HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 8.06

Hardening Guide

Document Release Date: December 2010
Software Release Date: December 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.

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

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

This guide provides you with detailed instructions on hardening the HP Business Availability Center platform.

Note to HP Software-as-a-Service customers: Only the Web Browser Security in HP Business Availability Center 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 HP Business Availability Center Platform

Describes the concept of a secure HP Business Availability Center platform and discusses the planning and architecture required to implement a secure platform.

Chapter 2 Web Browser Security in HP Business Availability Center

Describes how to configure a Web browser in order to secure your browser access to HP Business Availability Center.

Chapter 3 Using a Reverse Proxy in HP Business Availability Center

Describes how to use a reverse proxy with HP Business Availability Center in order to help secure HP Business Availability Center architecture.

Chapter 4 Using SSL in HP Business Availability Center

Describes how to configure the HP Business Availability Center 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 DDM Probe

Describes how to configure Discovery and Dependency Mapping to support Secure Sockets Layer (SSL) communication.

Chapter 10 Using SSL with the Staging Data Replicator

Describes how to configure the HP Business Availability Center platform with the Staging Data Replicator to support Secure Sockets Layer (SSL) communication.

Chapter 11 Using Basic Authentication in HP Business Availability Center

Describes how to configure the HP Business Availability Center platform to support communication using basic authentication.

Who Should Read This Guide

This guide is intended for the following users of HP Business Availability Center:

- HP Business Availability Center administrators
- Security administrators

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

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the *HP Business Availability Center Deployment Guide* PDF.

1

Introduction to Hardening the HP Business Availability Center Platform

This chapter introduces the concept of a secure HP Business Availability Center 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.

This chapter includes:

Introduction to Hardening

The HP Business Availability Center 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) HP Business Availability Center 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 HP Business Availability Center. You can also invoke dedicated Gateway deployment, in which several Gateway servers are assigned different tasks.

The hardening information provided is intended primarily for HP Business Availability Center administrators, and for the technical operator of each component that is involved in the implementation of a secure HP Business Availability Center 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

In order 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 HP Business Availability Center platform into your network.
- Review all the hardening guidelines.

A good understanding of the HP Business Availability Center technical framework and HP Business Availability Center security capabilities will facilitate designing a solid plan for implementing a secure HP Business Availability Center 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 HP Business Availability Center 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 HP Business Availability Center servers to support SSL, read "Using SSL in HP Business Availability Center" on page 63 and then follow all the instructions chronologically.

- The HP Business Availability Center 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 HP Business Availability Center platform. Using the machines for other purposes in addition to HP Business Availability Center may yield problematic results.

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

Deploying HP Business Availability Center in a Secure Architecture

Several measures are recommended to securely deploy your HP Business Availability Center 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 HP Business Availability Center clients and the HP Business Availability Center 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 to deploy HP Business Availability Center using a reverse proxy. HP Business Availability Center 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 HP Business Availability Center:

➤ No HP Business Availability Center logic or data resides on the DMZ.

➤ No direct communication between HP Business Availability Center clients and servers is permitted.

➤ No direct connection from the DMZ to the HP Business Availability Center database is required.

- The protocol used to communicate with the reverse proxy can be HTTP/S. 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 HP Business Availability Center 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 HP Business Availability Center to achieve a secure architecture. For details on configuring a reverse proxy for use with HP Business Availability Center, see "Using a Reverse Proxy in HP Business Availability Center" on page 29.

If you must use another type of secure architecture with your HP Business Availability Center 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 HP Business Availability Center.**

This chapter contains information on configuring your Web browser to support secure Web browsing. For details, see "Web Browser Security in HP Business Availability Center" on page 21.

➤ **Using a reverse proxy in HP Business Availability Center.**

This chapter contains information on using a reverse proxy with HP Business Availability Center in order to help secure HP Business Availability Center architecture. For details, see "Using a Reverse Proxy in HP Business Availability Center" on page 29.

➤ **Configuring the HP Business Availability Center platform to use SSL communication.**

This chapter contains information on configuring each HP Business Availability Center component to support Secure Sockets Layer (SSL) communication. For details, see "Using SSL in HP Business Availability Center" on page 63.

➤ **Configuring the HP Business Availability Center platform to use basic authentication.**

This chapter contains information on configuring each HP Business Availability Center component to support communication using the basic authentication protocol. For details, see "Using Basic Authentication in HP Business Availability Center" on page 141.

Communication channels between HP Business Availability Center servers, data collectors, application users, and HP Business Availability Center platform components use various protocols on specific ports. For details, see "Port Usage" in the *HP Business Availability Center Deployment Guide* PDF.

➤ **Configuring your web server to work with HP Business Availability Center.**

This chapter contains information on configuring the Web server on an HP Business Availability Center 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).

2

Web Browser Security in HP Business Availability Center

This chapter describes the security setup of a Web browser running on Windows or Solaris and contains instructions for configuring your Web browser to work with HP Business Availability Center.

This chapter includes:

HP Business Availability Center and Web Browsers

Web Browser Configuration Overview

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

- **JavaScript execution.** Java scripting enables you to use HP Business Availability Center 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 Availability Center 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 Availability Center.

This section includes the following topics:

To configure Java scripting and applets:

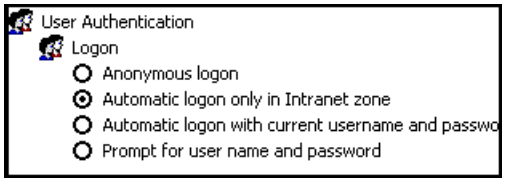
1. In the Internet Explorer Web browser, select **Tools** > **Internet Options**, and click the **Advanced** tab.
2. Scroll down to the **Java (Sun)** section. Select **Use Java2**. Any Java2 version v1.5.x or v1.6x is acceptable.

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 Availability Center. Select the option most suitable for your site.



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 Java2** in step 2, you must restart your browser for the changes to take effect. If **Use Java2** 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.

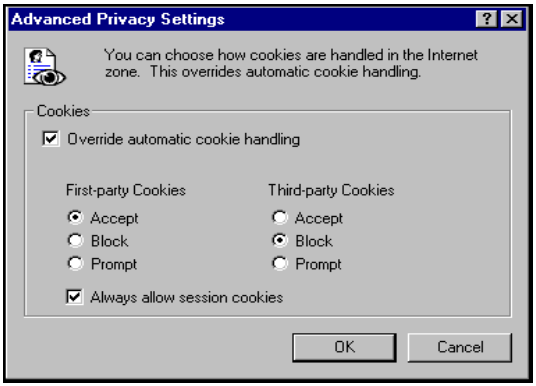
2 In the Settings pane, you can configure cookies in one of two ways:

- ➤ 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.



➤ Click **OK** to save your settings. Proceed to step 5 on page 24.

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 Availability Center.

This section includes the following topics:

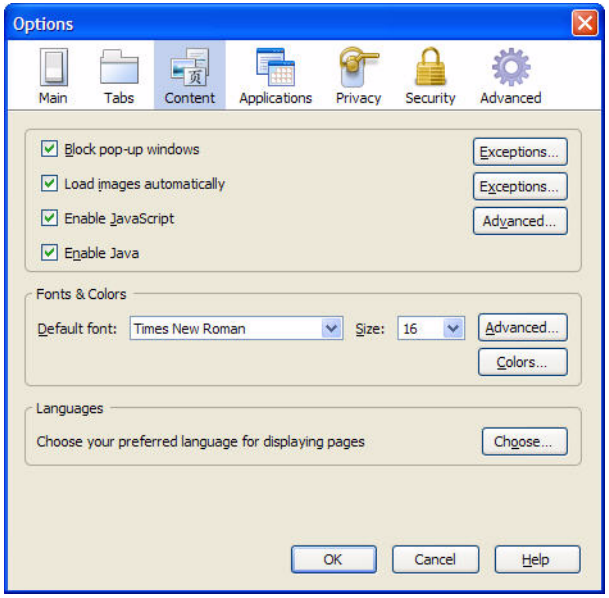
➤ "To configure Java scripting and applets:" on page 25

➤ "To configure cookies:" on page 27

To configure Java scripting and applets:

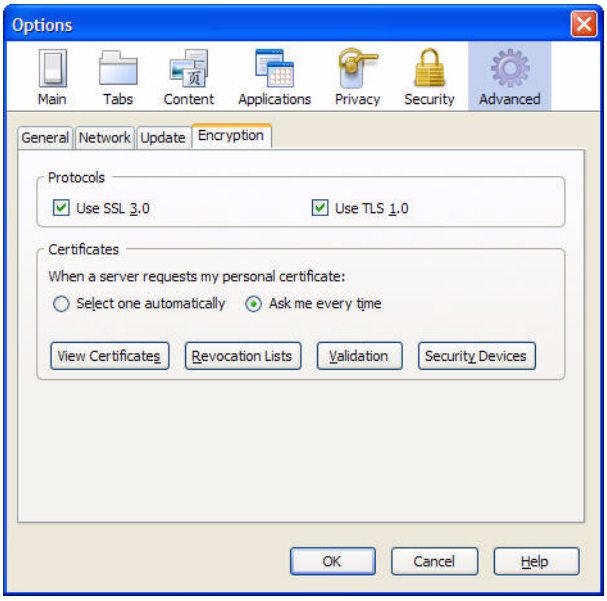
1 In the FireFox Web browser, select **Tools** > **Options** and click the **Content** button.

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



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

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



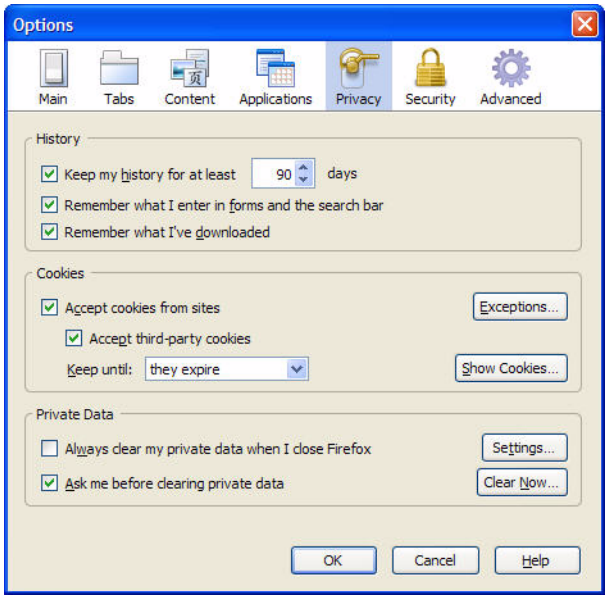
5 Click **OK** to save your settings and close the Options dialog box.

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.



3

Using a Reverse Proxy in HP Business Availability Center

This chapter describes the security ramifications of reverse proxies and contains instructions for using a reverse proxy with HP Business Availability Center.

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.

This chapter includes:

Overview of Reverse Proxies

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.

For configuration information when using a reverse proxy with an external UCMDB server, see "Connect the DDM Probe by Reverse Proxy" in *Discovery and Dependency Mapping Guide*.

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.

