HP Business Service Management

for the Windows operating system

Software Version: 9.01

Hardening Guide

Document Release Date: September 2010

Software Release Date: September 2010

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.

Java™ is a US trademark of Sun Microsystems, Inc.

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 TransactionVision

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

Chapter 9 Using SSL with the Staging Data Replicator

Describes how to configure the BSM platform with the Staging Data Replicator 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.

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, you should 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 51 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 out 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 Solaris 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 31.

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 23.

- **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 31.

- **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 51.

- **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 103.

  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 *HP Business Service Management Deployment Guide* PDF.

- **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).
  - **For Sun Java System Web Server.** The Sun Web site (http://docs.sun.com/app/docs/coll/1308.3).

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" on page 25.
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 Business Service Management 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

This section includes the following topics:

- "Web Browser Configuration Overview" on page 23
- "Notes and Limitations" on page 24

Web Browser Configuration Overview

A Web browser on a client machine connecting to HP Business Service Management must enable the following:

- **JavaScript execution.** Java scripting enables you to use HP Business Service Management interactively in a Web browser.
- **Sun 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.** Sun 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.** HP Business Service Management 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

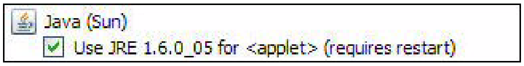
You must configure Java scripting, applets, and cookies in the Internet Explorer Web browser to connect to HP Business Service Management.

This section includes the following topics:

- "To configure Java scripting and applets:" on page 24
- "To configure cookies:" on page 25

To configure Java scripting and 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.



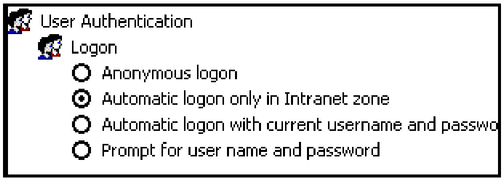
Java (Sun)

☑ 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 HP Business Service Management. 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 configure cookies:

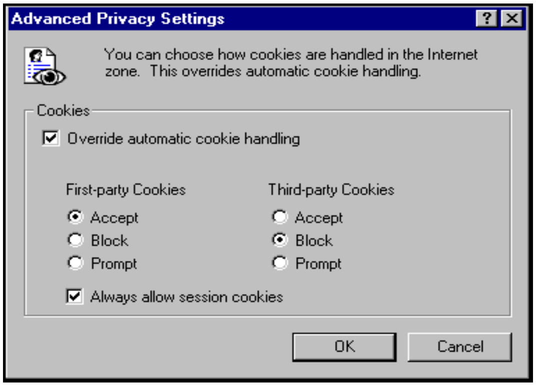
1 Open the Internet Explorer Web browser, select **Tools** > **Internet Options** and select the **Privacy** tab.

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 on page 26.

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 HP Business Service Management.

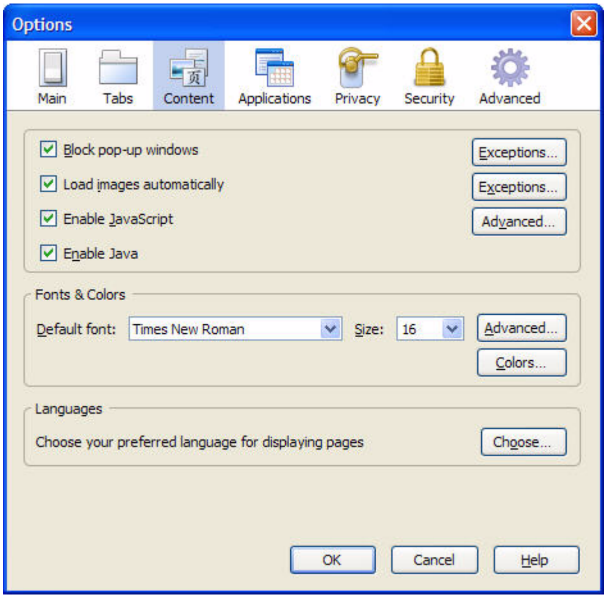
This section includes the following topics:

- ➤ "To configure Java scripting and applets:" on page 27
- ➤ "To configure cookies:" on page 28

To configure Java scripting and applets:

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

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



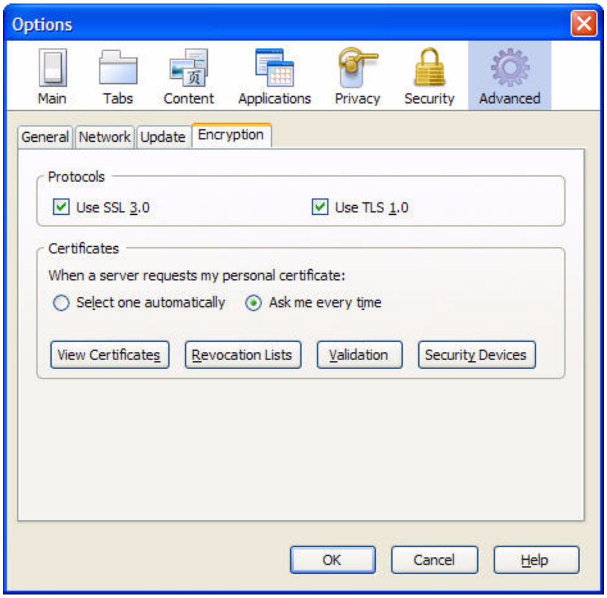
☑ Block pop-up windows
☑ Load images automatically
☑ Enable JavaScript
☑ Enable Java

