HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.12

Hardening Guide

Document Release Date: November 2011

Software Release Date: November 2011

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

Note: Only the Web Browser Security in BSM chapter of this guide is relevant to HP Software-as-a-Service (SaaS) customers.

This chapter includes:

How This Guide Is Organized

The guide contains the following chapters:

Chapter 1 Introduction to Hardening the BSM Platform

Describes the concept of a secure BSM platform and discusses the planning and architecture required to implement a secure platform.

Chapter 2 Web Browser Security in BSM

Describes how to configure a Web browser in order to secure your browser access to BSM.

Chapter 3 Using a Reverse Proxy in BSM

Describes how to use a reverse proxy with BSM in order to help secure BSM architecture.

Chapter 4 Using SSL in BSM

Describes how to configure the BSM platform to support Secure Sockets Layer (SSL) communication.

Chapter 5 Using SSL with SiteScope

Describes how to configure HP SiteScope to support Secure Sockets Layer (SSL) communication.

Chapter 6 Using SSL with the Business Process Monitor Agent

Describes how to configure Business Process Monitor to support Secure Sockets Layer (SSL) communication.

Chapter 7 Using SSL with Real User Monitor

Describes how to configure Real User Monitor to support Secure Sockets Layer (SSL) communication.

Chapter 8 Using SSL with Data Flow Probe

Describes how to configure Data Flow Probe to support Secure Sockets Layer (SSL) communication.

Chapter 9 Using SSL with TransactionVision

Describes how to configure TransactionVision to support Secure Sockets Layer (SSL) communication.

Chapter 10 Using Basic Authentication in BSM

Describes how to configure the BSM platform to support communication using basic authentication.

Chapter 11 Troubleshooting and Limitations

Describes common problems that you may encounter when securing the BSM platform.

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

Introduction to Hardening the BSM Platform

This chapter includes:

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.

Before You Start

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 all the hardening guidelines.

A good understanding of the BSM technical framework and BSM security capabilities will facilitate designing a solid plan for implementing a secure BSM platform.

Note: The hardening information provided in this section is not intended as a guide to making a security risk assessment for your computerized systems.

You should also note the following points when using the hardening guidelines:

- Verify that the BSM platform is fully functioning before starting the hardening procedures.
- Follow the hardening procedure steps chronologically in each chapter. For example, if you decide to configure the BSM servers to support SSL, read "Using SSL in BSM" on page 53 and then follow all the instructions chronologically.
- The BSM components do not support basic authentication with blank passwords. Do not use a blank password when setting basic authentication connection parameters.

- The hardening procedures are based on the assumption that you are implementing only the instructions provided in these chapters, 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 following chapters will be performed on machines dedicated to the BSM platform. Using the machines for other purposes in addition to BSM may yield problematic results.

Tip: Print the hardening procedures and check them off as you implement them.

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 33.

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.

Using the Hardening Guidelines

The chapters in this guide discuss the following hardening topics:

- **Web browser security in BSM.**

  This chapter contains information on configuring your Web browser to support secure Web browsing. For details, see "Web Browser Security in BSM" on page 25.

- **Using a reverse proxy in BSM.**

  This chapter contains information on using a reverse proxy with BSM in order to help secure BSM architecture. For details, see "Using a Reverse Proxy in BSM" on page 33.

- **Configuring the BSM platform to use SSL communication.**

  These chapters contain information on configuring each BSM component to support Secure Sockets Layer (SSL) communication. For details, see "Using SSL in BSM" on page 53.

- **Configuring the BSM platform to use basic authentication.**

  This chapter contains information on configuring each BSM component to support communication using the basic authentication protocol. For details, see "Using Basic Authentication in BSM" on page 111.

  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.

- **Configuring your web server to work with BSM.**

  This chapter contains information on configuring the Web server on a BSM server machine to support required security settings. Additional instructions for configuring these settings can be found in the appropriate Web server documentation, available at the following sites:

  - **For IIS 5.0/6.0.** The Microsoft Web site (http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/848968f3-baa0-46f9-b1e6-ef81dd09b015.mspx?mfr=true).

  - **For Apache.** The Apache Jakarta Web site (http://httpd.apache.org).

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

- **Recommendations.** It is recommended to:
  - 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.

- **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, found in the HP BSM Documentation Library.

  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.

2

Web Browser Security in BSM

This chapter includes:

- BSM and Web Browsers on page 25
- Configuring the Internet Explorer Web Browser on page 26
- Configuring the FireFox Web Browser on page 28

BSM and Web Browsers

This section includes the following topics:

- "Web Browser Configuration Overview" on page 25
- "Notes and Limitations" on page 26

Web Browser Configuration Overview

A Web browser on a client machine connecting to BSM must enable the following:

- **JavaScript execution.** Enables you to use BSM interactively in a Web browser.
- **Java plug-in for applet execution.** This plug-in is automatically installed when an applet is accessed for the first time on your browser.
- **Signed and unsigned applets.** Java plug-in gives different permissions to applets based on whether they are signed or unsigned. For this reason, both signed applets and unsigned applets must be enabled.

- **Session cookies.** These are cookies stored in your computer's memory while you are using the Web browser. When you exit the browser, these cookies are removed from memory.
- **First-party cookies.** BSM creates these cookies and stores them on your computer's hard disk.

Notes and Limitations

If the client machine's operating system is Windows XP, Service Pack 2, you must disable the firewall in the Windows Security Center before configuring the Web browser. For details, see http://support.microsoft.com/kb/283673.

Configuring the Internet Explorer Web Browser

You must configure JavaScript, Java applets, and cookies in the Internet Explorer Web browser to connect to BSM.

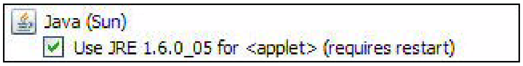
This section includes the following topics:

- "To enable JavaScript and Java applets:" on page 26
- "To accept cookies:" on page 27

To enable JavaScript and Java applets:

1 In the Internet Explorer Web browser, select **Tools** > **Internet Options**, and click the **Advanced** tab.

2 Scroll down to the **Java (Sun)** section. Select **Use JRE** (Java Runtime Environment). Any JRE version v1.5.x or v1.6x is acceptable.



Java (Sun)

☑ Use JRE 1.6.0_05 for <applet> (requires restart)

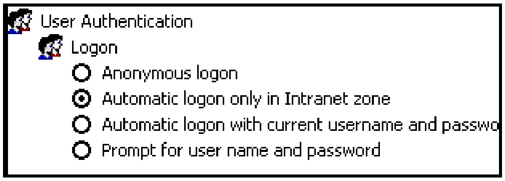
3 Click the **Security** tab and then click the **Custom Level** button. The Security Settings dialog box opens.

4 Scroll down to the **Scripting** section.

- In **Active scripting**, select **Enable** or **Prompt**.
- In **Allow programmatic clipboard access**, select **Enable**.

- ➤ In **Scripting of Java applets**, select **Enable** or **Prompt**.

5 Scroll down to the **User Authentication** section. All of the options permit connecting to BSM. Select the option most suitable for your site.



User Authentication
Logon
○ Anonymous logon
◉ Automatic logon only in Intranet zone
○ Automatic logon with current username and passwo
○ Prompt for user name and password

6 Click **OK** to save your settings and close the Security Settings dialog box.

7 Click **OK** to save your settings and close the Internet Options dialog box.

Note: If you selected **Use JRE** in step 2, you must restart your browser for the changes to take effect. If **Use JRE** was already selected, you do not need to restart.

To accept cookies:

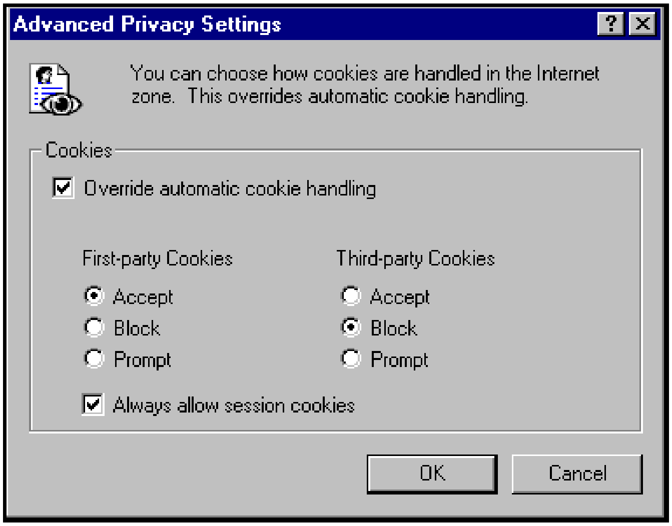
1 Open the Internet Explorer Web browser, select **Tools** > **Internet Options** and select the **Privacy** tab.