HP Business Availability Center and Reverse Proxies

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

If a reverse proxy is being used for application users, HP Business Availability Center must be configured to recognize use of a reverse proxy. If not, the HP Business Availability Center URL optimization mechanism will not be able to properly calculate absolute paths.

If a reverse proxy is being used for data collectors, only the data collectors and reverse proxy must be configured to recognize its use.

HP Business Availability Center servers can be installed using the following two architectures:

- **Single server installation.** The Data Processing and Gateway Servers reside on the same machine.
- **Two server installation.** The Data Processing and Gateway Servers reside on separate machines.

To configure a reverse proxy for either of these architectures, see "Using a Reverse Proxy with a One and Two Machine Installation" on page 34.

You can connect the following to HP Business Availability Center via a reverse proxy:

- HP Business Availability Center data collectors
- HP Business Availability Center application users

Specific and Generic Reverse Proxy Mode Support for HP Business Availability Center

HP Business Availability Center 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, HP Business Availability Center must be configured to return the reverse proxy base URL, instead of the HP Business Availability Center 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 HP Business Availability Center server(s).

There are two proxy modes that control user access to HP Business Availability Center servers:

- "Specific Mode" on page 33
- "Generic Mode" on page 33

Specific Mode

This mode should be used if you want to concurrently access HP Business Availability Center 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 or HTTPS request causes HP Business Availability Center to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Centers Server URL** or the **Local Virtual Centers Server URL** (when defined), if the HTTP or HTTPS request came through one of the IP addresses defined for the **HTTP** or **HTTPS Reverse Proxy IPs** parameter. If the HTTP or HTTPS request did not come through one of these IP addresses, the base URL that HP Business Availability Center receives in the HTTP or HTTPS 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.

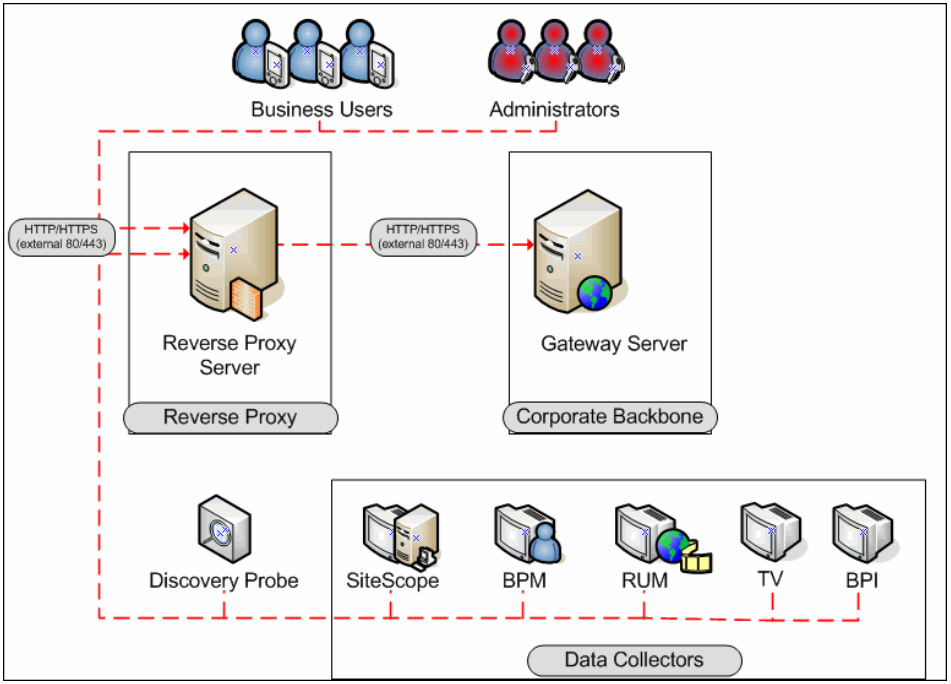
If you are working in this mode, each time an HTTP or HTTPS request causes the HP Business Availability Center application to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Centers Server URL** or the **Local Virtual Centers Server URL** (when defined).

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

Using a Reverse Proxy with a One and Two Machine Installation

This section includes the following topics:

A reverse proxy can be used with a single machine installation (Gateway and Data Processing Servers are on one machine) and for a two machine installation (Gateway Server is on one machine while the Data Processing Server is on the second machine).



Reverse Proxy Configuration

In this topology, all contexts must point to the same machine, on which the HP Business Availability Center servers are installed.

Reverse proxy HP Business Availability Center support should be configured differently in each of the following cases:

Scenario #	HP Business Availability Center Components Behind the Reverse Proxy
1	Data collectors (Business Process Monitor, Real User Monitor, SiteScope, Discovery Probe)
2	Application users
3	Data collectors and application users

Note: Different types of reverse proxies require different configuration syntaxes. For an example of an Apache 2.2.x reverse proxy configuration, see "Apache 2.2.x – Example Configuration" on page 46.

Support for HP Business Availability Center Data Collectors

The following configuration is required if only data collectors are connected via a reverse proxy to your one or two machine HP Business Availability Center installation:

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/topaz_api/*	http://[HP Business Availability Center server]/topaz/topaz_api/* https://[HP Business Availability Center server]/topaz/topaz_api/*
/topaz/sitescope/*	http://[HP Business Availability Center server]/topaz/sitescope/* https://[HP Business Availability Center server]/topaz/sitescope/*
/ext/*	http://[HP Business Availability Center server]/ext/* https://[HP Business Availability Center server]/ext/*
/mam-collectors/*	http://[HP Business Availability Center server]/mam-collectors/* https://[HP Business Availability Center server]/mam-collectors/*
/tv/*	http://[HP Business Availability Center Gateway Server]/tv/* https://[HP Business Availability Center Gateway Server]/tv/*
/axis2/*	http://[HP Business Availability Center Gateway Server]/axis2/* https://[HP Business Availability Center Gateway Server]/axis2/*

Support for HP Business Availability Center Application Users

The following configuration is required if only application users are connected via a reverse proxy to your one or two machine HP Business Availability Center installation:

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/HPBAC/*	http://[HP Business Availability Center server] /HPBAC/* https://[HP Business Availability Center server] /HPBAC/*
/hpbac/*	http://[HP Business Availability Center server] /hpbac/* https://[HP Business Availability Center server] /hpbac/*
/MercuryAM/*	http://[HP Business Availability Center server] /MercuryAM/* https://[HP Business Availability Center server] /MercuryAM/*
/mercuryam/*	http://[HP Business Availability Center server] /mercuryam/* https://[HP Business Availability Center server] /mercuryam/*
/topaz/*	http://[HP Business Availability Center server] /topaz/* https://[HP Business Availability Center server] /topaz/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/sitescope/GroupPermissions.jsp	http://[HP Business Availability Center server]/topaz/sitescope/GroupPermissions.jsp https://[HP Business Availability Center server]/topaz/sitescope/GroupPermissions.jsp
/webinfra/*	http://[HP Business Availability Center server]/webinfra/* https://[HP Business Availability Center server]/webinfra/*
/filters/*	http://[HP Business Availability Center server]/filters/* https://[HP Business Availability Center server]/filters/*
/TopazSettings/*	http://[HP Business Availability Center server]/TopazSettings/* https://[HP Business Availability Center server]/TopazSettings/*
/opal/*	http://[HP Business Availability Center server]/opal/* https://[HP Business Availability Center server]/opal/*
/mam/*	http://[HP Business Availability Center server]/mam/* https://[HP Business Availability Center server]/mam/*
/mam_images/*	http://[HP Business Availability Center server]/mam_images/* https://[HP Business Availability Center server]/mam_images/*
/mcrs/*	http://[HP Business Availability Center server]/mcrs/* https://[HP Business Availability Center server]/mcrs/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/rumproxy/*	http://[HP Business Availability Center server] /rumproxy/* https://[HP Business Availability Center server] /rumproxy/*
/bpi/*	http://[HP Business Availability Center server] /bpi/* https://[HP Business Availability Center server] /bpi/*
/dashboard/*	http://[HP Business Availability Center server] /dashboard/* https://[HP Business Availability Center server] /dashboard/*
/utility_portlets/*	http://[HP Business Availability Center server] /utility_portlets/* https://[HP Business Availability Center server] /utility_portlets/*
/tv/*	http://[HP Business Availability Center server] /tv/* https://[HP Business Availability Center server] /tv/*
/tvb/*	http://[HP Business Availability Center server] /tvb/* https://[HP Business Availability Center server] /tvb/*

Support for Both HP Business Availability Center Data Collectors and Application Users

The following configuration is required if both data collectors and application users are connected via a reverse proxy to your one or two machine HP Business Availability Center installation:

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/HPBAC/*	http://[HP Business Availability Center server] /HPBAC/* https://[HP Business Availability Center server] /HPBAC/*
/hpbac/*	http://[HP Business Availability Center server] /hpbac/* https://[HP Business Availability Center server] /hpbac/*
/MercuryAM/*	http://[HP Business Availability Center server] /MercuryAM/* https://[HP Business Availability Center server] /MercuryAM/*
/mercuryam/*	http://[HP Business Availability Center server] /mercuryam/* https://[HP Business Availability Center server] /mercuryam/*
/topaz/topaz_api*	http://[HP Business Availability Center server] /topaz/topaz_api/* https://[HP Business Availability Center server] /topaz/topaz_api/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/webinfra/*	http://[HP Business Availability Center server] /webinfra/* https://[HP Business Availability Center server] /webinfra/*
/filters/*	http://[HP Business Availability Center server] /filters/* https://[HP Business Availability Center server] /filters/*
/TopazSettings/*	http://[HP Business Availability Center server] /TopazSettings/* https://[HP Business Availability Center server] /TopazSettings/*
/opal/*	http://[HP Business Availability Center server] /opal/* https://[HP Business Availability Center server] /opal/*
/mam/*	http://[HP Business Availability Center server] /mam/* https://[HP Business Availability Center server] /mam/*
/mam_images/*	http://[HP Business Availability Center server] /mam_images/* https://[HP Business Availability Center server] /mam_images/*
/mcrs/*	http://[HP Business Availability Center server] /mcrs/* https://[HP Business Availability Center server] /mcrs/*
/ext/*	http://[HP Business Availability Center server] /ext/* https://[HP Business Availability Center server] /ext/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/mam-collectors/*	http://[HP Business Availability Center server] /mam-collectors/* https://[HP Business Availability Center server] /mam-collectors/*
/rumproxy/*	http://[HP Business Availability Center server] /rumproxy/* https://[HP Business Availability Center server] /rumproxy/*
/bpi/*	http://[HP Business Availability Center server] /bpi/* https://[HP Business Availability Center server] /bpi/*
/dashboard/*	http://[HP Business Availability Center server] /dashboard/* https://[HP Business Availability Center server] /dashboard/*
/utility_portlets/*	http://[HP Business Availability Center server] /utility_portlets/* https://[HP Business Availability Center server] /utility_portlets/*
/tv/*	http://[HP Business Availability Center server] /tv/* https://[HP Business Availability Center server] /tv/*
/tvb/*	http://[HP Business Availability Center server] /tvb/* https://[HP Business Availability Center server] /tvb/*
/axis2/*	http://[HP Business Availability Center Gateway Server]/axis2/* https://[HP Business Availability Center Gateway Server]/axis2/*

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 2.2.x – Example Configuration" on page 46.