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

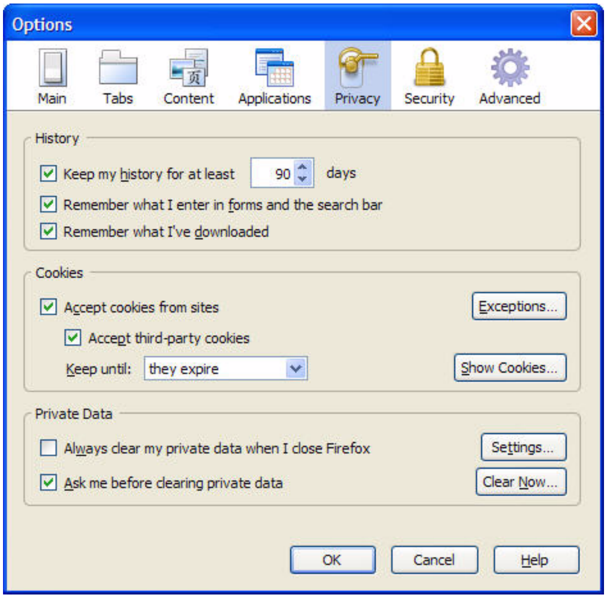
5 Click **OK** to save your settings and close the Options dialog box.

To configure 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** checkboxes.



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 35.

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 34
- "Generic Mode" on page 35

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:

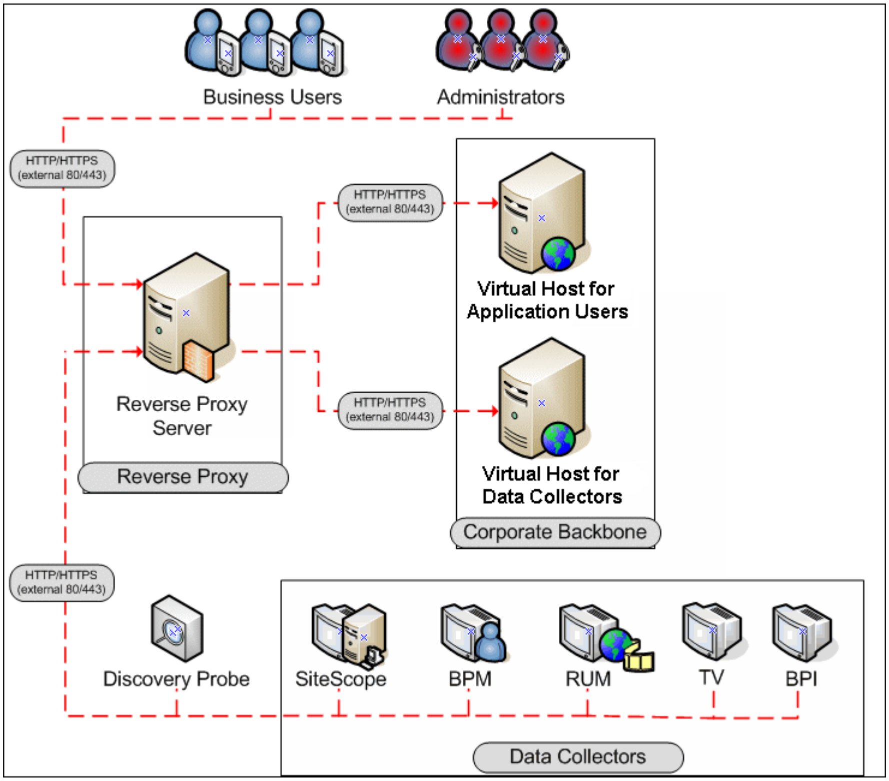
- "Reverse Proxy Configuration" on page 35
- "Configuring BBC Port 383 Connection on Reverse Proxy" on page 42
- "HP BSM Specific Configuration" on page 44
- "Limitations" on page 46
- "Apache 2.x – Distributed Configuration Example" on page 46

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, Discovery 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 46.
- 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/*
/mam-collectors/*	http://[Virtual Host for Data Collectors]/mam-collectors/* https://[Virtual Host for Data Collectors]/mam-collectors/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/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 46.

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:

Note: In an LW-SSO environment, the [BSM server] portion of the syntax must be represented by the FQDN, for example: **<server_name>.<domain_name>/topaz**.

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/*

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/opr-admin-server/*	http://[Virtual Host for Application Users]/opr-admin-server/* https://[Virtual Host for Application Users]/opr-admin-server/*
/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/*

Requests for... on the Reverse Proxy Server	**Proxy Request to be Served by:**
/ucmdb-api/*	http://[Virtual Host for Application Users] /ucmdb-api/* https://[Virtual Host for Application users] /ucmdb-api/*
/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. Obtain a certificate for reverse proxy node from any certificated server that is trusted (e.g., OM W/U/L, OMi):

   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:+EX
P:+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 **Platform Administration**.

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

➤ **Default Virtual Gateway Server URL for application users** and **Default Virtual Gateway Services Server URL for data collectors.** 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.apex.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.apex.com:80.

- **Local Virtual Gateway Server URL for application users** and **Local Virtual Gateway Services Server URL for data collectors** (optional). If you must use more than one URL (the one defined for the **Default Virtual Server URL** parameter) 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.apex.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.

✎

3. **Direct Server URL.** Click the **Edit** button and delete the URL in the **value** field.

✎

4. **Direct Services Server URL.** Click the **Edit** button and delete the URL in the **value** field.
5. 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.