2 In the Settings pane, you can configure cookies in one of two ways:

- ➤ select **Advanced** and configure manually.
- ➤ raise or lower the button on the vertical bar to select **Low** or **Medium**.

3 If you select **Advanced**, the Advanced Privacy Settings dialog box opens.

- ➤ Select **Override automatic cookie handling** and **Always allow session cookies**.
- ➤ In First-party Cookies, select **Accept**. In Third-party Cookies, select **Accept** or **Block,** based upon your site's security needs.



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	○ Accept
○ Block	● Block
○ Prompt	○ Prompt

☑ Always allow session cookies

- ➤ Click **OK** to save your settings. Proceed to step 5, below.

4 If you select **Low** or **Medium**, click **Apply** to save your settings.

5 Click **OK** again to close the Internet Options dialog box.

Configuring the FireFox Web Browser

You must configure the FireFox Web browser to connect to BSM.

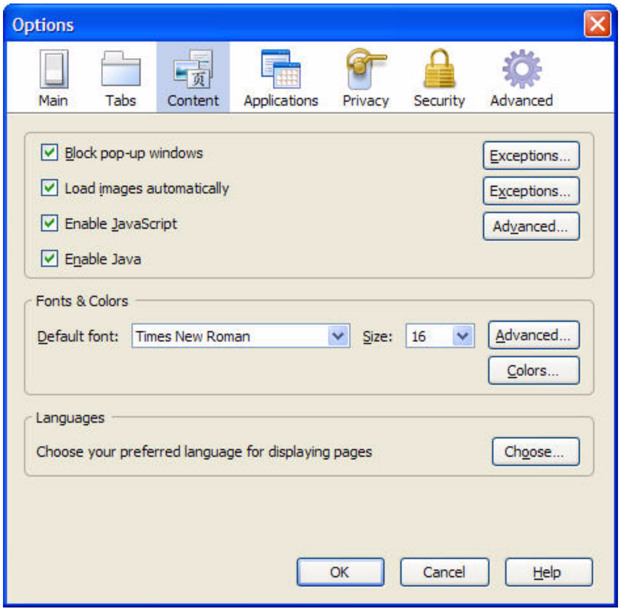
This section includes the following topics:

- ➤ "To enable JavaScript and Java applets:" on page 29
- ➤ "To accept cookies:" on page 30

To enable JavaScript and Java applets:

1 In the FireFox Web browser, select **Tools** > **Options** and click the **Content** button.

2 Select **Enable JavaScript** and **Enable Java**.



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

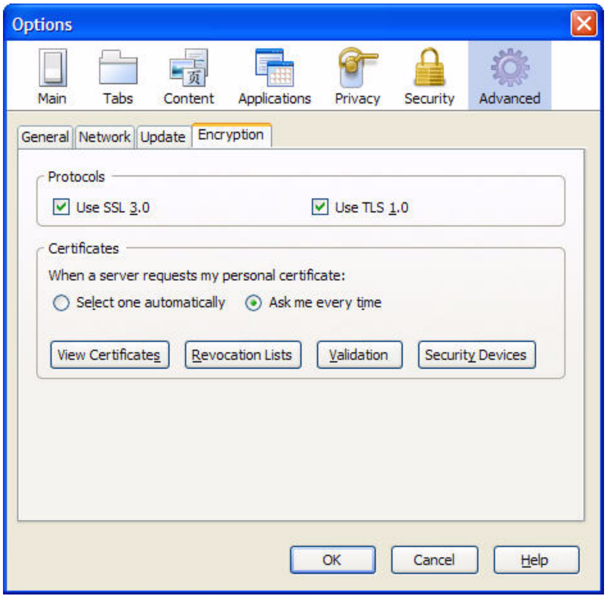
Default font: Times New Roman

Size: 16

Choose your preferred language for displaying pages

3 Click the **Advanced** button. Select the **Encryption** tab.

4 Select **Use SSL 3.0** and **Use TLS 1.0**.



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

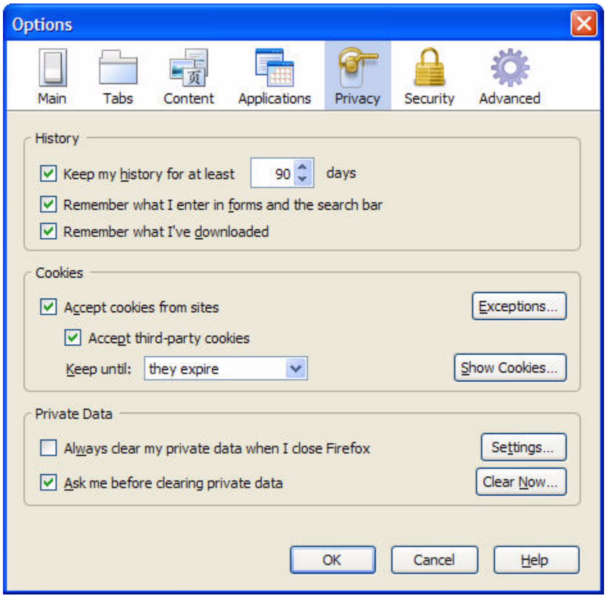
5 Click **OK** to save your settings and close the Options dialog box.

To accept cookies:

1 Open the FireFox Web browser, select **Tools** > **Options**.

2 Click the **Privacy** button.

3 Select the **Accept cookies from sites** and **Accept third-party cookies** check boxes.



History

☑ Keep my history for at least 90 days

☑ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

☑ Accept third-party cookies

Keep until: they expire

Private Data

□ Always clear my private data when I close Firefox

☑ Ask me before clearing private data

3

Using a Reverse Proxy in BSM

This chapter includes:

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 37.

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 36
- "Generic Mode" on page 37

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:

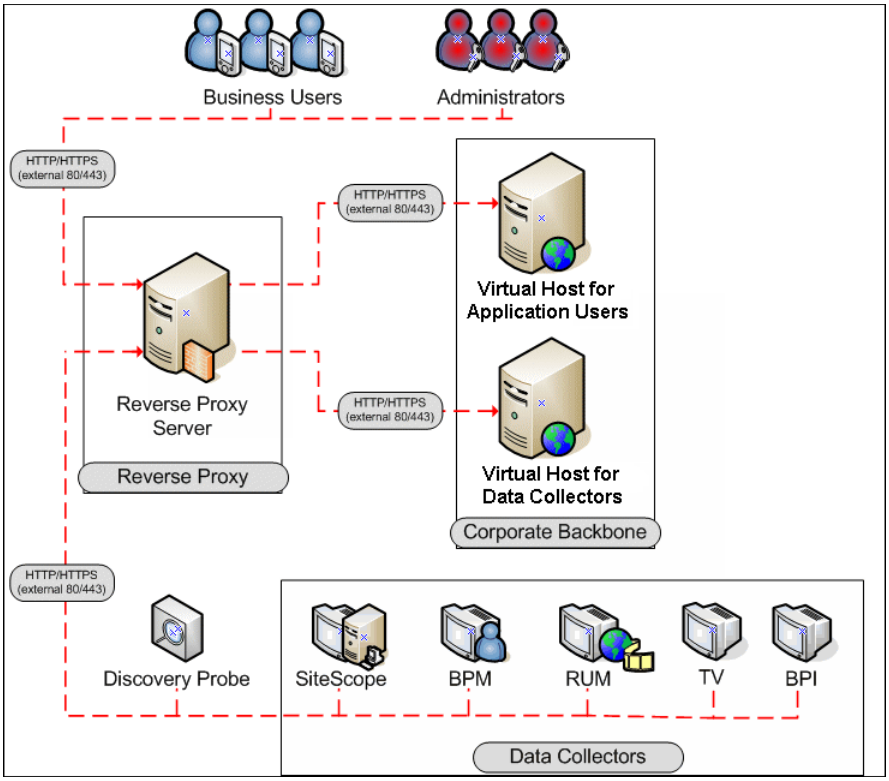
- "Reverse Proxy Configuration" on page 37
- "Configuring BBC Port 383 Connection on Reverse Proxy" on page 44
- "HP BSM Specific Configuration" on page 46
- "Limitations" on page 49
- "Apache 2.x – Distributed Configuration Example" on page 49

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 49.
- 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 49.

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

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

This section includes the following topics:

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.