For additional configuration information when working with an embedded HP Universal CMDB server, see "Using a Reverse Proxy" in the *HP Universal CMDB Deployment Guide* PDF.

HP Business Availability Center-Specific Configuration

In addition to configuring the reverse proxy to work with HP Business Availability Center, you must configure HP Business Availability Center to work with the reverse proxy.

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

To configure HP Business Availability Center 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 Centers Server URL** and **Default Virtual Core Services Server URL.** Verify that these parameters represent the URL of the machine (reverse proxy, load balancer, or other type of machine) used to access the Gateway server machine. For example, http://my_reverse_proxy.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.

     If the reverse proxy server requires SSL, then you must enter the protocol and port as required for SSL, along with the reverse proxy server machine name. For example:
     https://my_reverse_proxy.apex.com:443

➤ **Local Virtual Centers Server URL** and **Local Virtual Core Services Server URL** (optional). If you must use more than one URL (the one defined for the **Default Virtual Core Server URL** parameter) to access the Gateway server machine, define a **Local Core Centers Server URL** for each machine through which you want to access the Gateway server machine. For example, http://my_specific_virtual_server.apex.com:80.

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 Centers Server URL** parameter is defined for a specific machine, this URL is used instead of the **Default Virtual Centers 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 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 the IP address of the reverse proxy sending the HTTP or HTTPS request is included in the list of IP addresses defined for this parameter, the URL returned to the client is either the **Default Virtual Centers Server URL** or the **Local Virtual Centers Server URL** (when defined). If the IP address of the reverse proxy sending the HTTP or HTTPS 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 or HTTPS request.

Note: If no IP addresses are defined for this parameter (the default option), HP Business Availability Center works in Generic Mode and the Gateway server machine returns the **Default Virtual Centers Server URL** or the **Local Virtual Centers 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 Business Availability Center service on the HP Business Availability Center machine.

Note: Once you change the HP Business Availability Center 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 HP Business Availability Center to work in Generic Mode, all the HP Business Availability Center clients must access the HP Business Availability Center machine via the reverse proxy.

Apache 2.2.x – Example Configuration

Below is a sample configuration file that supports the use of an Apache 2.2.x reverse proxy in a case where both data collectors and application users are connecting to a one or two machine Gateway server installation.

Note: In the example below, the Gateway Server machine's DNS name is **BAC_Server**.

---

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          /mercuryam      http://BAC_server/mercuryam
ProxyPassReverse   /mercuryam      http://BAC_server/mercuryam
ProxyPass          /MercuryAM      http://BAC_server/MercuryAM
ProxyPassReverse   /MercuryAM      http://BAC_server/MercuryAM
ProxyPass          /hpbac          http://BAC_server/hpbac
ProxyPassReverse   /hpbac          http://BAC_server/hpbac
```

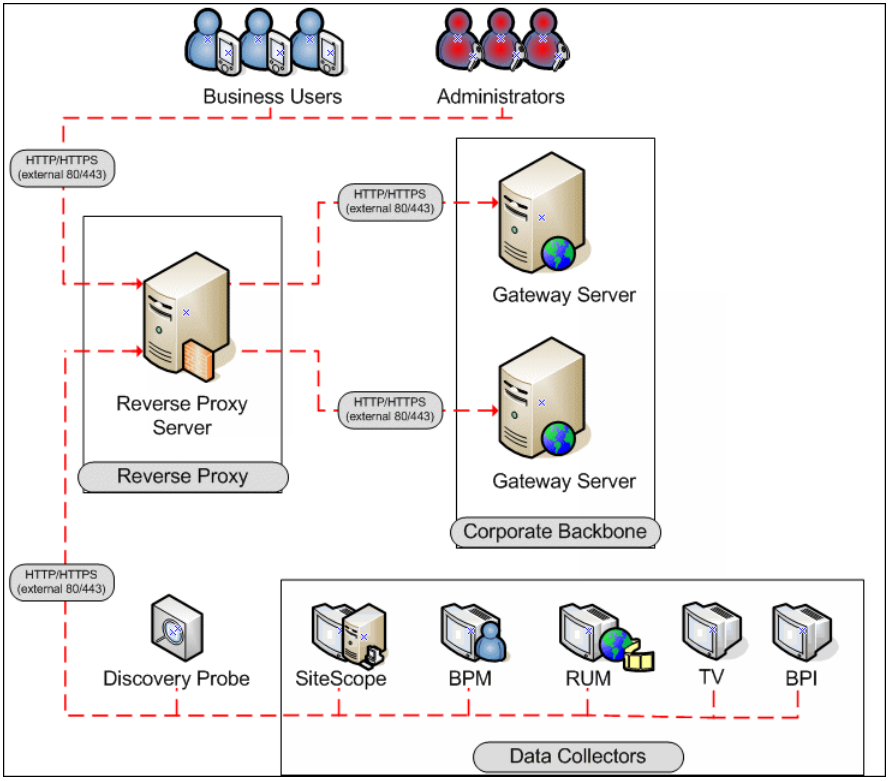
ProxyPass	/HPBAC	http://BAC_server/HPBAC
ProxyPassReverse	/HPBAC	http://BAC_server/HPBAC
ProxyPass	/topaz	http://BAC_server/topaz
ProxyPassReverse	/topaz	http://BAC_server/topaz
ProxyPass	/ext	http://BAC_server/ext
ProxyPassReverse	/ext	http://BAC_server/ext
ProxyPass	/webinfra	http://BAC_server/webinfra
ProxyPassReverse	/webinfra	http://BAC_server/webinfra
ProxyPass	/filters	http://BAC_server/filters
ProxyPassReverse	/filters	http://BAC_server/filters
ProxyPass	/TopazSettings	http://BAC_server/TopazSettings
ProxyPassReverse	/TopazSettings	http://BAC_server/TopazSettings
ProxyPass	/opal	http://BAC_server/opal
ProxyPassReverse	/opal	http://BAC_server/opal
ProxyPass	/mam	http://BAC_server/mam
ProxyPassReverse	/mam	http://BAC_server/mam
ProxyPass	/mam_images	http://BAC_server/mam_images
ProxyPassReverse	/mam_images	http://BAC_server/mam_images
ProxyPass	/mam-collectors	http://BAC_server/mam-collectors
ProxyPassReverse	/mam-collectors	http://BAC_server/mam-collectors
ProxyPass	/mcrs	http://BAC_server/mcrs
ProxyPassReverse	/mcrs	http://BAC_server/mcrs
ProxyPass	/rumproxy	http://BAC_server/rumproxy
ProxyPassReverse	/rumproxy	http://BAC_server/rumproxy
ProxyPass	/bpi	http://BAC_server/bpi
ProxyPassReverse	/bpi	http://BAC_server/bpi
ProxyPass	/dashboard	http://BAC_server/dashboard
ProxyPassReverse	/dashboard	http://BAC_server/dashboard
ProxyPass	/utility_portlets	http://BAC_server/utility_portlets
ProxyPassReverse	/utility_portlets	http://BAC_server/utility_portlets
ProxyPass	/tv	http://BAC_server/tv
ProxyPassReverse	/tv	http://BAC_server/tv
ProxyPass	/tvb	http://BAC_server/tvb
ProxyPassReverse	/tvb	http://BAC_server/tvb

Note: This syntax also works on Apache 2.0.x versions.

Using a Reverse Proxy with a Distributed Server Installation

A reverse proxy can be used when the Gateway Server for Data Collectors and the Gateway Server for Application Users are installed on separate machines.

The use of a reverse proxy with a distributed server installation is illustrated in the diagram below:



This section includes the following topics:

Reverse Proxy Configuration

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

- communication that is redirected to the Gateway Server for Data Collectors.
- communication that is redirected to the Gateway Server for Application Users.

Reverse proxy HP Business Availability Center support should be configured differently in each of the following cases:

Scenario #	HP Business Availability Center Components Behind the Reverse Proxy
1	Data collectors (Business Process Monitor, Real User Monitor, SiteScope, Discovery Probe)
2	Application users
3	Data collectors and application users

Note:

- Different reverse proxies require different configuration syntaxes. For an example of an Apache 2.2.x reverse proxy configuration, see "Apache 2.2.x – Example Configuration" on page 60.
- 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 HP Business Availability Center Data Collectors

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/topaz/topaz_api/*	http://[Gateway Server for Data Collectors]/topaz/topaz_api/* https://[Gateway Server for Data Collectors]/topaz/topaz_api/*
/topaz/sitescope/*	http://[Gateway Server for Data Collectors]/topaz/sitescope/* https://[Gateway Server for Data Collectors/topaz/sitescope/*
/ext/*	http://[Gateway Server for Data Collectors]/ext/* https://[Gateway Server for Data Collectors]/ext/*
/mam-collectors/*	http://[Gateway Server for Data Collectors]/mam-collectors/* https://[Gateway Server for Data Collectors]/mam-collectors/*
/tv/*	http://[HP TransactionVision UI/Job Server]: 21000/tv/* https://[HP TransactionVision UI/Job Server]: 21001/tv/* **Note:** If you want to use AJP to enable the Reverse Proxy server to communicate with the HP TransactionVision UI/Job Server, use the following: http://[HP TransactionVision UI/Job Server]: 21002/tv/*
/axis2/*	http://[HP Business Availability Center Gateway Server]/axis2/* https://[HP Business Availability Center Gateway Server]/axis2/*

Support for HP Business Availability Center Application Users

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

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

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/HPBAC/*	http://[Gateway Server for Application users] /HPBAC/* https://[Gateway Serverfor Application users] /HPBAC/*
/hpbac/*	http://[Gateway Server for Application users] /hpbac/* https://[Gateway for Application users] /hpbac/*
/MercuryAM/*	http://[Gateway Server for Application users] /MercuryAM/* https://[Gateway Server for Application users] /MercuryAM/*
/mercuryam/*	http://[Gateway Server for Application users] /mercuryam/* https://[Gateway Server for Application users] /mercuryam/*
/topaz/*	http://[Gateway Server for Application users] /topaz/* https://[Gateway Server for Application users] /topaz/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/webinfra/*	http://[Gateway Server for Application users] /webinfra/* https://[Gateway Server for Application users] /webinfra/*
/filters/*	http://[Gateway Server for Application users] /filters/* https://[Gateway Server for Application users] /filters/*
/TopazSettings/*	http://[Gateway Server for Application users] /TopazSettings/* https://[Gateway Server for Application users] /TopazSettings/*
/opal/*	http://[Gateway Server for Application users] /opal/* https://[Gateway Server for Application users] /opal/*
/mam/*	http://[Gateway Server for Application users] /mam/* https://[Gateway Server for Application users] /mam/*
/mam_images/*	http://[Gateway Server for Application users] /mam_images/* https://[Gateway Server for Application users] /mam_images/*
/mcrs/*	http://[Gateway Server for Application users] /mcrs/* https://[Gateway Server for Application users] /mcrs/*

Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
/rumproxy/*	http://[Gateway Server for Application users] /rumproxy/* https://[Gateway Server for Application users] /rumproxy/*
/bpi/*	http://[Gateway Server for Application users] /bpi/* https://[Gateway Server for Application users] /bpi/*
/tv/*	http://[Gateway Server for Application users] /tv/* https://[Gateway Server for Application users] /tv/*
/tvb/*	http://[Gateway Server for Application users] /tvb/* https://[Gateway Server for Application users] /tvb/*

Support for Both HP Business Availability Center Data Collectors and Application Users

The following configuration is required on the reverse proxy if data collectors are connecting to the Gateway Server for Data Collectors and application users are connecting to the Gateway Server for Application Users via the same reverse proxy:

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

Priority	Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
1	/topaz/topaz_api/*	http://[Gateway Server for Data Collectors]/topaz/topaz_api/* https://[Gateway for Data Collectors]/topaz/topaz_api/*
1	/ext/*	http://[Gateway Server for Data Collectors]/ext/* https://[Gateway Server for Data Collectors]/ext/*
1	/mam-collectors/*	http://[Gateway Server for Data Collectors]/mam-collectors/* https://[Gateway Server for Data Collectors]/mam-collectors/*
2	/HPBAC/*	http://[Gateway Server for Application users] /HPBAC/* https://[Gateway Server for Application users] /HPBAC/*
2	/hpbac/*	http://[Gateway Server for Application users] /hpbac/* https://[Gateway Server for Application users] /hpbac/*

Priority	Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
2	/MercuryAM/*	http://[Gateway Server for Application users] /MercuryAM/* https://[Gateway Server for Application users] /MercuryAM/*
2	/mercuryam/*	http://[Gateway Server for Application users] /mercuryam/* https://[Gateway Server for Application users] /mercuryam/*
2	/topaz/*	http://[Gateway Server for Application users] /topaz/* https://[Gateway Server for Application users] /topaz/*
2	/webinfra/*	http://[Gateway Server for Application users] /webinfra/* https://[Gateway Server for Application users] /webinfra/*
2	/filters/*	http://[Gateway Server for Application users] /filters/* https://[Gateway Server for Application users] /filters/*
2	/TopazSettings/*	http://[Gateway Server for Application users] /TopazSettings/* https://[Gateway Server for Application users] /TopazSettings/*
2	/opal/*	http://[Gateway Server for Application users] /opal/* https://[Gateway Server for Application users] /opal/*

Priority	Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
2	/mam/*	http://[Gateway Server for Application users] /mam/* https://[Gateway Server for Application users] /mam/*
2	/mam_images/*	http://[Gateway Server for Application users] /mam_images/* https://[Gateway Server for Application users] /mam_images/*
2	/mcrs/*	http://[Gateway Server for Application users] /mcrs/* https://[Gateway Server for Application users] /mcrs/*
2	/rumproxy/*	http://[Gateway Server for Application users] /rumproxy/* https://[Gateway Server for Application users] /rumproxy/*
2	/bpi/*	http://[Gateway Server for Application users] /bpi/* https://[Gateway Server for Application users] /bpi/*
2	/tv/*	http://[Gateway Server for Application users] /tv/* https://[Gateway Server for Application users] /tv/*
2	/tvb/*	http://[Gateway Server for Application users] /tvb/* https://[Gateway Server for Application users] /tvb/*
2	/axis2/*	http://[HP Business Availability Center Gateway Server]/axis2/* https://[HP Business Availability Center Gateway Server]/axis2/*

The priority column on the left means that the requests in priority 1 must be handled before those in priority 2. 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 2.2.x – Example Configuration" on page 60.

HP Business Availability Center-Specific Configuration

In addition to configuring the reverse proxy to work with HP Business Availability Center, you must configure HP Business Availability Center to work with the reverse proxy.

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

To configure HP Business Availability Center 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 Centers Server URL** and **Default Virtual Core Services Server URL.** Verify that these parameters represent the URL of the machine (reverse proxy, load balancer, or other type of machine) used to access the Gateway Server.
   - **Local Virtual Centers Server URL** and **Local Virtual Core Services Server URL (optional).** If you must use more than one URL (the one defined for the **Default Virtual Core Server URL** parameter) to access the Gateway Server, define a **Local Virtual Core Services Server URL** for each machine through which you want to access the Gateway Server. If this parameter is set, the **Default Virtual Core Server URL** is overridden.
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 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 for Application Users. If the IP address of the reverse proxy sending the HTTP or HTTPS request is included in the list of IP addresses defined for this parameter, the URL returned to the client is either the **Default Virtual Centers Server URL** or the **Local Virtual Centers Server URL** (when defined). If the IP address of the reverse proxy sending the HTTP or HTTPS request is not included in the list of IP addresses defined for this parameter, the Gateway Server for Application Users returns the base URL that it receives in the HTTP or HTTPS request.

Note: If no IP addresses are defined for this parameter (the default option), HP Business Availability Center works in Generic Mode and the Gateway Server for Application users returns the **Default Virtual Centers Server URL** or the **Local Virtual Centers 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 Business Availability Center service on the HP Business Availability Center machine.

Note: Once you change the HP Business Availability Center 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 HP Business Availability Center to work in Generic Mode, all the HP Business Availability Center clients must access the HP Business Availability Center servers via the reverse proxy.

Apache 2.2.x – Example Configuration

Below is a sample configuration file that supports the use of an Apache 2.0.x reverse proxy in a case where data collectors are connecting to the Gateway Server for Data Collectors and application users are connecting to the Gateway Server for Application Users through the same reverse proxy.

Note: In the example below, the Gateway for Data Collectors Server DNS name is **BAC_DCGW** and the Gateway Server for Application Users DNS name is **BAC_USRGW**.

---

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://BAC_DCGW/ext
ProxyPassReverse   /ext                 http://BAC_DCGW/ext
ProxyPass          /topaz/topaz_api     http://BAC_DCGW/topaz/topaz_api
ProxyPassReverse   /topaz/topaz_api     http://BAC_DCGW/topaz/topaz_api
ProxyPass          /mam-collectors      http://BAC_DCGW/mam-collectors
ProxyPassReverse   /mam-collectors      http://BAC_DCGW/mam-collectors
ProxyPass          /mercuryam           http://BAC_USRGW/mercuryam
ProxyPassReverse   /mercuryam           http://BAC_USRGW/mercuryam
ProxyPass          /MercuryAM           http://BAC_USRGW/MercuryAM
```