6 Restart the HP BSM service on the BSM machine.

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

You need to configure SSL to work with HP Business Service Management 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

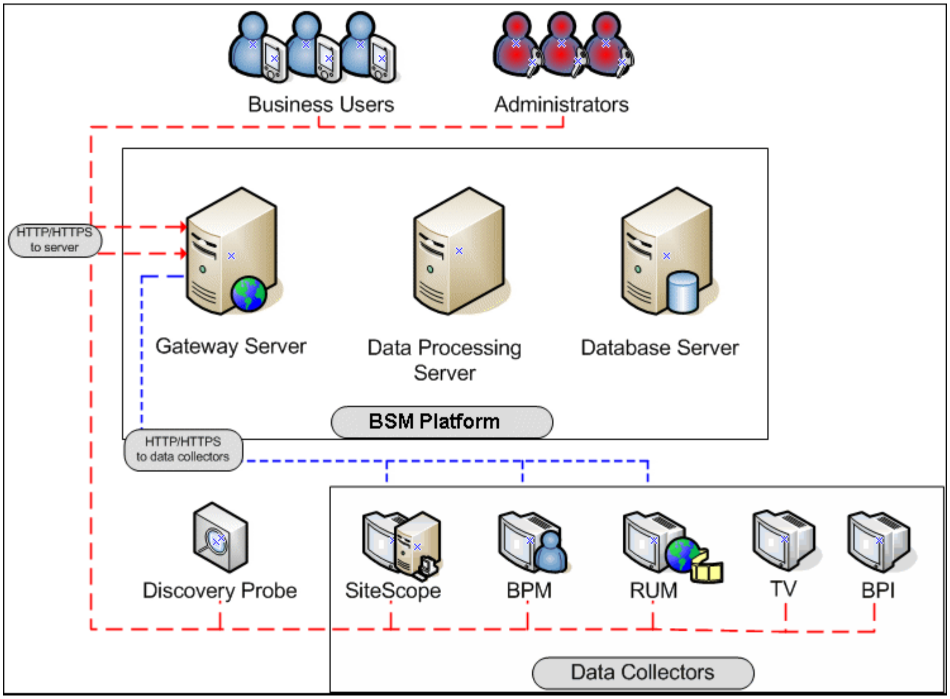
SSL provides BSM with the following:

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

Note: Client authentication is optional.

- **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 *HP Business Service Management Deployment Guide* PDF.

Overview of Configuring SSL in BSM

The section "SSL-Supported Topologies in BSM" on page 58 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 58 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 31.

  For example, if you have configured the Gateway Server to use a secure Reverse Proxy (HTTPS channel only) and have defined a URL of **https://myReverseProxy:443**, you import the certificate returned from the myReverseProxy Web server into the BSM Gateway Server's JRE truststore.
- For details on enabling SSL between the Gateway Server and Business Process Monitors, see "Configuring SSL from the Gateway Server to the BPM Agent" on page 79.

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 57
- "BSM Clients Supporting SSL" on page 57

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	**Sun Java System Web Server**	**Apache Web Server**
Operating System	Windows 2000 Windows 2003	Solaris	Solaris 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 Discovery 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.

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) 5.0 and 6.0.** See http://support.microsoft.com/kb/299875/en-us 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**).
- **Sun Java System Web Server 6.0.** See http://docs.sun.com/app/docs/doc/819-2629/6n4tgd1sf?a=view for information on enabling SSL for all interaction with the Web server. SSL should be enabled for the Sun Java System Web site under which BSM is installed.

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 URL for application users and Default Virtual Gateway Services Server URL for data collectors.** You must enter the server URL with the SSL protocol https and the SSL port (default is 443). For example: https://my_server.apex.com:443
   - **Local Virtual Gateway Server URL for application users** and **Local Virtual Gateway Services Server URL for data collectors** (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.apex.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 Centers Server URL.** Click the **Edit** button and delete the URL in the **value** field.
4. **Direct Core Services Server 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:

Note: Steps 1 through 3 provide instructions on how to create a certificate for the LDAP keystore, enabling the LDAP server to work with SSL. If the LDAP server already has a certificate in its keystore, skip directly to step 4.

To configure the LDAP server to work with SSL:

1 Create a certificate request for the LDAP server, from the LDAP User Interface.

2 Apply the LDAP server's certificate request to the certificate authority to retrieve a digital identity certificate.

3 Import the created certificate to the LDAP server keystore.

4 Import the LDAP trusted certificate to the BSM server truststore. For details on performing this task, see "Setting JRE to Work With Security Certificates" on page 63.

   If you do not have an LDAP server trusted certificate, contact your LDAP administrator to obtain one.

5 Restart BSM.

6 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.

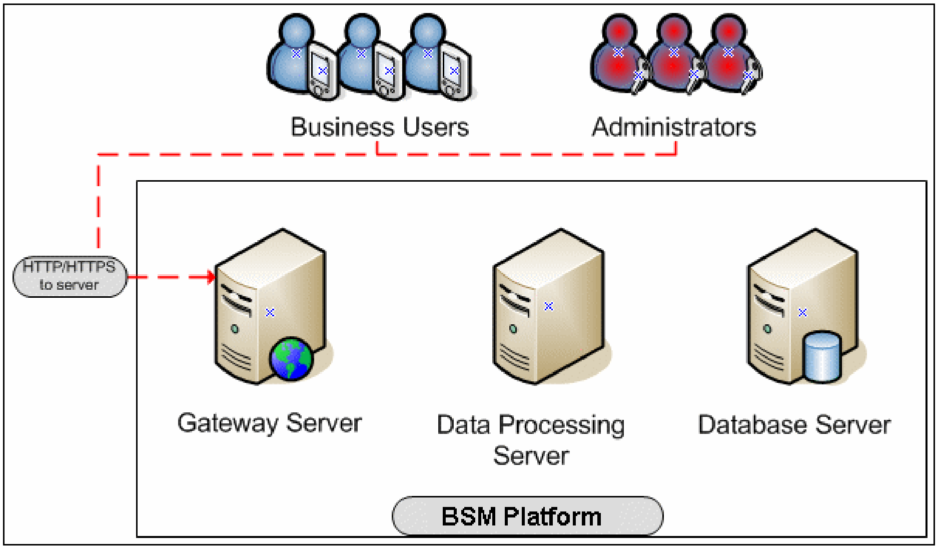
   b Enter the URL of your LDAP server, according to the following syntax: ldaps://machine_name:port/[??scope]

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 Business Service Management 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 certificate into BSM's JVM for communicating with the data collectors over SSL.