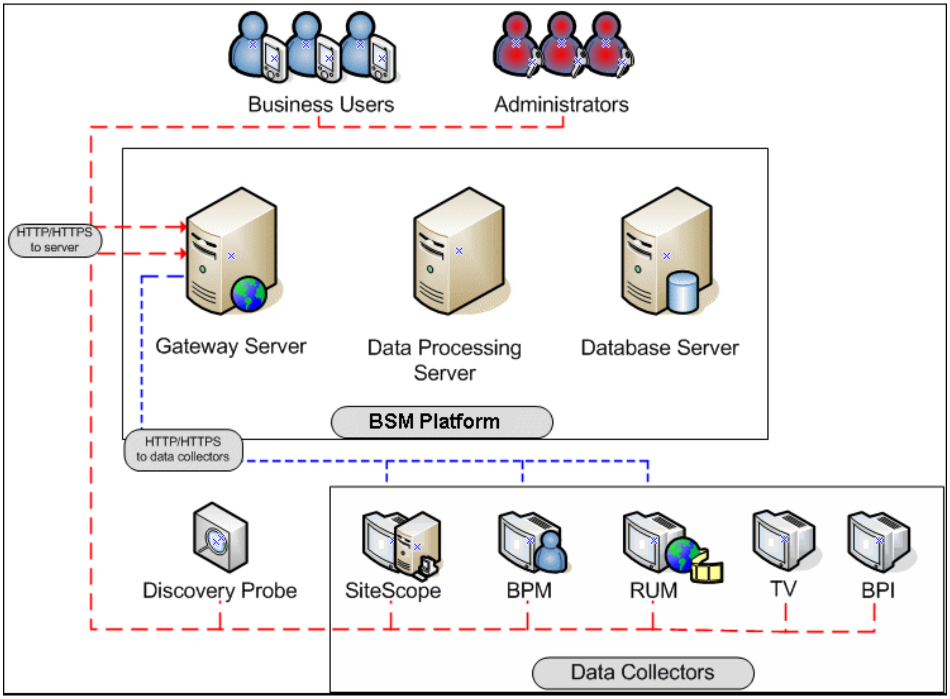
The BSM platform fully supports the SSL 3.0 protocol. The SSL channel is configured on the BSM servers/clients as required.

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.

Overview of Configuring SSL in BSM

The section "SSL-Supported Topologies in BSM" on page 62 discusses the various BSM-SSL topologies that are supported and provides links to each configuration step that is required.

Before proceeding with the configuration steps, ensure that:

- You read this chapter in its entirety before you begin performing the configuration.
- The BSM platform is operating as it is supposed to without an SSL channel.
- You define your secure communication requirements (use an SSL channel only where necessary).
- You consult the section "SSL-Supported Topologies in BSM" on page 62 to determine which topology is most suitable for the specific SSL architecture you are using.

Note: The configuration specified for each BSM server is also relevant for a single machine installation, in which all the servers reside on the same machine.

Special SSL Configuration Considerations

The following points should be taken into consideration when configuring SSL in BSM:

- If you have configured a Reverse Proxy or Load Balancer server to work with your Business Service Management configuration, it is recommended that you configure SSL on the Reverse Proxy or Load Balancer only.
- If the default or local virtual Gateway Server URL has been configured to support HTTPS, you must set the Gateway Server's JRE to trust the server-side certificate returned by the URL configured for the virtual Gateway Server. For details on configuring the default and local virtual Gateway Server URL, see "Using a Reverse Proxy in BSM" on page 33.
- For details on enabling SSL between the Gateway Server and Business Process Monitors, see "Secure Connection from BSM Gateway to BPM Agent" on page 93.

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 83".

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.

BSM Components Supporting SSL

You set a BSM server to support SSL by configuring the Web server installed on the BSM Gateway Server to support SSL.

You configure BSM clients to support SSL by defining the appropriate settings for each particular type of client, as described in the relevant client sections later in this chapter.

Note: For each client configuration, the HTTPS URL must match the SSL certificate common name that is used by the Web server for server-side authentication.

This section includes the following topics:

- "BSM Servers Supporting SSL" on page 61
- "BSM Clients Supporting SSL" on page 62

BSM Servers Supporting SSL

BSM Gateway Servers require Web servers to communicate with their clients.

The servers can be configured to support SSL using one of the following Web servers, according to the operating system on which they are running:

- Microsoft IIS
  - Windows 2000
  - Windows 2003
- Apache Web Server
  - Linux
  - Windows 2000
  - Windows 2003

BSM Clients Supporting SSL

The following BSM clients support SSL communication with the BSM servers:

- **Browsers**. When used as BSM machine (when BSM is installed on a single machine) or Gateway Server clients.
- **Data collectors**. Business Process Monitor, Real User Monitor, SiteScope, and Data Flow Probe, when used as BSM machine (when BSM is installed on a single machine) or Gateway Server clients.

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. For more information, see "Securing BSM Web Server to Require a Client Certificate" on page 68.

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 "Setting JRE to Trust a Security Certificate" on page 70.

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

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.

Securing Communication Between an LDAP Server and BSM Server Over SSL

This section describes the procedure for securing communication between an LDAP server and a BSM server over SSL:

1 Obtain the root CA certificate from the Certificate Authority that issued the LDAP server certificate. Import it into the truststore of the JVM on each BSM gateway (do it for both JRE and JRE64). You may need to restart the BSM gateway machines.

examples:

```
cd C:\HPBSM\JRE64\bin
```

```
keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer  -keystore
..\lib\security\cacerts
```

```
cd C:\HPBSM\JRE\bin
```

```
keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer  -keystore
..\lib\security\cacerts
```

2 Restart BSM.

3 Verify that communication between the LDAP server and the BSM server is valid over SSL, using the Authentication Management Wizard, as follows:

a Navigate to the Authentication Management Wizard by selecting **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, click **Configure** and navigate to the **LDAP General** page.

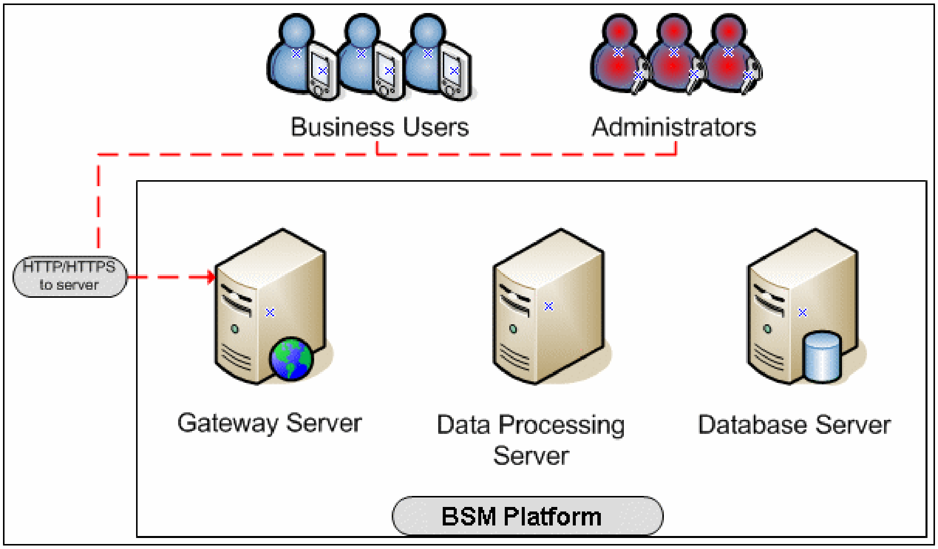
b Enter the URL of your LDAP server, according to the following syntax: ldaps://machine_name:port/[??scope]

Ensure that the protocol is **ldaps:**//, and the port number is configured according to the SSL port, as configured on the LDAP server (default is 636).

c Test your configuration on the LDAP General Configuration page by entering the UUID and password of a known LDAP user in the relevant fields. Click **Test** to authenticate the user. For details, see "LDAP General Configuration Page" in the *Platform Administration* guide, found in the HP BSM Documentation Library.

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.

Working with Client Certificates

This section includes the following topics:

- "Securing BSM Web Server to Require a Client Certificate" on page 68
- "Creating a Keystore" on page 68
- "Configuring Java to Work with the Keystore" on page 70

Securing BSM Web Server to Require a Client Certificate

You can configure your BSM web server to require a client certificate using standard procedures for this type of web server. In addition, it is possible to configure LW-SSO to handle user authentication through a digital certificate. For details, see "How to Secure User Access to BSM Using Client-Side Authentication Certificates" in the *Platform Administration* guide, found in the HP BSM Documentation Library.