ProxyPassReverse	/MercuryAM	http://BAC_USRGW/MercuryAM
ProxyPass	/hpbac	http://BAC_USRGW/hpbac
ProxyPassReverse	/hpbac	http://BAC_USRGW/hpbac
ProxyPass	/HPBAC	http://BAC_USRGW/HPBAC
ProxyPassReverse	/HPBAC	http://BAC_USRGW/HPBAC
ProxyPass	/topaz	http://BAC_USRGW/topaz
ProxyPassReverse	/topaz	http://BAC_USRGW/topaz
ProxyPass	/webinfra	http://BAC_USRGW/webinfra
ProxyPassReverse	/webinfra	http://BAC_USRGW/webinfra
ProxyPass	/filters	http://BAC_USRGW/filters
ProxyPassReverse	/filters	http://BAC_USRGW/filters
ProxyPass	/TopazSettings	http://BAC_USRGW/TopazSettings
ProxyPassReverse	/TopazSettings	http://BAC_USRGW/TopazSettings
ProxyPass	/opal	http://BAC_USRGW/opal
ProxyPassReverse	/opal	http://BAC_USRGW/opal
ProxyPass	/mam	http://BAC_USRGW/mam
ProxyPassReverse	/mam	http://BAC_USRGW/mam
ProxyPass	/mam_images	http://BAC_USRGW/mam_images
ProxyPassReverse	/mam_images	http://BAC_USRGW/mam_images
ProxyPass	/mcrs	http://BAC_USRGW/mcrs
ProxyPassReverse	/mcrs	http://BAC_USRGW/mcrs
ProxyPass	/rumproxy	http://BAC_USRGW/rumproxy
ProxyPassReverse	/rumproxy	http://BAC_USRGW/rumproxy
ProxyPass	/bpi	http://BAC_USRGW/bpi
ProxyPassReverse	/bpi	http://BAC_USRGW/bpi
ProxyPass	/tv	http://BAC_USRGW/tv
ProxyPassReverse	/tv	http://BAC_USRGW/tv
ProxyPass	/tvb	http://BAC_USRGW/tvb
ProxyPassReverse	/tvb	http://BAC_USRGW/tvb

4

Using SSL in HP Business Availability Center

This chapter provides introductory information on how to configure your HP Business Availability Center platform and data collectors to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

Introducing SSL Deployment in HP Business Availability Center

You need to configure SSL to work with HP Business Availability Center 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 an HP Business Availability Center server, SSL authenticates the server, and can also be configured to authenticate the client. Additionally, HP Business Availability Center establishes an encryption method and a unique key for the communication session.

The HP Business Availability Center platform fully supports the SSL 3.0 protocol. The SSL channel is configured on the HP Business Availability Center servers/clients as required.

Overview of SSL and HP Business Availability Center

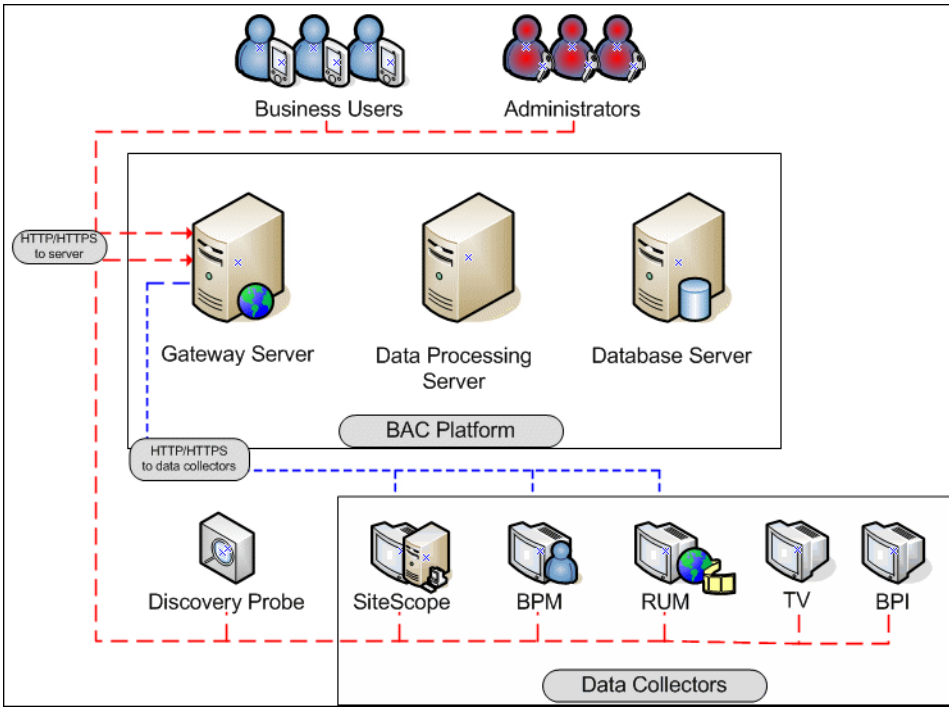
SSL provides HP Business Availability Center with the following:

- **Server authentication.** Provides authentication of the HP Business Availability Center server used for communication.
- **Client authentication.** Provides authentication of the client communicating with the HP Business Availability Center 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 HP Business Availability Center are illustrated in the following diagram:



Communication channels between HP Business Availability Center servers, data collectors, application users, and HP Business Availability Center platform components use various protocols on specific ports. For details, see "Port Usage" in the *HP Business Availability Center Deployment Guide* PDF.