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 security certificate and to use client/server-side authentication.

This section includes the following topics:

- "Setting JRE to Trust a Security Certificate" on page 63
- "Setting JRE to Use Client Side Authentication" on page 65

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 are 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)
- You can set 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 certificate, or any of its users across the certificate issuing chain, to the truststore used by your JRE.

To import a required certificate to the truststore:

Add the required certificate to the truststore in PEM format using the **keytool.exe** utility.

The import command should be similar to the following:

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

For example, for a server with SSL support called **www.mysslserver.com**, a JRE truststore called **c:\<HPBSM root directory>\jre\lib\security\cacerts**, and a CA issued certificate called **mysslserver** found in the file **c:\mycacert.pem**, the following is the correct format for the command to import the required certificate to the truststore:

```
> keytool -import -alias mycacert -file c:\mycacert.pem -keystore
c:\jre150\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.

Setting JRE to Use Client Side Authentication

When the JRE is used as the server-side in an SSL communication channel, it can be required to send a client/server-side certificate. The JRE uses its keystore to look for the certificate and the corresponding private key. To support the sending of certificates by JRE, carry out the following steps:

1. Import, or create, a keystore containing the certificates and private keys.
2. Define the keystore parameters in the JVM run-time properties.

Note: The default keystore used by the JRE is a file called **.keystore,** and is located in the user's home directory.

To import or create a keystore containing the certificates and private keys:

- The keystore can be either a JKS file or a PKCS#12 file.
- You can create a JKS file with a self-signed certificate using keytool.exe.

  An example of the keytool command for creating a JKS file is:

  ```
  /> %JAVA_HOME%\bin\keytool -genkey -dname "CN=your name,
  OU=organization unitO=organization" -validity <number of days> -keystore
  <new keystore> -alias <key alias>-keypass <key password> -storepass
  <store password>
  ```

  The parameters used are:

  - **dname.** Distinguished name.
  - **validity.** Certificate validity.
  - **keystore.** The new store to be created, or to which to add the new key.
  - **alias.** The new certificate and key alias name in the keystore.
  - **keypass.** The password for using the private key.
  - **storepass.** The password for using the keystore.

- You can generate a self-signed certificate using the keys generated by the previous command.

  An example of the keytool command for creating a JKS file is:

  ```
  /> keytool -selfcert -alias <key alias> -keystore <new keystore>-keypass <key password> -storepass <store password>
  ```

  The parameters used are:

  - **keystore.** The new store to be created, or to which to add the new key.
  - **alias.** The new certificate and key alias name in the keystore.
  - **keypass.** The password for using the private key.
  - **storepass.** The password for using the keystore.

To define the keystore parameters in the JVM run-time properties:

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=PKCS12 or JKS

Configuring Tomcat to Support HTTPS

This section describes the procedure for configuring Apache Tomcat 5.0.x to support HTTPS.

To configure Tomcat 5.0.x to support HTTPS:

1. Uncomment the following connector element in the %TOMCAT_HOME%\conf\server.xml file:

   ```
   <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="false" sslProtocol="TLS"/>
   ```

Note: If you are not using the default port number 8443 for the Tomcat SSL communications, change the port number in the connector element accordingly.

2 Locate the XML Connector element that is not commented out 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

3 Add the following attribute to the connector element:

```
keystoreFile="myKeyStore"
```

where myKeyStore is the JKS file that contains the Web server certificate and a corresponding private key (e.g., d:\sitescope\java\lib\security\cacerts).

4 Change the keystore type password accordingly in the connector element:

```
keystorePass="your password"
```

```
keystoreType="jks" or "pkcs12"
```

5 Restart Tomcat.

Configuring Tomcat to Trust Client-side Certificates

You must set Apache Tomcat to trust the client-side certificate sent by BSM. For details, refer to http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

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 63.

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****jbossweb-tomcat55.sar****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 Remove the first line from the file, so that the file's opening syntax reads, <Connector port="8443" address="${jboss.bind.address}

c Enter the keystore file's path in the keystoreFile attribute, and the keystore's password in the keystorePass attribute.

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.
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 64.

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 51.

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 in the SiteScope Help.

Configuring SSL from the Gateway Server 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:

- Configure SiteScope's Tomcat to support SSL. For details, see "Configuring SiteScope's Tomcat to Support SSL" on page 74.
- 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 75.
- 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 75.

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 75.

Configuring SiteScope's Tomcat to Support SSL

To enable a SiteScope monitor to communicate using SSL, you must configure Tomcat 5.0.x to support HTTPS.

For details on how to configure Tomcat 5.0.x to support HTTPS, see "Configuring Tomcat to Support HTTPS" on page 66.

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 63.

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

Configuring BSM to Use HTTPS to Connect to a SiteScope Monitor

In monitor administration, right-click the SiteScope profile you want to configure in the monitors tree and select **Edit**.

On the Edit SiteScope page, under **Main Settings**, perform the following:

- Select the **Use SSL** check box.
- 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 add a client-side certificate that can be sent from BSM to SiteScope.

To add a client-side certificate:

1. Request client certificate for your BSM Server.
2. If you do not use a Certificate Authority, set the BSM Java Virtual Machine (JVM) to support client-side authentication. For details, see "Setting JRE to Trust a Security Certificate" on page 63.

Note: You must define the keystore used by BSM as described in "Setting JRE to Trust a Security Certificate" on page 63.

3 Configure Tomcat to trust BSM’s client-side certificate. For details on performing this task, see "Configuring Tomcat to Trust Client-side Certificates" on page 68.

Configuring SSL from SiteScope to the Gateway Server

If the SiteScope machine is required to communicate with the Gateway Server via SSL, you must configure the SiteScope machine to connect to the Gateway Server using SSL.

This section details how to enable an SSL connection from SiteScope to the Gateway Server using the BSM Monitor Administration pages, or directly via the SiteScope Administration pages.

Import the certificate/CA certificate Used by the Gateway Server(s) into the SiteScope Truststore

SiteScope uses its Java Runtime Environment (JRE) to communicate with the Gateway Server using SSL. To be able to validate the certificate coming from the Gateway Server by the JRE used in SiteScope, the certificate, or its issuer, must be trusted by the JRE.

SiteScope’s JRE uses a truststore (a store of trusted CAs and certificates) which is located in the file:

<**SiteScope root directory**>**java****lib****security****cacerts**

By default, the **cacerts** file contains common CA certificates, so if the Gateway Server is using a certificate issued by a known issuer, it is likely that no import operation to the truststore will be needed.

If the Gateway Server is using a certificate issued by an unknown CA, or it is using a self-signed certificate, you must import the certificate used by the Gateway Server, or the CA certification path that issued the certificate, to the truststore.

Note: The keystore used can be in either PKCS12, or JKS format.

For details on importing a required certificate, see "To import a required certificate to the truststore:" on page 64.

To configure SiteScope for SSL using BSM Monitor Administration:

1 In the BSM monitor tree, 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.

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 51.

Configuring SSL from the Gateway Server to the BPM Agent

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

- Configure a Business Process Monitor to support SSL. For details, see "Configuring a BPM Web Server to Support SSL" on page 80.
- 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 83.
- 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 83.

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

3. Locate the XML Connector element that is not commented out and comment it out. For example, change:

   ```
   <Connector port="2696" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   redirectPort="8443" acceptCount="100" connectionTimeout="20000"
   disableUploadTimeout="true" />
   ```

   to:

   ```
   <!--  <Connector port="2696" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   redirectPort="8443" acceptCount="100" connectionTimeout="20000"
   disableUploadTimeout="true" />     -->
   ```

4. Locate the XML Connector element with an attribute scheme set to **https** and uncomment it. For example, change:

   ```
   <!--<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https"
   secure="true" clientAuth="false" sslProtocol="TLS" />-->
   ```

   to:

   ```
   <Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https"
   secure="true" clientAuth="false" sslProtocol="TLS" />
   ```

5. Save the <**Business Process Monitor root directory**>\ServletContainer\conf\server.xml file.

6 Create a keystore certificate by running the following command:

- **For Windows** – <Business Process Monitor root directory>\JRE\bin\keytool -genkey -alias tomcat -keyalg RSA
- **For Solaris** – <Business Process Monitor root directory>/JRE/bin/keytool -genkey -alias tomcat -keyalg RSA

7 When prompted for the keystore password, enter changeit (all lower case). To choose a different password, see the Tomcat documentation (http://jakarta.apache.org/tomcat/tomcat-4.0-doc/ssl-howto.html).

8 Enter general information about the certificate when prompted for this information.

9 When prompted for the key password for the certificate, use the same password you used previously for the keystore.

10 Execute the following command:

```
keytool -list
```

and enter the password: changeit

The following is an example of the message that appears after when the command is completed:

```
Keystore type: jks

Keystore provider: SUN

Your keystore contains 1 entry

tomcat, 27.11.2009, keyEntry,

Certificate fingerprint (MD5):
1C:6E:99:0C:69:B4:B0:F5:92:62:9B:55:87:B1:F8:14
```

11 For Windows only, ensure that the **.keystore** file was added to:

- **Windows Vista** – C:\Users\Administrator\
- **Windows 2003 and Windows XP** – C:\Documents and Settings\Administrator\

12 For Windows Vista only, copy the **.keystore** file to **C:\Windows\System32\config\systemprofile\** so that the .keystore file is located in both the administrator and system profile directories.

13 For Solaris only, copy the **.keystore** file that was created in the home directory of the user with which you ran the above command to the home directory of the user running Business Process Monitor Admin (**root** user).

14 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.

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/Tomact/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 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.

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

You must 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 63.

You must import the Business Process Monitor server-side certificate into the truststore file used by BSM. The truststore file is **%mercury_root%\JRE\lib\security\cacerts** and it is a JKS type file.

Configuring SSL from the BPM Agent to the Gateway Server

Configuring SSL support for the Business Process Monitor involves the following procedures:

- "Configuring a Connection to the Gateway Server Using SSL" on page 84
- "Configuring an SSL Client-Side Certificate" on page 85

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
```

and then restart the IIS.

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

1. Obtain the truststore file in PEM format, base64 encoded. The file can consist of the server-side certificate itself, or the certificate of the CA that issued the server-side certificate, or all certificates required for the trust path (all certificates must be placed in the same PEM file).
2. Open Business Process Monitor Admin (**http://<Business Process Monitor machine>:2696**).

3 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.