Creating a Keystore

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

The keystore may be either a JKS file or a PFX/PKCS#12 file. You can do this in one of two ways:

- **Option 1: Use a Certificate Authority.**
  - Request a client 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.

➤ 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:\server.jks -storepass
changeit

List contents of the keystore, for example:

C:\<HPBSM root directory>\JRE\bin>keytool -list -keystore C:\server.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 using keytool.exe, as in the following example:**

```
1) Create keystore using FQDN of your server:

keytool -genkey -keyalg RSA -alias <your alias> -keystore C:\server.jks  -keypass
changeit -storepass changeit

2) Create a self-signed certificate:

keytool -selfcert -alias <your alias> -keystore C:\server.jks -keypass changeit -
storepass changeit
```

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

Configuring Java to Work with the Keystore

After you have created a keystore that contains the required certificates, you must configure JVM to use the keystore.

To configure JVM to use the keystore, add the following parameters to your JVM instance:

- -Djavax.net.ssl.keyStore=<keystore>
- -Djavax.net.ssl.keyStorePassword=<keystore password as defined>
- -Djavax.net.ssl.keyStoreType=JKS

Setting JRE to Work with Security Certificates

To set the Java Runtime Environment (JRE) to work with security certificates, you must set the JRE to trust a specific security certificate or the authority that issued it.

Setting JRE to Trust a Security Certificate

When the JRE is used to connect to an SSL Web server, or whenever it accepts a certificate, it must be able to validate and trust the certificate to establish the SSL session.

To trust and validate a certificate, JRE uses a trusted certificates store called a **truststore**. If the JRE can find a certificate in its truststore that is identical to the certificate requiring validation, validation is completed and the establishment of the session continues. Otherwise, the JRE will try to validate the digital signature of the certificate signed by the certificate issuer, using the issuing chain.

In order to validate a certificate signed by an issuer, or chain, the issuer's certificate must be included in the truststore used by the JRE. A certificate issuer is a Certification Authority (CA) that signs certificates. If you import the certificate of the CA into the JRE truststore, each certificate issued by this CA can be validated by the JRE.

When a session is started between the JRE 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 JRE and no configuration is required. However, if the CA is not trusted by the JRE, the JRE must be configured to validate the server-side certificate that is sent.

Configuring the Truststore

The following is applicable to the truststore:

- The default truststore file used by the JRE is <**jre root directory**>**\lib\security\cacerts**
- The cacerts file type is JKS (Java Key Store)

Note: If you are not using the default truststore, set the path to the truststore used by your JRE instance by adding two system properties to the JVM as parameters:

- -Djavax.net.ssl.trustStore=<your truststore>
- -Djavax.net.ssl.trustStorePassword=<your truststore password>

To enable your JRE to validate a certificate, import the individual certificate or CA root certificate to the truststore used by your JRE.

To import a required certificate to the truststore:

Add the required certificate to the truststore in binary DER or base 64-encoded format using the **keytool.exe** utility.

The import command should be similar to the following:

```
> <JAVA_HOME>\bin\keytool -import -alias <your alias name> -file <certificate file> -keystore <the truststore used by the JRE> -trustcacerts -storepass <store password>
```

Note: If you are running this procedure on a BSM Gateway Server, it must be applied in both the JRE and JRE64 folders.

For example:

```
cd <BSM root directory>/JRE(64)/bin
```

```
> keytool -import -alias myCA -file c:\myCArootcert.cer -keystore ..\lib\security\cacerts -trustcacerts -storepass changeit
```

Note: The default password of the truststore is **changeit**.

Once the command has been run, the JRE is able to validate the certificate sent by the SSL Web server.

Configuring Tomcat to Support HTTPS

This section describes the procedure for configuring Apache Tomcat 5.x to support HTTPS.

Note: This is a general procedure for Tomcat servers such as those used by SiteScope, RUM, BPM. For specific instructions on how to configure the Application server JMX console on the BSM Gateway, see "Configuring the Application Server JMX Console to Work with SSL" on page 75.

This section includes the following topics:

- "Configuring Tomcat 5.x to Support HTTPS" on page 73
- "Configuring Tomcat to Require Client-Side Certificates" on page 74

Configuring Tomcat 5.x to Support HTTPS

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. For details, see "Setting JRE to Trust a Security Certificate" on page 70.

Configuring the Application Server JMX Console to Work with SSL

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

To configure the Application Server JMX console to work with SSL:

1 Open the file <**HPBSM root directory**>**\EJBContainer\server\mercury\deploy\jboss-web.deployer\server.xml**, located on either the Gateway or Data Processing server, and locate the following section:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
    <Connector port="8443" address="${jboss.bind.address}"
        maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
        emptySessionPath="true"
        scheme="https" secure="true" clientAuth="false"
        keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
        keystorePass="rmi+ssl" sslProtocol = "TLS" />
    -->
```

a Remove the comment indicators **<!--** and **-->** from the file.

b Change every reference to port 8443 in server.xml to an unoccupied port (try 29443).

c Specify keystoreFile, keystoreType (PKCS12 or JKS) and keystorePass. If you have a server certificate in .pfx format, you can use it here and indicate keystoreType = PKCS12, while specifying password to the private key in keystorePass. Alternatively you can create a java keystore and set keystoreType = JKS.

2 Open the file <**HPBSM root directory**>**\EJBContainer\server\mercury\deploy\jmx-console.war\WEB-INF\web.xml**, located on either the Gateway or Data Processing server, and add the following syntax before the closing security-constraint element:

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

so that the file's syntax is displayed as follows:

```
<security-constraint>
     <web-resource-collection>
          <web-resource-name>HtmlAdaptor</web-resource-name>
          <description>An example security config that only allows users with the role
JBossAdmin to access the HTML JMX console web application
          </description>
          <url-pattern>/*</url-pattern>
          <http-method>GET</http-method>
          <http-method>POST</http-method>
      </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>
```

3 Restart BSM.

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 enabled, you can create one. For details, see "Configuring the Truststore" on page 71.

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>\JRE(64)\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**>**\JRE(64)\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 the SYSTEM user. To do this manually, navigate to **Properties** > **Security** > **Advanced** > **Owner.** Click **Other Users or Groups**, type "**SYSTEM**", and click **Check Names**. Verify that you see **Current Owner=SYSTEM**.
- **b** Change the permissions of **jmxremote.password** file to be **Read Only By The Owner** (cmd: cacls jmxremote.password /P SYSTEM:R).
- **c** Try to open the password file. You should now be denied access to it.

In Linux:

- **a** **chmod 600 jmxremote.password**
- **b** Try to open the password file. You should now be denied access to it.

4 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
```

5 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
```

6 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).

Create keystore with the server certificate. Use the FQDN (Fully Qualified Domain Name) of the server in the name field.

Example:

```
keytool -genkey -alias SecureServer -keyalg RSA -keystore Server_Keystore
```

where **SecureServer** is an alias, and **Server_Keystore** is the keystore file name.

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=<HPBSM root directory>\conf\<keystore file name>

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 the SYSTEM user.
- **b** Change the permissions of the **jmx-rmi.properties** file to be read only by the owner (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 SqSL 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:

```
keytool -import -alias SecureServer -file Server.cer -keystore <HPBSM
root directory>\JRE(64)\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.

Configuring a BSM Gateway to Provide a Client Certificate

1 Create Java keystore with a client certificate and store it on the BSM Gateway. For details, see "Creating a Keystore" on page 68.

2 Configure JBOSS to use this keystore:

Add the following parameters to <**HPBSM root directory**>**EJBContainer****bin****mercury_run.bat** (in Linux, **mercury_run.sh**):

- -Djavax.net.ssl.keyStore=<keystore>
- -Djavax.net.ssl.keyStorePassword=<keystore password as defined>
- -Djavax.net.ssl.keyStoreType=JKS

  For example, add this line:

  ```
  set SECURITY_OPTS=-Djavax.net.ssl.keyStore=c:\server.ks -
  Djavax.net.ssl.keyStorePassword=changeit -
  Djavax.net.ssl.keyStoreType=JKS
  ```

  Append %SECURITY_OPTS% to the end of JAVA_OPTS, for example:

  ```
  set JAVA_OPTS=%REMOTE_JMX_ACCESS% %MERCURY_OPTS%
  %PRODUCT_OPTS% %JAVA_OPTS% %SECURITY_OPTS%
  ```

3 Restart BSM Application Server via Nanny manager or disable/enable BSM Gateway.

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.**

Note: The opr-console.war directory may not exist in your installation, in which case ignore this step.