Overview of Configuring SSL in HP Business Availability Center

The section "SSL-Supported Topologies in HP Business Availability Center" on page 70 discusses the various HP Business Availability Center-SSL topologies that are supported and provides links to each configuration step that is required.

Before proceeding with the configuration steps, ensure that:

- the HP Business Availability Center platform is operating as it is supposed to without an SSL channel.
- you read this chapter in its entirety before you begin performing the configuration.
- you define your secure communication requirements (use an SSL channel only where necessary).
- you consult the section "SSL-Supported Topologies in HP Business Availability Center" on page 70 to determine which topology is most suitable for the specific HP Business Availability Center-SSL architecture you are using.

Note: The configuration specified for each HP Business Availability Center 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 HP Business Availability Center:

- If you have configured a Reverse Proxy or Load Balancer server to work with your Business Availability Center 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 HP Business Availability Center" on page 29.

  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 HP Business Availability Center Gateway Server's JRE truststore.
- If you change your Web server to support SSL only (SSL required mode), the Web Guard must be configured to use SSL. For details on configuring the Web Guard, see "Configuring the Web Guard to Support SSL" on page 72.
- Business Process Monitors use certificates issued to the IP address of the Business Process Monitor Web server and not to the Web server name. For details on enabling SSL between the Gateway Server and Business Process Monitors, see "Configuring SSL from the Gateway Server to the Business Process Monitor Agent" on page 96.
- You can configure the JMX console to work with SSL. For details, see "Configuring the Application Server JMX Console to Work With SSL" on page 160, and "Configuring the JMX Console to Work With SSL in Other Processes" on page 161.

HP Business Availability Center Components Supporting SSL

You set an HP Business Availability Center server to support SSL by configuring the Web server installed on the HP Business Availability Center server to support SSL.

You configure HP Business Availability Center 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:

➤ "HP Business Availability Center Servers Supporting SSL" on page 69

➤ "HP Business Availability Center Clients Supporting SSL" on page 70

HP Business Availability Center Servers Supporting SSL

HP Business Availability Center 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

HP Business Availability Center Clients Supporting SSL

The following HP Business Availability Center clients support SSL communication with the HP Business Availability Center servers:

- **Browsers**. When used as HP Business Availability Center machine (when HP Business Availability Center 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 HP Business Availability Center machine (when HP Business Availability Center is installed on a single machine) or Gateway Server clients.

SSL-Supported Topologies in HP Business Availability Center

SSL optional topologies in HP Business Availability Center are divided into two main categories:

- Application users that communicate with HP Business Availability Center Gateway servers using SSL.
- Data collectors that communicate with HP Business Availability Center Gateway servers using SSL.

  Client authentication using a client-side certificate is optional with HP Business Availability Center clients.

Configuring HP Business Availability Center to Work with SSL

To configure an HP Business Availability Center Gateway Server (or an HP Business Availability Center 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
- change the URL for accessing HP Business Availability Center in Infrastructure Settings.

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 HP Business Availability Center 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 HP Business Availability Center, 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 HP Business Availability Center 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 HP Business Availability Center 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 Centers Server URL** and **Default Virtual Core Services Server URL.** 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 Centers Server URL** and **Local Virtual Core Services Server URL** (optional). If you must use more than one URL (the one defined for the **Default Virtual Core Server URL** parameter) to access the Gateway server machine, define a **Local Core Centers Server URL** for each machine through which you want to access the Gateway server machine. For example, https://my_specific_virtual_server.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 Centers Server URL** parameter is defined for a specific machine, this URL is used instead of the **Default Virtual Centers 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 Business Availability Center service on the HP Business Availability Center machine.

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

Configuring the Web Guard to Support SSL

Web Guard is a component in each HP Business Availability Center server that tracks the validity of the HP Business Availability Center components using HTTP/HTTPS. If you changed your Web server to support only SSL (SSL required mode), the Web Guard must be configured to use SSL.

To configure the Web Guard to use SSL, you must:

- "Set the Web Guard's Configuration File to Support SSL"
- "Set the Web Guard JRE to Support SSL"

Set the Web Guard's Configuration File to Support SSL

If your Web server supports only SSL, you must configure the Web Guard's configuration file to support SSL.

To configure the Web Guard's configuration file to support SSL:

1. Open the **<HP Business Availability Center server root directory>\conf\core\WebPlatform\webserver_guard.conf** file.
2. Add the following lines to the bottom of the file:

```
ssl=1
host_name=<host name>
webserver_port=<SSL port number>
```

Set the Web Guard JRE to Support SSL

The Web Guard uses HP Business Availability Center servers' JRE to support SSL.

The truststore, which contains the Certification Authorities (CAs) to be trusted by the Web Guard JRE, enables the Web Guard JRE on each HP Business Availability Center server to communicate with the Web server(s) requiring SSL. The truststore to be used in the procedure below is: **<HP Business Availability Center server root directory>\JRE\lib\security\cacerts**.

For details on how to set the Web Guard JRE to support SSL, see "Setting JRE to Trust a Client/Server Certificate" on page 78.

If you configure the Web server on the HP Business Availability Center server to require client authentication as well (an optional SSL handshake setting), the Web Guard JRE must be configured to send a client-side certificate when connecting to the Web server requiring SSL.

To enable the JRE to send a client-side certificate, you must add parameters to the relevant command line, as follows:

1. Open the file **<HP Business Availability Center root directory/bin/webServerGuard_run.bat**.
2. Locate the syntax, EXE_FILE=MercuryWSGuard.exe-Xrs

3 Add the following parameters:

- **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.

For details on enabling the JRE to send client-side certificate, see "Setting JRE to Use Client Side Authentication" on page 80.

Securing Communication Between an LDAP Server and HP Business Availability Center Server Over SSL

This section describes the procedure for securing communication between an LDAP server and an HP Business Availability Center server over SSL:

1 Import the LDAP trusted certificate to the HP Business Availability Center server truststore. For details on performing this task, see "Setting Java Runtime Environment to Work with Client/Server Certificates" on page 78.

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

2 Verify that communication between the LDAP server and the HP Business Availability Center 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).

Enabling SSL for the Login Process

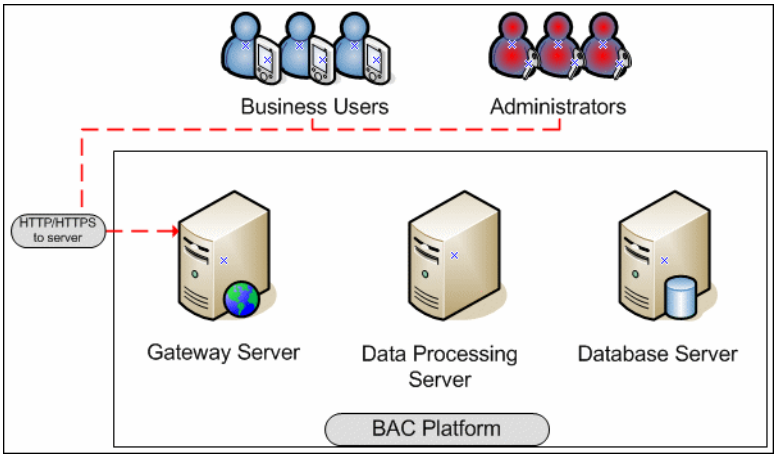
Even if you decide not to implement SSL in Business Availability Center, you can choose to enable SSL just for the login process to prevent the exposure of unencrypted user credentials.

To enable SSL just for the login process and not for the whole Business Availability Center deployment:

1. Enable SSL on the web server itself.
2. On the Business Availability Center Gateway, open **<Business Availability Center installation dir>/AppServer/site.war/WEB-INF/web.xml**.
3. Set **IsHTTPSForce** attribute to "true".
4. Restart the Business Availability Center Gateway.

Configuring SSL from the 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

HP Business Availability Center 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 Business Availability Center's JVM for communicating with the data collectors over SSL. For example on each Gateway server, run the following two commands:

```
Cd <BSM  JRE>/bin keytool -import -trustcacerts -alias <certificate name> -
keystore ..\lib\security\cacerts -file c:\ca.cer
Cd <BSM  JRE64>/bin keytool -import -trustcacerts -alias <certificate name> -
keystore ..\lib\security\cacerts -file c:\ca.cer
```

Setting Java Runtime Environment to Work with Client/Server Certificates

To set the Java Runtime Environment (JRE) to work with client/server certificates, you must set the JRE to trust a client/server certificate and to use client/server-side authentication.

This section includes the following topics:

➤ "Setting JRE to Trust a Client/Server Certificate" on page 78

➤ "Setting JRE to Use Client Side Authentication" on page 80

Setting JRE to Trust a Client/Server 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, you must 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 certificate alias name> -file
<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:\jre150\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 will use its keystore to look for the certificate and the corresponding private key. To support the sending of certificates by JRE, you must 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** that 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 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.

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

keystorePass="**your password**"

keystoreType="**jks**" **or** "**pkcs12**"

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

5 Restart Tomcat.

Configuring Tomcat to Trust Client-side Certificates

You must set the Tomcat to trust the client-side certificate sent by HP Business Availability Center. 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 HP Business Availability Center into this **cacerts** file. For details, see "Setting JRE to Trust a Client/Server Certificate" on page 78.

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 **<HP Business Availability Center 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 <**HP Business Availability Center 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 HP Business Availability Center.

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 HP Business Availability Center processes.

To configure the JMX console to work with SSL in other HP Business Availability Center processes:

1 Open the following files:

- **\<HP Business Availability Center root directory>\conf\spring\jmx-html-adaptor-spring.xml**
- **\<HP Business Availability Center 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 79.

5

Using SSL with SiteScope

This chapter describes how to configure your HP Business Availability Center platform with the SiteScope data collector to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see “Using SSL in HP Business Availability Center” on page 63.

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 page 90.
- Configure the Gateway Server's Java Runtime Environment (JRE) to trust the SiteScope certificate. For details, see page 90.
- Set HP Business Availability Center to use HTTPS to connect to the SiteScope monitor. For details, see page 91.

  In addition, if the SiteScope Web server has been configured to force client-side authentication, you must add a client-side certificate to HP Business Availability Center's keystore. For details, see page 91.

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 82.

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

You 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 Client/Server Certificate" on page 78.

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

Configuring HP Business Availability Center 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 HP Business Availability Center's Keystore

If Tomcat has been configured to force client-side authentication, you must add a client-side certificate that can be sent from HP Business Availability Center to SiteScope.