4 In the **General** section, change the Gateway Server URL to: **HTTPS://<Gateway Server URL>/topaz/**.

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

---

5 In the **SSL** section, configure the **SSL authority certificate file** to point to the truststore file (so that the Business Process Monitor instance recognizes the file), using the full path to a local file.

Alternatively, you can add a BSM certificate into the following Business Process Monitor truststore file:

<BPM Root Directory>\dat\cert\default_auth_cert.pem

to ensure that BSM is trusted by any Business Process Monitor instance.

The certificate file must be in PEM format and base64 encoded.

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

Configuring an SSL Client-Side Certificate

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

3 Enter the following SSL parameter values:

- **SSL client certificate file.** The path of the PEM file that holds the client-side certificate.
- **SSL private key file.** The path of the PEM file that holds the private key used as a public/private pair key for the public key in the client-side certificate.
- **SSL private key password.** The password of the private key, if the private key was encrypted with a password.

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

7

Using SSL with Real User Monitor

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 51.

Configuring SSL from the Gateway Server to the RUM Engine

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

- Configure Real User Monitor Tomcat to support SSL. For details, see "Configuring the RUM Tomcat to Support SSL" on page 88.
- 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 88.
- Configure BSM to use HTTPS to connect to Real User Monitor. For details, see "Configuring the RUM URL in BSM for HTTPS" on page 88.

Configuring the RUM Tomcat to Support SSL

To enable a Real User Monitor engine to support SSL communication, you must configure Tomcat 5.0.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 5.0.x, see "Configuring Tomcat to Support HTTPS" on page 66.

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 63.

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 BSM Monitor Administration to include the HTTPS protocol.

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

1 In BSM Monitor Administration, right-click the Real User Monitor engine object you want to configure and select **Edit**.

2 Open the **Advanced Settings** section.

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.

Configuring SSL from the RUM Engine to the Gateway Server

Configuring SSL support for Real User Monitor involves the following procedures:

- "Importing the certificate/CA certificate Used by the Gateway Server(s) into the RUM Truststore" on page 89
- "Configuring a Connection to the Gateway Server Using SSL" on page 90
- "Configuring an SSL Client-Side Certificate" on page 90

Note: For details on configuring Java Runtime Environment to work with security certificates when using SSL with the Real User Monitor Snapshot applet, see "Setting JRE to Trust a Security Certificate" on page 63.

Importing the certificate/CA certificate Used by the Gateway Server(s) into the RUM Truststore

Real User Monitor uses its Java Runtime Environment (JRE) to communicate with the Gateway Server using SSL. To be able to validate the certificate coming from the Gateway Server by the JRE used in Real User Monitor, the certificate, or its issuer, must be trusted by the JRE.

Real User Monitor's JRE uses a truststore (a store of trusted CAs and certificates) which is located in the file:

<Real User Monitor root directory>\java

For details on importing a certificate to the JRE truststore, see "To import a required certificate to the truststore:" on page 64.

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 an SSL Client-Side Certificate

If the Gateway Server is supporting SSL with client-side certificates, you must configure a client-side 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-side 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.

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

6 Click **Save Configuration**.

8

Using SSL with TransactionVision

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

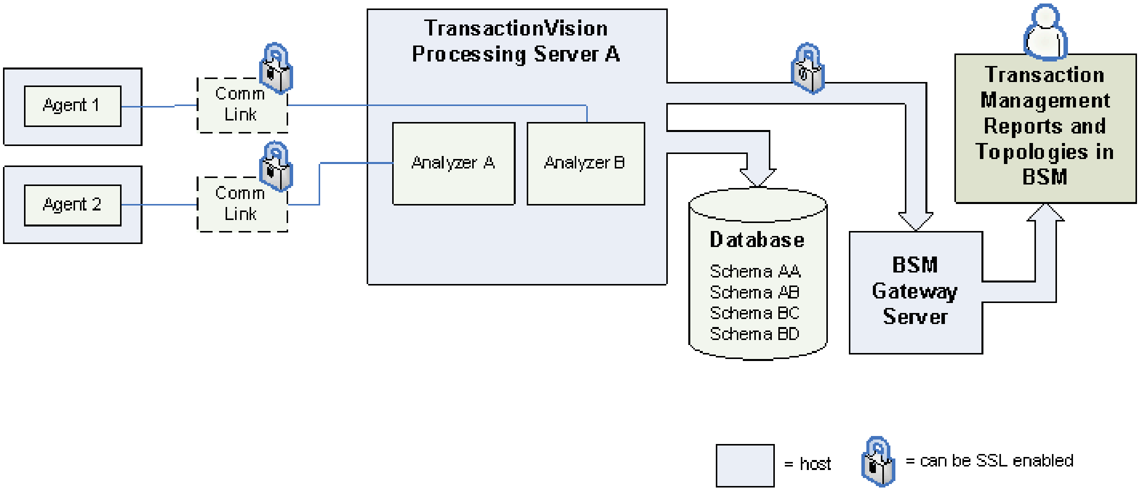
This chapter includes:

- About SSL and TransactionVision on page 94
- Configuring SSL Between a TransactionVision Processing Server and the BSM Gateway Server on page 95

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 51.

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 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.

Task 1: 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 needs to be restarted. For information about restarting these components, see *Using Transaction Management*.

Task 2: Generate a Certificate

To generate a certificate in the default keystore, follow these steps:

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 Solaris is /opt/HP/TransactionVision; on AIX it is /usr/lpp/HP/TransactionVision; and 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**.

Task 3: Import the Certificate to the BSM Truststore

The certificate generated in Task 2: 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 63.

This task requires the BSM Gateway Server to be restarted.

Task 4: 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** checkbox.