6 After replacing **services-config.xml** in all locations, restart BSM.

5

Using SSL with SiteScope

This chapter includes:

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 53.

For information on connecting SiteScope to a BSM server that requires a client certificate, see "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.

Secure Connection from SiteScope to BSM Gateway

To configure a secure connection from SiteScope to a BSM Gateway, do the following:

1. Configure Java truststore on a SiteScope server to trust the BSM server certificate. For details, see "To import a required certificate to the truststore:" on page 71.
2. Configure SiteScope for SSL. For details, see "To configure SiteScope for SSL using System Availability Management Administration:" on page 86.

3 If BSM requires a client certificate, additional SiteScope configuration is needed.

- ➤ For information on connecting SiteScope to a BSM server that requires a client certificate, see "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.
- ➤ For information on configuring the topology discovery agent in SiteScope to report topology to the BSM server, see "Configuring the Topology Discovery Agent in SiteScope When BSM Server Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.

To configure SiteScope for SSL using System Availability Management Administration:

1 In the SiteScope **Instances** list, right-click the SiteScope object for which you want to configure SSL and select **Edit**.

2 In the Profile Settings section of the Edit SiteScope page, select the **Web server use SSL (HTTPS protocol)** check box.

3 Click **OK** at the bottom of the page.

4 Restart the SiteScope instance.

Secure Connection from BSM Gateway to Sitescope

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

Note: In this situation, the Gateway Server acts as a client connecting to SiteScope using SSL (if required by the SiteScope).

To enable the Gateway Server to communicate with SiteScope using SSL, you must perform the following actions:

1. Configure SiteScope's Tomcat to support SSL. For details, see "Configuring SiteScope's Tomcat to Support SSL" on page 87.
2. Configure the Gateway Server's Java Runtime Environment (JRE) to trust the SiteScope certificate. For details, see "Configuring the Gateway Server's JRE to Trust the SiteScope Certificate" on page 88.
3. Set BSM to use HTTPS to connect to the SiteScope monitor. For details, see "Configuring BSM to Use HTTPS to Connect to a SiteScope Monitor" on page 88.

In addition, if the SiteScope Web server has been configured to force client-side authentication, you must add a client-side certificate to BSM's keystore. For details, see "Adding a Client-side Certificate to BSM's Keystore" on page 88.

Configuring SiteScope's Tomcat to Support SSL

To enable a SiteScope monitor to communicate using SSL:

Configure Tomcat 5.x to support HTTPS. For details, see "Configuring Tomcat to Support HTTPS" on page 72.

Configuring the Gateway Server's JRE to Trust the SiteScope Certificate

If you are not using a publicly known Certificate Authority such as VeriSign, you may need to configure the JRE used by the Gateway Server to trust the certificate sent by Tomcat. For details, see "Setting JRE to Trust a Security Certificate" on page 70.

You must import Tomcat's server-side certificate into the truststore file used by BSM. The truststore file is **<HPBSM root>\JRE\lib\security\cacerts** and it is a JKS type file.

Configuring BSM to Use HTTPS to Connect to a SiteScope Monitor

To configure BSM to use HTTPS to connect to a SiteScope monitor:

1. In System Availability Management Administration, right-click the SiteScope profile you want to configure in the monitors tree and select **Edit SiteScope**.
2. On the Edit SiteScope page, perform the following:
   - Under **Profile Settings**, select the **Use SSL** check box.
   - Under **Main Settings**, change the port number to the one used by the SSL server.

Adding a Client-side Certificate to BSM's Keystore

If Tomcat has been configured to force client-side authentication, you must configure the BSM Gateway to provide client authentication. For details, see "Configuring a BSM Gateway to Provide a Client Certificate" on page 82.

If not using a common Certificate Authority, you may need to configure Tomcat to trust BSM's client-side certificate. For details on performing this task, see "Configuring Tomcat to Require Client-Side Certificates" on page 74.

6

Using SSL with the Business Process Monitor Agent

This chapter includes:

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 53.

Secure Connection from BPM Agent to BSM Gateway

To configure a secure connection from Business Process Monitor to a BSM Gateway:

1 Configure Java truststore on BPM server to trust the BSM server certificate. For details, see "To import a required certificate to the truststore:" on page 71.

2 Configure BPM connection to BSM using SSL. For details, see "Configuring a Connection to the Gateway Server Using SSL" on page 90.

3 If BSM requires a client certificate, additional BPM configuration is needed. For details, see "Configuring Client Certificate Authentication" on page 92.

Configuring a Connection to the Gateway Server Using SSL

When a session is started between the Business Process Monitor and the Gateway Server, the Gateway Server sends the Business Process Monitor a server-side certificate that was issued by a Certification Authority (CA). The Business Process Monitor instance should be configured to trust the certificate or its CA and to communicate via SSL.

Note: When you configure SSL for the Gateway Server on IIS 6.0 or later, run the following command on the Gateway Server to enable BSM to receive samples from the Business Process Monitor:

```
cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs set
w3svc/1/uploadreadaheadsize 200000
```

On completion, restart IIS.

To configure the BPM to connect to the Gateway Server using SSL:

1 Obtain a CA root certificate in PEM format (Base64 encoded).

2 If you do not have a CA root certificate in PEM format:

- **a** Obtain a CA root certificate in Base64 format (you can usually export it from the browser, for example into c:\ca.cer)
- **b** Convert the certificate obtained in step a to PEM format using OpenSSL:
  - ➤ In BPM\bin\ directory, run openssl_10_x32.exe.
  - ➤ When prompted, enter x509 -in <Certificate file full path in Base64 format> -out <Certificate file full path in PEM format>.

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

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

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

4 In the Business Process Monitor page, click the Business Process Monitor instance you want to configure from the **Instances** tree. On the **Configuration** tab, under **Business Service Management Registration Properties**, change the Gateway Server URL to: **HTTPS://<Gateway Server URL>/topaz/**.

Notes:

➤ <**Gateway Server URL**> must match "Default Virtual Gateway Server URL for Data Collectors" as configured in BSM Infrastructure Settings.

➤ This may not be the actual BSM Gateway. It could be any man-in-the-middle server, such as load balancer or reverse proxy.

➤ The URL must end with **/topaz** and not **/MercuryAM** or **/HPBSM**.

5 Add the CA root certificate using one of the following options:

Option 1 - Import the CA root certificate into the BPM truststore:

a In **BPM\JRE6\bin**, run keytool –import –alias <your alias name> –file <certificate file> –keystore <the truststore used by the JRE> –trustcacerts –storepass <store password>

For example: keytool –import –alias myca –file c:\ca.cer -keystore ..\lib\security\cacerts –trustcacerts –storepass changeit

b In the security settings, set the **SSL authority certificate file** field to point to the CA root certificate file in PEM format.

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

Option 2 - Add the CA root certificate to the BPM truststore file to ensure that BSM is trusted by any BPM instance:

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

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

c Restart BPM.

Configuring Client Certificate Authentication

If the Gateway Server requires client-side certification, you must configure a client-side certificate for the Business Process Monitor instance.

To configure a client-side certificate on the BPM machine:

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

2 In the Business Process Monitor page, click the Business Process Monitor instance you want to configure from the **Instances** tree. On the **Configuration** tab, under **Business Service Management Registration Properties**, change the Gateway Server URL to: **HTTPS://<Gateway Server URL>/topaz/**.

3 Request a client certificate from your CA with keys marked as exportable, then export the certificaate in PFX format with a password protected private key.

4 Split the client certificate into two files in PEM format using OpenSSL:

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

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

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

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

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

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

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

d Set the **SSL private key password** field, in the security settings, with the password of the private key if the private key was encrypted with a password.

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

Secure Connection from BSM Gateway to BPM Agent

To configure a secure connection from a BSM Gateway to a Business Process Monitor Agent, do the following:

1 "Configuring a Connection from the Gateway Server to BPM Agent Using SSL" on page 93

2 In addition, if BPM requires a client certificate, do the following:

"Configuring Client Certificate Authentication" on page 96

Configuring a Connection from the Gateway Server to BPM Agent Using SSL

To enable the Gateway Server to communicate with a Business Process Monitor using SSL, you must perform the following actions:

1 Configure a Business Process Monitor to support SSL. For details, see "Configuring a BPM Web Server to Support SSL" on page 94.

2 Configure BSM to use HTTPS to connect to the Business Process Monitor. For details, see "Configuring BSM to Use HTTPS to Connect to a BPM" on page 95.