To add a client-side certificate:

1 Set the HP Business Availability Center Java Virtual Machine (JVM) to support client-side authentication. For details, see "Setting Java Runtime Environment to Work with Client/Server Certificates" on page 78.

Note: You must define the keystore used by HP Business Availability Center as described in "Setting Java Runtime Environment to Work with Client/Server Certificates" on page 78.

---

2 Configure Tomcat to trust HP Business Availability Center's client-side certificate. For details on performing this task, see "Configuring Tomcat to Trust Client-side Certificates" on page 83.

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 HP Business Availability Center 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 79.

To configure SiteScope for SSL using HP Business Availability Center Monitor Administration:

1. In the HP Business Availability Center 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 describes how to configure your HP Business Availability Center platform with the Business Process Monitor data collector to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see "Using SSL in HP Business Availability Center" on page 63.

Configuring SSL from the Gateway Server to the Business Process Monitor 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 page 96.
- Configure HP Business Availability Center to use HTTPS to connect to the Business Process Monitor. For details, see page 100.
- Configure the Gateway Server's Java Runtime Environment (JRE) to trust the Business Process Monitor certificate. For details, see page 100.

Configuring a Business Process Monitor 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 HP Business Availability Center to Use HTTPS to Connect to a Business Process Monitor

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 Business Process Monitor 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 Client/Server Certificate" on page 78.

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

Configuring SSL from the Business Process Monitor 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 101

➤ "Configuring an SSL Client-Side Certificate." on page 102

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.

To configure the Business Process Monitor 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 **/HPBAC**.

---

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 an HP Business Availability Center certificate into the following Business Process Monitor truststore file:

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

to ensure that HP Business Availability Center 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 Business Process Monitor 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 describes how to configure your HP Business Availability Center platform with the Real User Monitor data collector to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see "Using SSL in HP Business Availability Center" on page 63.

Configuring SSL from the Gateway Server to the Real User Monitor 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.
- Configure the Gateway Server's Java Runtime Environment (JRE) to trust the Real User Monitor certificate.
- Configure HP Business Availability Center to use HTTPS to connect to Real User Monitor.

Configuring the Real User Monitor 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 82.

Configuring the Gateway Server's JRE to Trust the Real User Monitor 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 Client/Server Certificate" on page 78.

You must import the Real User Monitor server-side certificate into the truststore file used by HP Business Availability Center. The truststore file is **%HP Business Availability Center_root%\JRE\lib\security\cacerts** and it is a JKS type truststore.

Configuring the Real User Monitor URL in HP Business Availability Center for HTTPS

You must configure the URL of the Real User Monitor engine defined in HP Business Availability Center Monitor Administration to include the HTTPS protocol.

To configure the Real User Monitor URL defined in HP Business Availability Center Monitor Administration for HTTPS:

1. In HP Business Availability Center 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 Real User Monitor 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 Real User Monitor Truststore" on page 106

➤ "Configuring a Connection to the Gateway Server Using SSL" on page 107

➤ "Configuring an SSL Client-Side Certificate" on page 107

Note: For details on configuring Java Runtime Environment to work with client/server certificates when using SSL with the Real User Monitor Snapshot applet, see "Setting Java Runtime Environment to Work with Client/Server Certificates" on page 78.

Importing the certificate/CA certificate Used by the Gateway Server(s) into the Real User Monitor 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 79.

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 **BAC 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 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** checkboxes.

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 **BAC 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 your HP Business Availability Center platform with TransactionVision to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see “Using SSL in HP Business Availability Center” on page 63.

Securing Communication between TransactionVision Components

The following sections describe how to configure secure communication among the TransactionVision components. In particular the built-in SonicMQ messaging infrastructure and the TransactionVision UI/Job Server.

For information about configuration of security for other third-party products in the TransactionVision environment, such as IBM's WebSphere MQ, Tibco EMS, or the external SonicMQ messaging middleware, see that product documentation.

Overview of SSL Configuration

The TransactionVision infrastructure consists of four primary components that must each be configured to enable secure communication:

- TransactionVision Sensors/Agents
- TransactionVision SonicMQ Server
- TransactionVision Analyzer
- TransactionVision UI/Job Server

The general process to enable secure communication is summarized below. Details about each step are provided in the sections that follow.

Step 1: Generate required certificates for encrypting traffic

The TransactionVision Analyzer, UI/Job Server, and SonicMQ Server each requires a private key to be created. If two or more of these components reside on the same hostname, they can share the same private key. Otherwise a unique key must be generated for each host that one of these components run on. See “Step 1: Generating a Keystore” on page 113.

Step 2: Configure the TransactionVision SonicMQ Server

Configure the TransactionVision SonicMQ Server to use a certificate generated in step 1. See “Step 2: Configure the TransactionVision SonicMQ Server” on page 114.

Step 3: Configure the Analyzer

a If using the HTTPS Configuration messages service (for use with NonStop TMF Sensors), configure the certificate generated in step 1.

b To communicate with the TransactionVision SonicMQ Server, configure the Analyzer to use the certificate set up in step 2.

See “Step 3: Configure the Analyzer Server for SSL” on page 115.

Step 4: Configure the UI/Job Server

a To support incoming SSL requests, configure the TransactionVision UI/Job Server with the certificate generated in step 1.

b To support outgoing SSL communication to BAC, configure the TransactionVision UI/Job Server to use a Business Availability Center public certificate and set it to use https protocol to communicate with Business Availability Center.

See "Step 4: Configuring SSL for the TransactionVision UI/Job Server" on page 117.

Step 5: Configure the Sensors/Agents

a If communicating directly with the TransactionVision SonicMQ Server, configure Sensors/Agents with the certificate set up in step 2.

b If using the HTTPS Configuration message service (for NonStop TMF Sensors), configure the Sensor to use certificate configured in Step 3a.

See "Step 5: Configuring Sensors/Agents for SSL Communication" on page 121.

Configuring SSL for TransactionVision

If the TransactionVision environment includes sensitive data being sent between the components, you can enable SSL for each communication path.

Before you can configure Secure Sockets Layer (SSL) communication, you must generate a certificate for use in encrypting the communication. A certificate consists of a private key (accessible only by the server), and a public key that is sent to clients in order to encrypt traffic. In order for the client to ensure that it is communicating with who it expects to, when it receives the public key from the server, it must establish whether this public key is trusted. A key is trusted if the key, or the certificate authority signing the key, belongs to a set of trusted entities that the client has been configured to trust.

In setting up TransactionVision components, it may be helpful to keep in mind that setting up the TransactionVision Analyzer (Configuration Message Service), UI/Job Server, and SonicMQ Server to accept SSL communication requires configuring both a private and public key. Setting up a communication component with the following clients requires ensuring the server's public key is trusted by the client:

- Java Agents/sensors (to SonicMQ server)
- TransactionVision Analyzer(to SonicMQ server)
- Browsers connecting to TransactionVision UI
- TransactionVision UI/Job server connecting to HP Business Availability Center.

The Analyzer acts as both a server for BEA Tuxedo and NonStop TMF Sensors requesting configuration messages, and as a client communicating messages to the SonicMQ server. Both of these modes can be configured to communicate using SSL technology.

The Sensors use SonicMQ to communicate event data for reading by the Analyzer and can be configured to use SSL for this data.

The TransactionVision UI/Job Server acts as both as server for incoming HTTP requests, and it itself also makes calls to the HP Business Availability Center Gateway server to send data. Either of these modes can also be configured to use SSL.

The Analyzer, SonicMQ Server and the TransactionVision UI/Job Server can all be configured to share the same keystore, if they all reside on the same host. If they reside on different hosts they require a separate key to be generated.

The procedure that follows uses the **keytool** Java utility to generate example certificates and keystores. See http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html for more information.

Step 1: Generating a Keystore

TransactionVision by default ships with and is configured to use a temporary certificate for using SSL. The temporary certificate is intended to act as an example about how and where the configuration is typically set up. This key cannot be used in a real deployment.

To generate a keystore, follow these steps:

1 Generate a keystore with the following command:

```
keytool -genkey -alias tvserverkey -keyalg RSA -storeType PKCS12 -keystore
TVHOME/serverkey.p12
```

The command prompts you for information regarding the creation of the key. If you use a password other than the default "changeit", be sure to record it as you it will be needed to access this key.

Note:

- While keytool does not enforce it, SonicMQ requires that the two-letter country code be no longer than 2 characters. Therefore specify a 1 or 2 character country code only.
- When generating a key the CN of the certificate should be set to the fully qualified hostname on which the Analyzer or UI/Job Server runs. In order to accomplish this, when keytool prompts for "your first and last name", the fully qualified Analyzer hostname should be used.
- If generating a key for the UI/Job Server, and if you have it running on a separate machine from the Analyzer, a separate key using the fully qualified hostname of the machine the UI/Job Server is running on would be required.

---

2 Export this servers certificate's public key:

```
Keytool -export -alias tvserverkey -file serverkey.cer -storeType PKCS12 -
keystore TVHOME/serverkey.p12
```

This exports the key to a file called **serverkey.cer**. Any client attempting to access use the SSL connection (Analyzer connecting to SonicMQ via SSL, agents connecting to SonicMQ and/or the Analyzer), needs to be configured to trust this certificate.

The BEA Tuxedo Sensor requires the server certificate's public key be in PEM format. To export the key in this format use the following command:

```
keytool -export -rfc -alias tvserverkey -file serverkey.pem -storeType PKCS12 -
keystore TVHOME/serverkey.pem
```

Step 2: Configure the TransactionVision SonicMQ Server

Use the Progress SonicMQ Management Console to configure SonicMQ for SSL communication.

1. In the Management Console, navigate to the Acceptors item of your broker.

   Under there you should see an SSL based Acceptor and a https based acceptor. The Tuxedo and NonStop TMF Sensors make use of the https based acceptor. If you are not using those agents, then configuring the https direct acceptor us not needed.

2. Open the properties of the SSL or HTTPS direct acceptors and click on the SSL tab. Define the key stores as follows.

   Format: PKCS12

Note: In the Generating a Keystore section, the PKCS12 format type is used in the example to generate keys. While Sonic can support the other keystore format (JKS) generated by keytool, it requires being configured differently. If you do chose to use a JKS keystore type will need to set your broker to use a jsseSSLImpl provider and configure it accordingly. Please see the SonicMQ documentation for more information on this.

Path Name: TVHOME/serverkey.p12

Password: enter the password for the key/keystore.

For additional topics related to securing SonicMQ, see the *Progress SonicMQ Deployment Guide*.

Step 3: Configure the Analyzer Server for SSL

Analyzer Communication with SonicMQ

In order for the Analyzer to communicate with Sonic via SSL, copy the certificate (serverkey.cer, in the example above) to <TVHOME>\Sonic\MQ7.5\certs\CA.

The Analyzer needs to be restarted for this to take effect.

Analyzer Configuration Message Service

Enabling HTTPS access to the Configuration Message Service (used by Tuxedo/Non-Stop Agents), requires setting a number of configuration parameters in TVHOME/config/services/Analyzer.properties.

Under HTTPS SSL Configuration Service Parameters you will see the related parameters.

