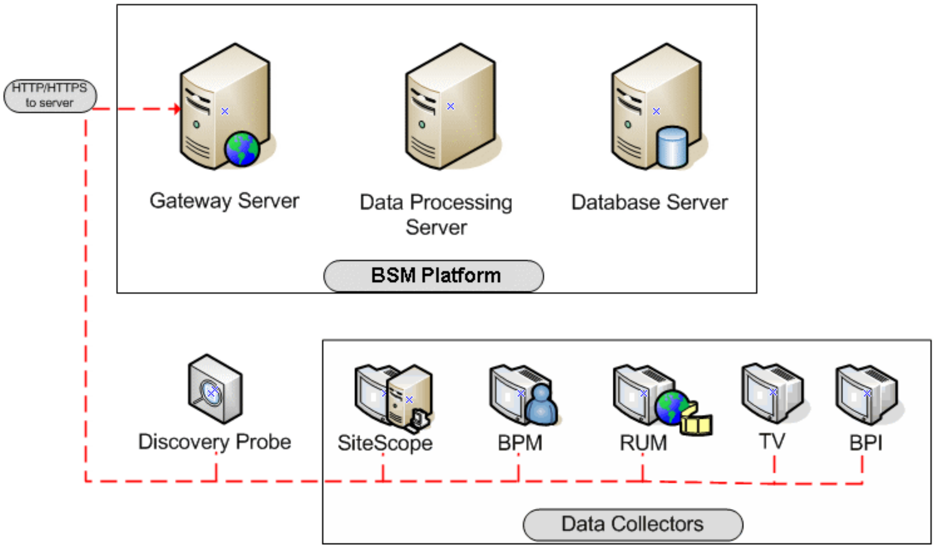
Basic Authentication Configuration for the Application Users

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 the 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.



This section describes the following topics:

- "Basic Authentication Configuration for the Gateway Server" on page 87
- "Basic Authentication Configuration for the Data Collectors" on page 88

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.

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 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 the Data Collectors

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

- "Business Process Monitor" on page 88
- "SiteScope" on page 89
- "Real User Monitor" on page 89

Note: The Staging Data Replicator (used during the staging part of the upgrade to repeat samples from an HP Business Availability Center 7.x machine to an HP Business Availability Center 8.0 machine) 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.

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**.

Auto Upgrading Data Collectors Remotely when Using Basic Authentication

You can perform a remote auto update for the Business Process Monitor and SiteScope data collectors by supplying parameters required to download the update from the Web server on which it is located. If the Web server from which you are downloading the update is using basic authentication, you must perform the following procedure in BSM in order to enable the remote auto upgrade.

To auto upgrade data collectors remotely when using basic authentication:

1. Select **Admin** > **Platform** > **Data Collection** > **Data Collector Maintenance**. The **Data Collector Maintenance** page opens.
2. Click the **SiteScope** or **Business Process Monitor** tab, depending on the type of data collector you want to upgrade.
3. Select the check box for the data collector instance you want to upgrade.

   To make your selections, you can also use the buttons at the bottom of the page for, **Select All**, **Clear All**, and **Invert Selection.**

4 Click **Upgrade** at the bottom of the page. The Upgrade dialog box opens.

5 Select **Use Basic Authentication** and enter the following authentication parameter values:

- **User Name.** The user name to be used to log in to the Gateway Server.
- **Password.** The user password to be used to log in to the Gateway Server.
- **Domain.** The domain name to be used to log in to the Gateway Server.

6 Click **Start Upgrade**.

7

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.

Issue	Resolution
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** and 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** and settingName=**lw.sso.configuration.xml** newValue=<**NEW_VALUE_STRING**> **2** Reload configuration: go to service = SSO invoke Start()

Index

A

Apache Tomcat
- configuring to support https 58
- configuring to trust client-side certificates 58, 59

application users
- configuring basic authentication support for 83
- configuring SSL support for 53
- support 33

B

basic authentication
- configuring between Gateway Server and Data Collectors 86
- configuring for Business Process Monitor 88
- configuring for data collectors 88
- configuring for SiteScope 89
- configuring support for application users 83
- configuring support for Gateway Server 83
- deployment 80
- remote upgrade 90
- using with BSM 79

basic authentication support
- configuring for Real User Monitor 89

BBC Port 383 36

Business Process Monitor
- configuring basic authentication support for 88

C

client-side certificates
- configuring Apache Tomcat to trust 58, 59

Configuring JMX-RMI with Basic Authentication 64

D

data collectors
- configuring basic authentication 86, 88
- support 31

deploying in a secure architecture 20

distributed configuration
- reverse proxy 41

G

Gateway Server
- configuring basic authentication 86
- configuring basic authentication support for 83
- configuring SSL for TransactiionVision Processing Server 73
- configuring SSL support for 53

generic mode
- reverse proxy 29

H

hardening
- BSM platform 19
- introduction 19

HP Software Support Web site 11

HP Software Web site 11

https
  configuring Apache Tomcat to support 58

J

JMX console
  configuring for SSL in other processes 63
JMX-RMI, configuring with Basic Authentication 64

K

Knowledge Base 11

M

mode support
  reverse proxy 28

O

online resources 11

R

Real User Monitor
  configuring basic authentication support for 89
remote upgrade
  when using basic authentication 90
reverse proxy
  and BSM 27
  BSM specific congfiguration 38
  configuration 29
  distributed configuration example 41
  generic mode 29
  limitations 41
  mode support 28
  overview 26
  security aspects 26
  specific mode 28
  using 29
  using in BSM 25

S

secure architecture 20
Securing JMX-RMI channel 64
security
  for BSM platform 19
SiteScope
  configuring basic authentication support for 89
specific mode
  reverse proxy 28
SSL
  and BSM 46
  and TransactionVision 72
  configuring between TransactionVision processing server and Gateway Server 73
  configuring BSM to work with 51
  configuring JMX console in other processes to work with 63
  configuring support for application users 53
  configuring support for Gateway Server 53
  deployment 46
  issuing certificates 48
  overview 46
  supported topologies 51
  using with BSM 45
  using with TransactionVision 71

T

Tomcat
  configuring to support https 58
  configuring to trust client-side certificates 58, 59
topologies
  SSL-supported 51
TransactionVision
  and SLL 72
  using SSL with 71
TransactionVision processing server
  configuring SSL for Gateway Server 73
Troubleshooting and Knowledge Base 11