3 Configure the Gateway Server's Java Runtime Environment (JRE) to trust the Business Process Monitor certificate. For details, see "Configuring the Gateway Server's JRE to trust the BPM certificate" on page 95.

Configuring a BPM Web Server to Support SSL

To enable a Business Process Monitor Web server to support SSL, carry out the following steps:

1 Stop the Business Process Monitor and make sure that all processes are stopped.

2 Open the **<BPM root directory>\ServletContainer\conf\server.xml** file in a text editor and configure Tomcat to support HTTPS. For details, see "Configuring Tomcat to Support HTTPS" on page 72.

3 If you are working on a Windows platform:

a Select **Start** > **Programs** > **HP Business Process Monitor**, then right-click the **Business Process Monitor Admin** link. Select **Properties** from the displayed menu to open the Business Process Monitor Admin Properties dialog box. In the **General** tab, note the path specified in the **Location** field.

b In a new window:

➤ Browse to the folder path noted in the previous step.

➤ Delete the **Business Process Monitor Admin** shortcut.

➤ Right-click the content area to open a menu and select **New** > **Shortcut**. The Create Shortcut dialog window opens.

In **Type the location of the item:** box, enter **https://localhost:8443/**.

In **Type a name for this shortcut:** box, enter **Business Process Monitor Admin**.

Click **Finish**. The Create Shortcut dialog window closes and the new shortcut to Business Process Monitor Admin is listed in the directory.

c Start Business Process Monitor.

d Access the Business Process Monitor Admin console using the new shortcut you created.

Configuring BSM to Use HTTPS to Connect to a BPM

The Business Process Monitor sends the Gateway Server its parameters—Port, URL, and Schema (HTTP/S)—every few hours. These parameters are automatically discovered by the Business Process Monitor according to the Tomcat configuration done above. The Gateway Server will use these parameters to communicate with the Business Process Monitor. It is not necessary to manually configure the Gateway Server.

However, to enable opening the BPM administrative console from the BSM UI using SSL, you may need to update the URL specified in BPM properties for your BPM agent under **Admin** > **End User Management** > **Settings**.

Configuring the Gateway Server's JRE to trust the BPM certificate

If you are not using the same certificate authority to issue all your certificates, you may need to configure the JRE used by the Gateway Server to trust the certificate sent by the Business Process Monitor Web server. For details, see "Setting JRE to Trust a Security Certificate" on page 70.

Troubleshooting

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

- **Windows 2003 and Windows XP** : C:\Documents and Settings\All Users\Application Data\HP\BPM\Tomcat\logs
- **Windows Vista:** C:\ProgramData\HP\BPM\Tomcat\logs
- **Solaris:** /var/opt/HP/BPM/Tomcat/logs

Locate the following string (the directory in the string changes according to the relevant operating system) and copy the **.keystore** file to the directory included in the string:

```
SEVERE: Error initializing endpoint java.io.FileNotFoundException:
C:\Windows\System32\config\systemprofile\.keystore (The system cannot find
the file specified)
```

Configuring Client Certificate Authentication

In order for BPM to require a client certificate, configure Tomcat used by the BPM Agent to require a client certificate. For details, see "Configuring Tomcat to Require Client-Side Certificates" on page 74.

In addition, the BSM server must be configured to provide a client certificate. For details, see "Configuring a BSM Gateway to Provide a Client Certificate" on page 82.

Troubleshooting

Problem: If you see an error like the following in catalina.log:

```
Jan 12, 2011 1:46:27 PM org.apache.coyote.http11.Http11BaseProtocol start

SEVERE: Error starting endpoint

java.io.IOException: DerInputStream.getLength(): lengthTag=109, too big.
```

your keystore is not in the correct format. With client certificate, keystore is expected to be in **.jks** format.

Solution: Convert your server certificate from **.pfx** to **.jks**.

7

Using SSL with Real User Monitor

This chapter includes:

- ➤ Secure Connection from RUM Engine to BSM Gateway on page 97
- ➤ Secure Connection from BSM Gateway to RUM Engine on page 99

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 53.

Secure Connection from RUM Engine to BSM Gateway

To configure a secure connection from Real User Monitor to a BSM Gateway, do the following:

1. Configure Java truststore on RUM Engine server to trust the BSM server certificate. For details, see "To import a required certificate to the truststore:" on page 71.
2. Configure RUM connection to BSM using SSL. For details, see "Configuring a Connection to the Gateway Server Using SSL" on page 98.
3. If BSM requires a client certificate, additional RUM configuration is needed. For details, see "Configuring Client Certificate Authentication" on page 98.

Configuring a Connection to the Gateway Server Using SSL

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

To configure Real User Monitor to connect to the Gateway Server using SSL:

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

2 Click the **Configuration** tab.

3 Select **BSM Connection Settings**.

4 Under **General**, select **HTTPS**.

5 Under **SSL**, enter the following:

- ➤ **<keystore path>.** You can either accept the path of the JRE default keystore file, or enter the path of the keystore file containing the client certificate that you want to use.
- ➤ **<keystore password>.** The password used to access your keystore file.

Select the **Validate that the server certificates are trusted** and the **Validate that the server certificates are not expired** check boxes.

Configuring Client Certificate Authentication

If the Gateway Server requires SSL with client certificates, you must configure a client certificate for the Real User Monitor engine. To do so, obtain a keystore file in JKS format containing the client certificate and private key.

To configure a client certificate on the Real User Monitor engine:

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

2 Click the **Configuration** tab.

3 Select **BSM Connection Settings**.

4 Under **General**, select **HTTPS**.

5 Under **SSL**, fill in the following:

➤ **<keystore path>.** The path of the keystore file you want to use.

➤ **<keystore password>.** The password used to access your keystore file.

➤ **<private key password>.** The password used to access the private key.

Tip: The <private key password> is optional if it is the same as the <keystore password>.

6 Click **Save Configuration**.

Secure Connection from BSM Gateway to RUM Engine

To enable the Gateway Server to communicate with Real User Monitor using SSL, you must perform the following actions:

1 Configure Real User Monitor Tomcat to support SSL. For details, see "Configuring the RUM Tomcat to Support SSL" on page 99.

2 Configure the Gateway Server's Java Runtime Environment (JRE) to trust the Real User Monitor certificate. For details, see "Configuring the Gateway Server's JRE to Trust the RUM Certificate" on page 100.

3 Configure BSM to use HTTPS to connect to Real User Monitor. For details, see "Configuring the RUM URL in BSM for HTTPS" on page 100.

Configuring the RUM Tomcat to Support SSL

To enable a Real User Monitor engine to support SSL communication, you must configure Tomcat 5.x to support HTTPS. The Real User Monitor Tomcat is located at:

```
<Real User Monitor root
directory>\EJBContainer\server\mercury\deploy\jbossweb-tomcat50.sar
```

For details on configuring Tomcat 5.x, see "Configuring Tomcat to Support HTTPS" on page 72.

Configuring the Gateway Server's JRE to Trust the RUM Certificate

You must configure the JRE used by the Gateway Server to trust the certificate sent by the Real User Monitor Web server. For details, see "Setting JRE to Trust a Security Certificate" on page 70.

You must import the Real User Monitor server-side certificate into the truststore file used by BSM. The truststore file is **<HPBSM_root>\JRE\lib\security\cacerts** and it is a JKS type truststore.

Configuring the RUM URL in BSM for HTTPS

You must configure the URL of the Real User Monitor engine defined in End User Management Administration to include the HTTPS protocol.

To configure the Real User Monitor URL defined in End User Management Administration for HTTPS:

1. In End User Management Administration, navigate to **Settings** > **Real User Monitor Settings** > **RUM Engines**. Right-click the Real User Monitor engine object you want to configure and select **Edit Engine**.
2. Select the **Override default connection settings** check box.
3. Change the Real User Monitor URL to:

   https://<RUM domain name>:<HTTPS port number>

   where:

   - <RUM domain> name is the fully qualified domain name of the Real User Monitor engine.
   - <HTTPS port number> is the port number used for HTTPS in the Real User Monitor Web server.

8

Using SSL with Data Flow Probe

This chapter includes:

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 53.

Secure Connection from Data Flow Probe to BSM Gateway

To configure a secure connection from Data Flow Probe to a BSM Gateway, do the following:

1 Configure Java truststore on Data Flow Probe server to trust the BSM server certificate. For details, see "To import a required certificate to the truststore:" on page 71.

2 Configure Data Flow Probe connection to BSM using SSL. For details, see "How to Configure SSL from the Data Flow Probe to the Gateway Server" in the *RTSM Data Flow Management Guide*.