Example contents of Analyzer.properties:

```
##########################################
# HTTPS SSL Configuration Service Parameters
##########################################

# Enable https configuration service , DEFAULT: false
configuration_server_ssl_enabled=false

# HTTPS port, DEFAULT: 21103
# configuration_server_ssl_port=21103

# Keystore location, DEFAULT(not set):  do not override default java keystore
# configuration_server_ssl_keystore_location=

# Keystore password, DEFAULT: changeit
# configuration_server_ssl_keystore_password=

# Key password, DEFAULT: defaults to keystore password if not specified
# configuration_server_ssl_key_password=
```

```
# Keystore type - JKS or PKCS12, DEFAULT: JKS
# configuration_server_ssl_keystore_type=
```

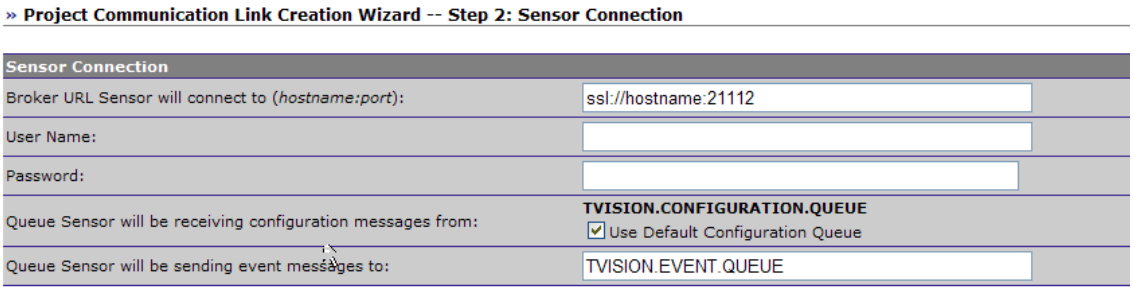
In order to enable the HTTPS server, set configuration_server_ssl_enabled to true. In addition, at minimum, the configuration_server_ssl_keystore_location should be set to the keystore location, and configuration_server_ssl_keystore_type need to be set.

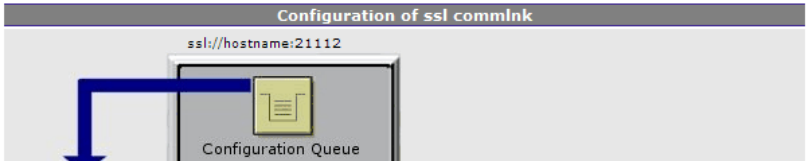
Continuing with the above example, configuration_server_ssl_keystore_location would be set to TVHOME/serverkey.p12. Set the configuration_server_ssl_keystore_password according to the value you set the password to on key creation. configuration_server_ssl_keystore_type should be set to PKCS12.

The Analyzer needs to be restarted for this to take effect.

Configuring Communication Links to Use SSL

To configure the communication link to use SSL, you need to specify the SSL protocol when setting the broker host URL in the project's communication link definition as follows:





Changing the HTTP commlink similarly involves changing the Sensor Connection URL to be https://hostname:21113/tv_http.

Step 4: Configuring SSL for the TransactionVision UI/Job Server

There are two components to consider in securing the TransactionVision UI/Job Server to use SSL. As with the Analyzer the TransactionVision UI/Job Serer operates both as a server for accepting Web requests as well client making calls to various HP Business Availability Center components. There is configuring the TransactionVision UI/Job Server to allow for incoming SSL connections. And there is configuring SSL on outbound connections to the HP Business Availability Center server.

Supporting HTTPS requests on the TransactionVision UI/Job Server

The TransactionVision UI/Job Server can either reside on the same machine as the HP Business Availability Center Gateway server, or on a separate system. In the scenario where the TransactionVision server resides on the HP Business Availability Center Gateway server machine, there is no additional configuration needed to enable SSL. In this case HP Business Availability Center will do all the forwarding to the TransactionVision server via its proxy server. So only HP Business Availability Center needs to be configured to use SSL as described in the HP Business Availability Center documentation.

If the TransactionVision server is on a separate machine, some additional steps need to be done to configure SSL. In this case a certificate must be installed and configured on the TransactionVision UI/Job Server. See “Step 1: Generating a Keystore” on page 113. By default Tomcat will use the default keystore of the Java Runtime Environment.

This can be configured in Tomcat by the following steps:

1. Modify <TVISION-HOME>\apache-tomcat\conf\server.xml, look for the section labeled "Define a SSL HTTP/1.1 Connector"

   The "Connector" entry underneath this line is commented out by default.

   ```
   <!-- Define a SSL HTTP/1.1 Connector on port 21001

   <Connector port="21001" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" />

   -->
   ```

   becomes:

   ```
   <!-- Define a SSL HTTP/1.1 Connector on port 21001 -->

   <Connector port="21001" maxHttpHeaderSize="8192" maxThreads="150"
   minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100"  scheme="https"
   secure="true" clientAuth="false" sslProtocol="TLS" />
   ```

   If the TransactionVision UI/Job Server, the Analyzer and TransactionVision's sonic server are all installed on the same machine, it is possible for all three components to share the same keystore. If this is desired, the keystoreFile, keystorePass, keystoreType attributes of the <Connector> element in the server.xml need to be modified to point to the common keystore. (See “Step 3: Configure the Analyzer Server for SSL” on page 115.)

   If you wish to further customize the location and type of the keystore, follow steps 2-4.

2. Add the following attribute to the connector element:

   keystoreFile="myKeyStore" where myKeyStore is the JKS or PKCS12 file that contains the Web server certificate and a corresponding private key

   To create a certificate for tomcat, see Generating Keystore section above.

3. If the keystore password is different from the default password changeit, you must configure it accordingly in the connector element: keystorePass="your password"

4. If you are using a PKCS12 file, you must set the keystoreType attribute to PKCS12
5. Restart Tomcat.

   If a certificate has been digitally signed as a result of submitting a Certificate Signing Request to a trusted certificate authority a browser should be able to automatically be able to authenticate the validity of the key. If this is not the case for the certificate, for example if it is self signed, when first accessing some TransactionVision pages prompts may appear to accept the certificate on a temporary or permanent basis. In order for the SSL connection to work, the certificate must be accepted at least on a temporary basis.

Enabling HTTPS for Requests Made by the TransactionVision UI/Job Server Back to HP Business Availability Center

The TransactionVision UI/Job Server communicates with the HP Business Availability Center Gateway Server to publish a number of different types of data. CMDB entries are published from TransactionVision to HP Business Availability Center, TransactionVision Transaction statistics information is published to HP Business Availability Center by the TransactionVision BAC Sample job, and TransactionVision communicates with the User Management component of HP Business Availability Center for determining user authorization and publishing resources created in TransactionVision for User Management (projects, reports).

To configure TransactionVision to trust HP Business Availability Center's certificate, you must import the HP Business Availability Center servers public certificate into the trust store used by the TransactionVision UI/Job Server.

Configuring TransactionVision to communicate with HP Business Availability Center via SSL requires the following steps.

1. Obtain a copy of the certificate used by the Web Server on the HP Business Availability Center Gateway Server.
2. Import HP Business Availability Center's certificate into TransactionVision's TrustStore.

```
keytool -import -trustcacerts -alias bacAlias -keystore
TVHOME\jre\lib\security\cacerts -file baccert.cer
```

Note: If your HP TransactionVision UI URL setting is configured using **https:**// in the HP Business Availability Center Infrastructure Settings Manager, you must also access HP Business Availability Center using **https:**//. Using **http:**// to log into HP Business Availability Center in this case produces mixed mode content errors on each page.

Configuring TransactionVision UI/Job Server-HP Business Availability Center Integration Settings to Enable SSL

After the TransactionVision UI/Job Server has been configured to either connect to Business Availability Center using SSL, or to serve Web pages using SSL as described in the preceding sections, you need to register and configure the SSL URLs that are now to be used.

Registration of these SSL URLs can be accomplished by running TVisionSetupInfo on the TransactionVision UI/Job Server and/or Analyzer host. As part of the setup, this tool will ask if you wish to register TransactionVision with Business Availability Center. It will prompt for the hosts the Business Availability Center server and TransactionVision server reside on, whether to use SSL or not, and at the end register TransactionVision and Business Availability Center to use the URLs specified.

Example of output from TvisionSetupInfo after all input has been specified:

```
The HP Business Availability Center server at https://bacGWserver:80 will be
configured with:
TransactionVision Web Server:          https://TVWebServer:21001
Please review the above settings a verify that they are correct.
Proceed with registration to HP Business Availability Center? [y] :
```

Note: These settings can also be configured manually. From the TransactionVision Administration > HP Business Availability Center Settings page, you can change the URL, protocol and port that TransactionVision uses to communicate to Business Availability Center. (Although this requires the TransactionVision UI to be running first before this page can be accessed, if the TransactionVision UI is not available then TVisionSetupInfo is the only way to configure this setting). The setting of the URL that Business Availability Center uses to communicate with TransactionVision, can be found under the Infrastructure Settings manager. Select Foundations:Integrations with other Applications, TransactionVision settings can be found under the HP TransactionVision section.

Step 5: Configuring Sensors/Agents for SSL Communication

To configure Java Agents to use SSL:

1. Modify probe_home/etc/TV.properties to add rsa_ssl.jar to appTransportLoadPath as follows:

   ```
   appTransportLoadPath=mfcontext.jar;sonic_Client.jar;sonic_Client_ext.jar;sonic
   _XA.jar;rsa_ssl.jar;jms.jar
   ```

2. Modify JAVA_AGENT_HOME/config/ SensorConfiguration.xml to change SonicMQTransport BrokerURL from tcp://yourhost:21111 to ssl://yourlhost:21112 as follows:

   ```
   <SonicMQTransport>
    <BrokerURL>
    ssl:// yourlhost:21112
   </BrokerURL>
   …..
   </SonicMQTransport>
   ```

By default Java Agents configured to talk to the TransactionVision Message bus via SSL look at the TVHOME/config/sensor directory for the certificates to trust. So you would need to have the certificate (serverkey.cer, in the example above) copied to the <TVHOME>/config/sensor directory on any machine with a Java Agents installed.

Note:

- This default directory location can be changed by setting the defaultTransport.ssl_cert_dir property located in the probe_home/etc/TV.properties file. The path here can be either a relative path or a full path if directory location exists outside of the TransactionVision install. If you do enter a custom path, it is important to note that only forward slashes '/' should be used when entering the directory path, even on windows.
- If the application that is being monitored by a Java Agent is itself using SSL enabled Sonic to communicate with queues, some additional items need to be considered. Because of a limitation in SonicMQ, it is not possible to configure two separate components running within the same process to use a differing directory location for where certificate files are lookup. Thus, both the Agent and the application itself would need to have any trusted certificates located in the same location. If this is the scenario, you would need to change the defaultTransport.ssl_cert_dir property located in the probe_home/etc/TV.properties file to point to where the application is already configured to look for its certificates and additionally copy the TransactionVision certificate to that directory.