Enter the Keystore Password and Location, and the Key password. These values were provided as result of Task 2: 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.

To modify the SSL port for the SonicMQ Broker

1. Select **Admin** > **Transaction Management** > **Configuration** > **TransactionVision** > **Configurative** > **General.**
2. Edit the **oobsonic.xml** to enable SSL.

For more information about these configuration options, see "Processing Servers" and "Analyzers" in *Using Transaction Management.*

Task 5: Enable SSL on the SonicMQ Brokers

If the TransactionVision deployment environment is using the built-in SonicMQ messaging middleware, the SonicMQ Broker must also be enabled for SSL. Each Processing Server has its own SonicMQ Broker.

To enable SSL on the SonicMQ Broker, refer to the *Progress SonicMQ Deployment Guide*. This document is available on the Progress SonicMQ Documentation page at <TVISION_HOME>/Sonic/ mq_documentation_7.6.htm.

The SonicMQ acceptors can be modified to use the same certificate and keystore created in Task 2: Generate a Certificate. This procedure is described in chapter 8 in the *Progress SonicMQ Configuration and Management Guide*.

When modifying the acceptors, note the following:

- You can use the Sonic Management Console to change the acceptor's properties. To access the console run <TVISION_HOME>\Sonic\MQ7.6\bin\startmc.(bat|sh).
- The TV_SSL_ACCEPTOR TCP/SSL Acceptor and SECURE_RUM_ACCEPTOR HTTP(S) Direct Acceptor are the acceptors that need to be modified. Click the JSSE button on the SSL tab when viewing the acceptor properties to modify them.
- A running SonicMQ broker responds dynamically to configuration changes associated with TCP and SSL acceptor types (but not HTTP(S) type acceptors). For example, as TCP or SSL type acceptors are added to a broker configuration, the running broker automatically starts accepting incoming connections on the newly-defined acceptor as soon as the broker receives the configuration changes. (A broker must be reloaded to reflect HTTP(S) type acceptor changes.)

Task 6: 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) > **BSM Settings**, and set the **Protocol** to https and **Port** to 443.

Task 7: 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.

9

Using SSL with the Staging Data Replicator

This chapter includes:

- SSL Configuration for the Staging Data Replicator on page 101

For introductory and general information on configuring BSM and its data collectors to support SSL, see "Using SSL in BSM" on page 51.

SSL Configuration for the Staging Data Replicator

The Staging Data Replicator (SDR) is used during the staging part of the upgrade to repeat samples from a BSM 7.x machine to a BSM 8.0 machine.

To configure the SDR to support SSL when sending samples to WDE:

Configure the SDR to use SSL. In the <**SDReplicator**>**\conf\b2g_translator.xml** file, edit the following, being sure to use **https**.

```
<ForwardURL
url="https://__DESTINATION_HOST_NAME__/ext/mod_mdrv_wrap.dll?type
=wde_bin_handler&acceptor_name=__DESTINATION_HOST_NAME__&me
ssage_subject=topaz_report/samples&request_timeout=30&force_keep_aliv
e=true&send_gd=true"/>
```

To configure the SDR to trust the BSM certificate:

1. Obtain a copy of the certificate used by the Web Server on the BSM Gateway Server. This file must be a DER encoded binary X.509 (.CER) file.
2. Import BSM's certificate into SDR's KeyStore. For details, see "To import a required certificate to the truststore:" on page 64.

   ➤ Configure SDR to use KeyStore, and add additional options in the file **<BSM Install dir>\SDR\7.x\bin\sdreplicator_run.bat**, as follows:

   ➤ Locate the following line: SET PROCESS_OPTS=%PROCESS_OPTS% -Dconf.file=%PRODUCT_HOME_PATH%\conf\b2g_translator.xml -Dprop.file=%PRODUCT_HOME_PATH%\conf\b2g_translator.properties -Dmsg.filter.file=%PRODUCT_HOME_PATH%\conf\b2g_exclude_samples.xml

   ➤ At the end of this line, add the following syntax:

   -Dnet.ssl.trustStore=<keystore path>

   -Dnet.ssl.trustStorePassword=passphrase

10

Using Basic Authentication in BSM

This chapter includes:

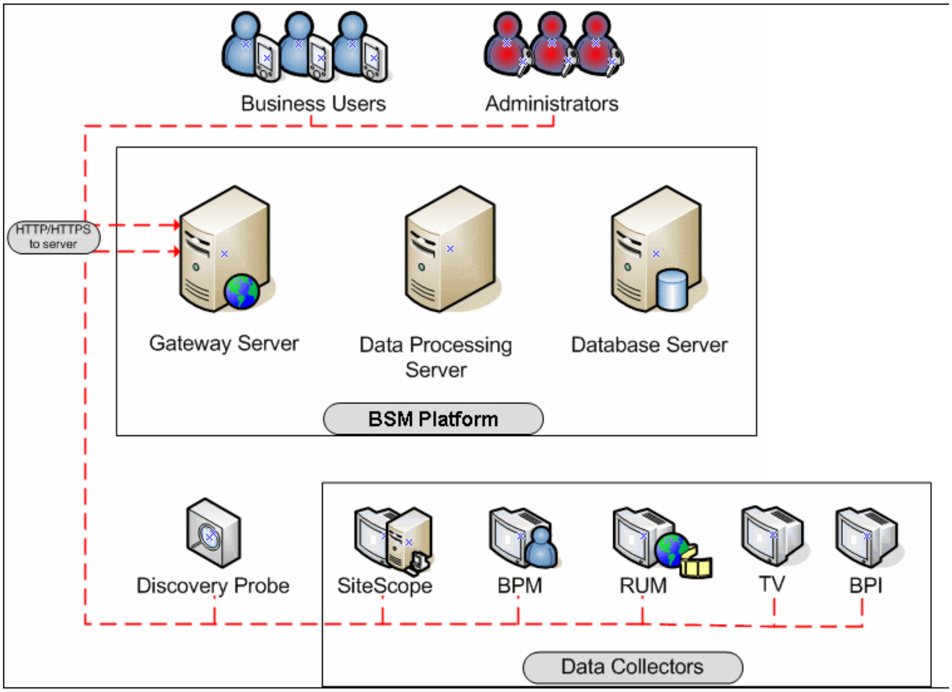
Introducing Basic Authentication Deployment in BSM

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 51.