Note: The default UCMDB SSL port, 8443, must be changed to the BSM SSL port, 443, in the **DiscoveryProbe.properties** file.

Configuring Client Certificate Authentication

If the Gateway Server requires client-side certification, you must configure a client-side certificate for the Data Flow Probe.

To configure a client-side certificate on the Data Flow Probe machine:

1. Create a Java keystore containing client certificate. For details, see Creating a Keystore on page 68.
2. Change the following two parameters in the **ssl.properties** file, located in **<Data Flobe Probe root directory>\conf\security** :

   javax.net.ssl.keyStore
   javax.net.ssl.trustStore

   for example:

   ```
   javax.net.ssl.keyStore=c:\\client.jks
   javax.net.ssl.trustStore=C:\\hp\\UCMDB\\DataFlowProbe\\bin\\jre\\l
   ib\\security\\cacerts
   ```
3. Use the MainProbe service in JMX console at port 1977 to encrypt your keystore and truststore passwords using the **getEncryptedKeyPassword** method.
4. Restart Data Flow Probe.

Troubleshooting

If Data Flow Probe fails to connect to BSM server:

- Check that fully qualified BSM server name was used.
- Check that SSL port (serverPortHttps) was changed from the default 8443 to 443.

9

Using SSL with TransactionVision

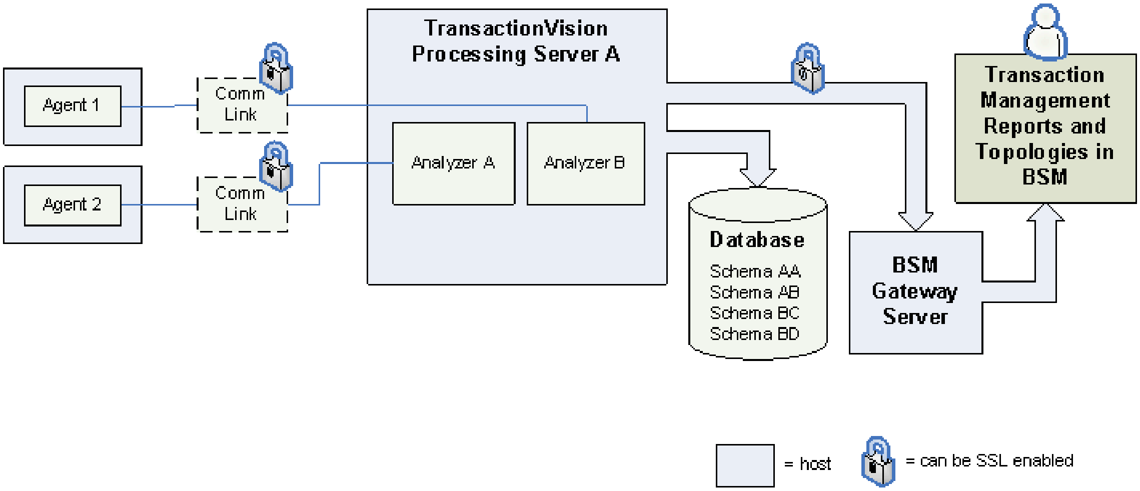
This chapter describes how to configure a BSM platform that includes TransactionVision components to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 53.

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 105
2. "Generate a Certificate" on page 106
3. "Import the Certificate to the BSM Truststore" on page 107
4. "Enable SSL on the TransactionVision Processing Servers" on page 107
5. "Set the BSM Communication Protocol and Port" on page 109
6. "Synchronize the Processing Server" on page 110

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.

For details on performing this task, see "Setting JRE to Work with Security Certificates" on page 70.

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

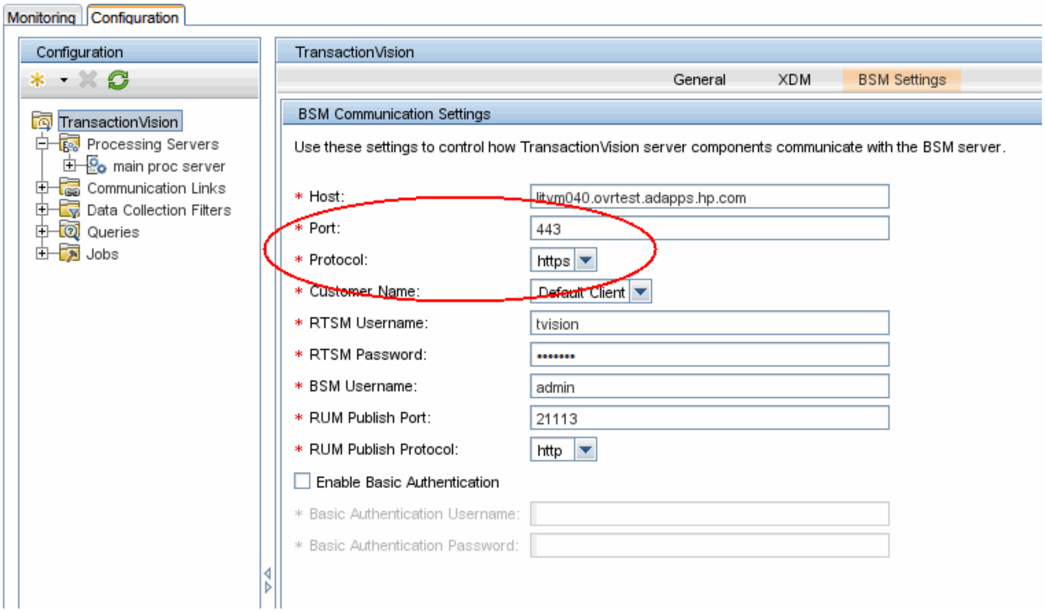
1 Select **Admin** > **Transaction Management** > **Configuration** > **Processing Servers** > <processing server> > <analyzer>**.**

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

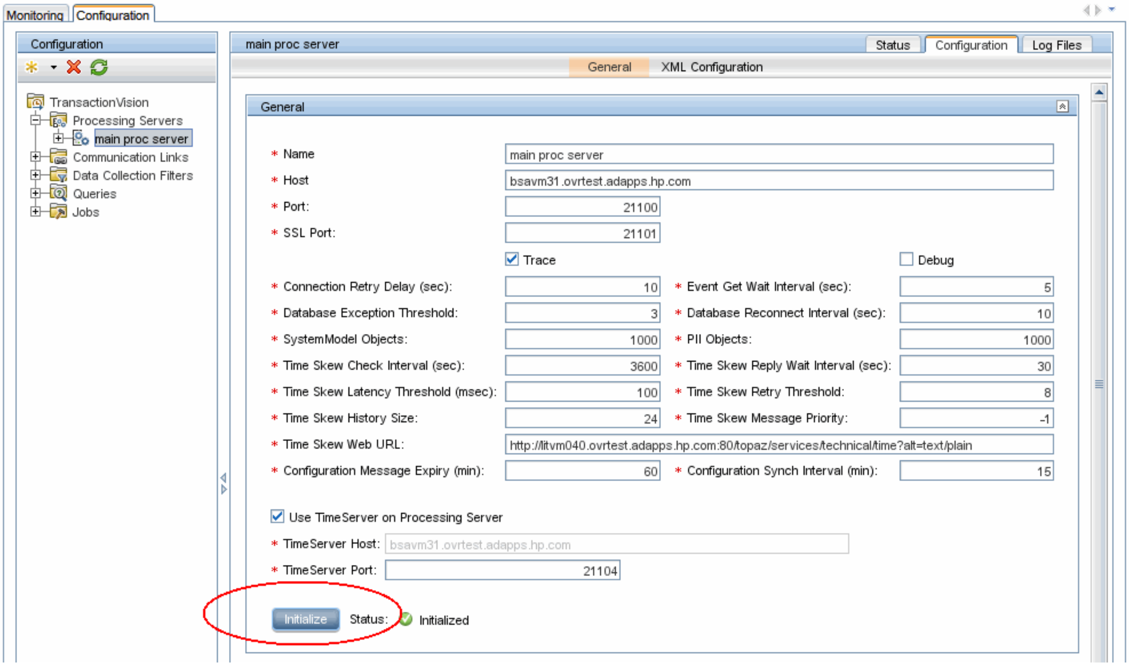
* Basic Authentication Username:	
* Basic Authentication Password:	

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

10

Using Basic Authentication in BSM

This chapter includes:

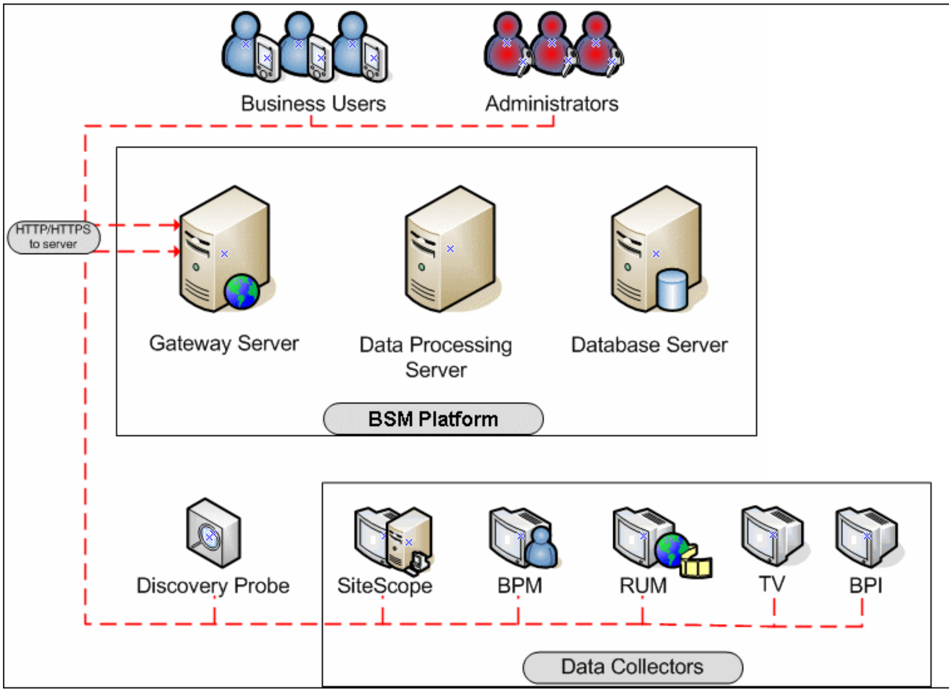
Introducing Basic Authentication Deployment in BSM

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 53.

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



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.

BSM Components Supporting Basic Authentication

You set a BSM server to support basic authentication by enabling basic authentication support for the Web server installed on the BSM server.

You configure BSM clients to support basic authentication by defining the appropriate settings for each particular type of client, as described in the relevant client sections later in this chapter.

This section includes the following topics:

- "Web Servers Supporting Basic Authentication" on page 114
- "BSM Clients Supporting Basic Authentication" on page 114

Web Servers Supporting Basic Authentication

The Web server–operating system combination required for basic authentication support is as follows:

- Microsoft IIS
  - Windows 2000
  - Windows 2003
- Apache Web Server
  - Linux
  - Windows 2000
  - Windows 2003

The Gateway Server requires Web servers to communicate with their clients.

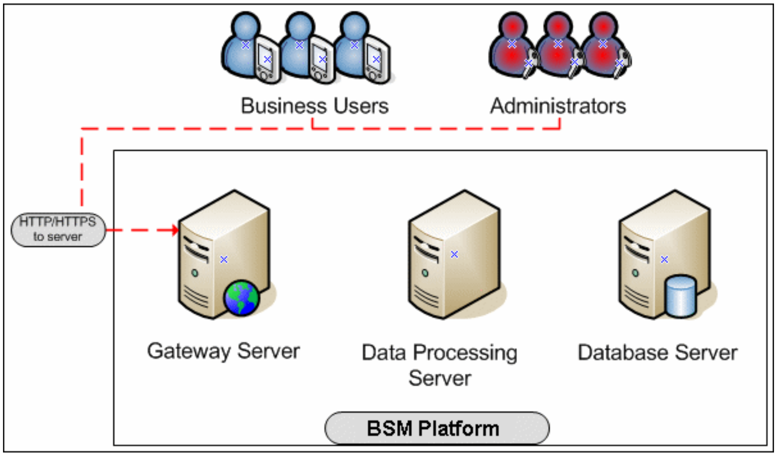
BSM Clients Supporting Basic Authentication

The following BSM clients support basic authentication communication with the BSM servers:

- **Browsers.** When used as BSM machine (when BSM is installed on a single machine) or Gateway Server clients.
- **Data collectors.** Business Process Monitor, Real User Monitor, SiteScope, and Discovery Probe when used as BSM machine (when BSM is installed on a single machine) or Gateway Server clients.

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 116
- "Basic Authentication Configuration for the Application Users" on page 117

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.

If you are not using a publicly known Certificate Authority for your server certificate, you must setup a Java truststore to trust the Certificate Authority that issued the server certificate. For details, see "Setting JRE to Trust a Security Certificate" on page 70.

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.

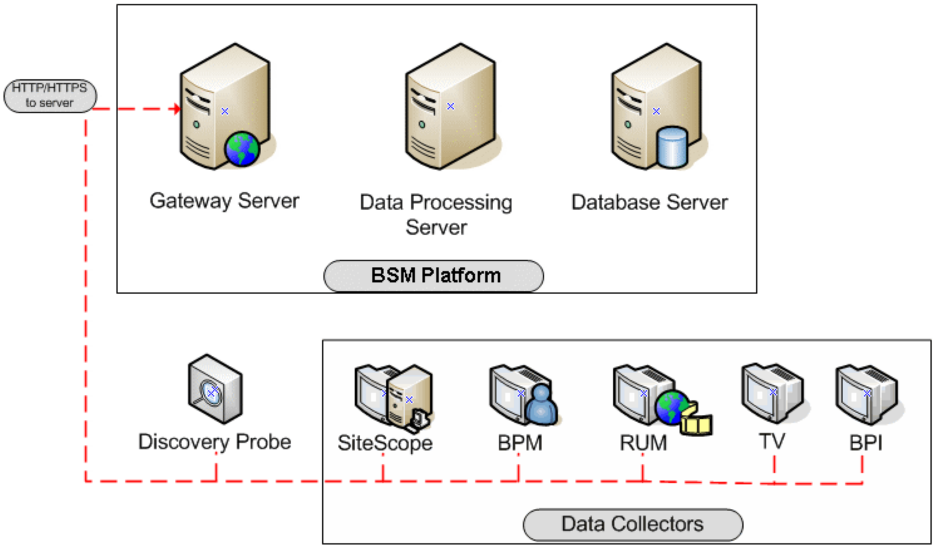
Basic Authentication Configuration for the Application Users

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 119
- "Basic Authentication Configuration for the Data Collectors" on page 120

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 120
- "SiteScope" on page 121
- "Real User Monitor" on page 122
- "Data Flow Probe" on page 122

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**.

Data Flow Probe

If you configured the Gateway Server to require basic authentication, you must configure the Data Flow Probe engine machine to connect to the Gateway Server using basic authentication.

1. Open the file **<Data Flow Probe root>\root\lib\collectors\DiscoveryProbe.properties**.
2. Configure the following properties:
   - **appilog.agent.Probe.BasicAuth.Realm = <authentication domain used to log into BSM>**
   - **appilog.agent.Probe.BasicAuth.User = <username used to log into BSM>**
   - **appilog.agent.Probe.BasicAuth.Pwd = <password used to log into BSM>**

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**.

Hardening JMX Consoles

The instructions in this section describe how to harden the JMX console.

To harden the JMX console:

1 Configure JMX console users by adding the string <**username**>=<**password**> to the following file:

<**HPBSM root directory**>**EJBContainer****server**\ **mercury****conf****props****jmx-console-users.properties**

The default JMX user's credentials are:

Login name = **admin**

Password = **admin**

The administrator can configure other users with other permission levels, and can change the default user's credentials to ensure security.

Caution: The password created in this file is not encrypted, and is therefore visible to anyone who has access to the jmx-console-users.properties file. It is recommended that you change this password immediately to avoid a security risk. Changing the password automatically encrypts it in this file. For details on how to perform this task, see "How to Change the JMX Password" in the *Platform Administration* guide, found in the HP BSM Documentation Library.

---

2 Assign roles to each JMX console user by adding the string <**username**>=<**role**> to the following file:

<**HPBSM root directory**>**EJBContainer****server**\ **mercury****conf****props****jmx-console-roles.properties**

For example, to enable the user **myuser** to operate the JMX console, you must assign the user the **JBossAdmin** role. Add the string **myuser=JBossAdmin** to the properties file above.

For details on configuring the JMX Console to work with SSL, see "Configuring the Application Server JMX Console to Work with SSL" on page 75, and "Configuring the JMX Console to Work with SSL in Other Processes" on page 77.

11

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