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 106
- "BSM Clients Supporting Basic Authentication" on page 106

Web Servers Supporting Basic Authentication

The following table details the Web server–operating system combination that is required for basic authentication support.

	Microsoft IIS	**Sun Java System Web Server**	**Apache Web Server**
Operating System	Windows 2000 Windows 2003	Solaris	Solaris Windows 2000 Windows 2003

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

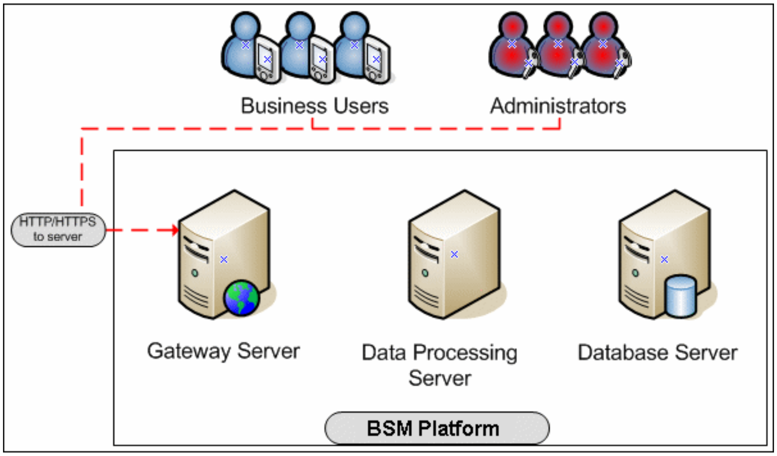
BSM Clients Supporting Basic Authentication

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 108
- "Basic Authentication Configuration for the Application Users" on page 109

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.

- **Sun Java System Web Server 6.0.** See http://docs.sun.com/app/docs/doc/819-2629/6n4tgd1sv?mfr=view for information on enabling basic authentication for all interaction with the Web server.

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

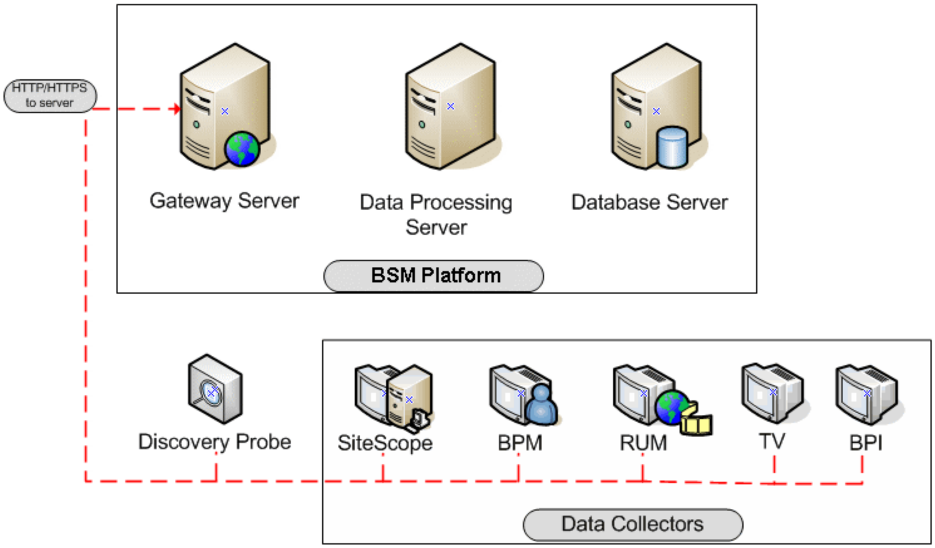
Basic Authentication Configuration for the Application Users

This section provides instructions for configuring the application users (Gateway Server clients) to support basic authentication.

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

Configuring Basic Authentication Between the Gateway Server and 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 111
- "Basic Authentication Configuration for the Data Collectors" on page 112

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.
- **Sun Java System Web Server 6.0.** See http://docs.sun.com/app/docs/doc/819-2629/6n4tgd1sv?mfr=view for information on enabling basic authentication for all interaction with 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 112
- "SiteScope" on page 113
- "Real User Monitor" on page 114
- "Discovery Probe" on page 114

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:

- If you are configuring SiteScope using BSM Monitor Administration, right-click the SiteScope you want to instruct to use basic authentication, and select **Edit**.

  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.

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

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

  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.

  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**.

Discovery Probe

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

1 Open the file **%discovery_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 *Platform Administration*.

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.

To harden the MX4J JMX console:

1. Create a .txt file in the directory **<HPBSM root directory>\conf**
2. Add the following line:

   <username> <password>

For example: myuser mypassword

Note: If you make a mistake when entering your username or password when logging into MX4J, you must close your browser and re-open it.

For details on configuring the JMX Console to work with SSL, see "Configuring the Application Server JMX Console to Work With SSL" on page 69, and "Configuring the JMX Console to Work With SSL in Other Processes" on page 70.

Index