When defining the communication link in the TransactionVision UI/Job Server, use the URL ssl://hostname:21112 instead of tcp://hostname:21111 when setting the BrokerUrl fields.

To configure the Tuxedo sensor to use SSL:

1. To retrieve configuration information from the Analyzer, edit the Tuxedo sensor property file.

   This can be found in the directory "<TVHOME>/tuxedo/config/TuxedoSensor.properties" on the host on which the Tuxedo sensor is installed.

2. In this property file, change the "transport" field to specify the HTTP over SSL URL for the Analyzer configuration service. By default, this URL is "https://myhost:21103".

3. To configure the Tuxedo Sensor to send events to the Analyzer using SSL, edit the communication link used by the Tuxedo sensor. In the TransactionVision application in Business Availability Center, choose Event Connection > Sensor Connection and edit the "Connection URL" field to specify the HTTP over SSL URL for the SonicMQ HTTP Direct for JMS Acceptor. By default, this URL is "https://myhost:21114".

   Tuxedo Sensors configured to use SSL need to have a copy of the SSL certificate in PEM format ("serverkey.pem" in the "Generating a keystore" example above). This must be copied to the "<TVHOME>/tuxedo/certs" directory on any machine on which the Tuxedo Sensor is installed.

   Additional properties controlling the Tuxedo Sensor's behavior with respect to SSL are available and documented in the Tuxedo sensor properties file "TuxedoSensor.properties".

To configure the .NET agent to use SSL:

Steps 1-19 step you through the process of installing the certificate. The final step involves editing an entry in the probe_config.xml file to enable SSL on the transport.

1. Copy the certificate from the TransactionVision SonicMQ Server to the machine where the .NET agent is installed.

2. From the Windows taskbar, select Start > Run.

3. Run the Microsoft Management Console by typing mmc, and then clicking OK.

4. On the Microsoft Management Console menu, select File > Add/Remove Snap-in to display the Add/Remove Snap-in dialog.
5. Click Add on the Add/Remove Snap-in dialog.
6. Select Certificates from the Available Standalone Snap-in list and click Add.
7. In the Certificates Snap-in dialog box select Computer account, and click Next.
8. In the Select Computer dialog box select Local Computer: (the computer this console is running on), and then click Finish.

   The NT User account under which the monitored process is running needs to have its Certificate Store configured to be able to verify the certificate which the Sonic MQ server is using for the secure communication. For an ASP.NET application running using "NETWORK SERVICE" (this is the default) credentials the Certificate Store is that of the "Local Computer". If this has been changed to be a different account, the certificate should be imported under that user, not Local Computer.
9. Click Close on the Add Standalone Snap-in.
10. Click OK on the Add/Remove Snap-in dialog.
11. On the Microsoft Management Console expand the listing for Certificates (Local Computer) in the left pane of the Console Root dialog.
12. Under Certificates (Local Computer), expand Trusted Root Certification Authorities.
13. Under Trusted Root Certification Authorities, right-click Certificates and select All Tasks > Import to start the Certificate Import Wizard.
14. Click Next to move past the Welcome dialog box of the Certificate Import Wizard.
15. Click Browse to navigate to directory where you have copied the exported certificate file. (serverkey.cer)
16. Click Next to import the file.
17. Click Next to accept the default Certificate Store location of "Trusted Root Certification Authorities."
18. Click Finish on Completing the Certificate Import Wizard.
19. Click OK on the Certificate Import Wizard confirmation dialog.

20 Modify probe_config.xml and change the broker URL for the <transport> element that configures the transport the .NET agent uses. For example:

```
<transport type="sonicmq" connectionstring="broker=ssl://brokerhost;
port=21112; user=; password=;
configurationqueue=TVISION.CONFIGURATION.QUEUE"/> Note the broker
has been prefixed with "ssl://".
```

For SSL and the WMQ Sensors on Windows or UNIX:

If the WMQ sensor is monitoring a WMQ application making client connections, the WMQ sensor cannot open a connection independent of the type of connection the WMQ application itself makes. Thus if the application is making non-secured WMQ calls, the WMQ sensor is limited to that. If on the other hand the application itself is using an SSL connection, the WMQ sensor would use that secured connection.

If the WMQ sensor is monitoring a WMQ application making server connections, the only place where SSL would come into play is if there is a remote channel between the application's queue manager and a dedicated TV queue manager. This would be purely configured in WebSphere MQ - the application, or Sensor would not need to be aware of it. If the analyzer is also using a server WMQ connection to retrieve events, it similarly would not need SSL enabled. If the analyzer were making a client WMQ connection to retrieve the messages through a SSL enabled channel, then it would need to be configured accordingly (see "Configuring 3rd-Party Messaging Middleware to Support SSL for Analyzer and/or Java Agents" on page 126).

For SSL and the WMQ and CICS Sensors on z/OS:

Because the z/OS sensors all only use server connections, as mentioned above, SSL configuration is not needed. Again, the only place where SSL would come into play is if there is a remote channel between the application's queue manager and a dedicated TV queue manager. This would be purely configured in WebSphere MQ - the application, or Sensor would not need to be aware of it. If the analyzer reading these messages is also using a server WMQ connection to retrieve events, it similarly would not need SSL enabled. If the analyzer were making a client WMQ connection to retrieve the messages through a SSL enabled channel, then it would need to be configured accordingly (see "Configuring 3rd-Party Messaging Middleware to Support SSL for Analyzer and/or Java Agents" on page 126).

Configuring 3rd-Party Messaging Middleware to Support SSL for Analyzer and/or Java Agents

Support of SSL for connecting to a messaging middleware provider other than that shipped with TransactionVision is not supported out of the box, but can be accomplished in many cases by manual configuration. Some general guidance is provided here on how to accomplish this.

If you are not using the embedded SonicMQ messaging middleware that is bundled with TransactionVision, there are some manual steps you may have to perform. See the documentation of your messaging middleware provider for information on the general configuration of the server and clients. Typically, to configure the clients (the Analyzer or Agents in this case) requires providing vendor-specific information on the Java command line indicating where trusted certificates can be found. To add any applicable Java arguments to the Analyzer startup you can modify the service_jvm_flags property in TVHOME/config/services/Analyer.properties. To add properties to a Java Agent, modify the tvProperties field found in PROBEHOME/etc/TV.properties files.

Importing the Certificate from an SSL Enabled Business Availability Center System

If your Business Availability Center server has SSL enabled, the certificate obtained from the Business Availability Center server needs to be imported into the cacerts file on the TV analyzer system.

On Windows, the cacerts file is located at:

```
%JAVA_HOME%\lib\security\cacerts
```

or

```
%JAVA_HOME%\jre\lib\security\cacerts
```

On UNIX:

```
$JAVA_HOME/lib/security/cacerts
```

or

```
$JAVA_HOME/jre/lib/security/cacerts
```

Following import of the certificate, the Analyzer needs to be restarted.

Enabling SSL Communication for Events Reported to BPI

If BPI actions are defined in your classification rules, the Analyzer will send events to the BPI Engine when those corresponding transactions occur. These events are sent to BPI via the SonicMQ server. By default, this communication is not secured. To use a secure connection for sending BPI events, perform the following steps:

1. Go to the HP Business Process Insight page.
2. Change the JMS Connection Factory Name from its default, BPIQueueFactory, to BPISSLQueueFactory.

   Both these JNDI objects are defined by default within the TransactionVision SonicMQ server.

   After this step, BPI events will be sent with SSL enabled. You must also have set up the Analyzer environment to allow for SSL communication. See Configuring Analyzer Server for SSL communication section for the needed steps.

Enabling Authentication in TransactionVision SonicMQ

These are the steps to enable authentication in SonicMQ. In addition to securing messages through encryption using SSL, you can secure the SonicMQ Acceptors to require authentication from the Sensors and the Analyzer.

The following steps summarize how to define users and enable authentication on the broker. After performing these steps, define the communication link used by the Sensors and the Analyzer to use the user names specified here.

Similarly, for configuring RUM to use the Analyzer, the user name and password need to be configured by running TVisionSetupInfo or by manually changing the Settings Manager field in the Business Availability Center UI.

1 Shutdown the nanny using the command:

<TVISION_HOME>\bin\SupervisorStop.bat (Windows)

<TVISION_HOME>/bin/run_topaz stop (UNIX)

2 Start the SonicMQ domain manager using the script:

<TVISION_HOME>\Sonic\MQ7.5\bin\startdm.bat (Windows) or
<TVISION_HOME>/Sonic/MQ7.5/bin/startdm.sh (UNIX)

3 Start the SonicMQ broker using the script:

<TVISION_HOME>\Sonic\MQ7.5\bin\startbroker.bat (Windows) or
<TVISION_HOME>/Sonic/MQ7.5/bin/startbroker.sh (UNIX)

4 Start the Management Console using the script:

<TVISION_HOME>\Sonic\MQ7.5\bin\startmc.bat (Windows) or
<TVISION_HOME>/Sonic/MQ7.5/bin/startmc.sh (UNIX)

5 Turn on security in the broker, which is typically named the same as the hostname (without the domain name):

a Click on the Configure tab near the top of the SonicMQ Management Console Window.

b Click on the first '+' button named 'Brokers' to expand the list of brokers configured in SonicMQ.

c Select the Broker named the same as the hostname and right-click to view the dropdown menu; select 'Properties' from the menu.

d On the Edit Broker Properties Window, enable Security by checking the checkbox next to 'Security' in the Security section.

e Set the broker password by pressing the 'Set Broker Password...' button in the Security section on the window and entering the password.

Note: By default, the Default Authentication Domain and Default Authentication Policy is selected. You can find more information on creating and configuring Authentication Domains and Policies in chapter 12 of the SonicMQ Configuration and Management Guide (<TVISION_HOME>\Sonic\Docs7.5\mq_config_manager.pdf).

---

6 Create new users and set the same password for the new users as described in step 2.

7 Exit the management console.

8 Stop the SonicMQ domain manager using the script:

<TVISION_HOME>\Sonic\MQ7.5\bin\stopdm.bat (Windows) or
<TVISION_HOME/Sonic/MQ7.5/bin/stopdm.sh (UNIX)

9 Stop the SonicMQ broker using the script:

<TVISION_HOME>\Sonic\MQ7.5\bin\stopbroker.bat (Windows) or
<TVISION_HOME/Sonic/MQ7.5/bin/stopbroker.sh (UNIX)

10 cd to <SONICMQ_HOME>, which is the same as <TVISION_HOME>\Sonic\MQ7.5.

11 Edit <broker name>\db.ini and set ENABLE_SECURITY=true

12 Run the command: bin\dbtool /f <broker name>\db.ini /d a

13 Run the command: bin\dbtool /f <broker name>\db.ini /c a

14 Restart the nanny using the command:

<TVISION_HOME>\bin\SupervisorStart.bat (Windows) or
<TVISION_HOME/bin/run_topaz start (UNIX)

9

Using SSL with the DDM Probe

This chapter includes:

Concepts

Tasks

Using SSL with the DDP Probe Overview

This chapter describes how to configure your HP Business Availability Center platform with the Discovery and Dependency Mapping Probe and Staging Data Replicator to support communication using the Secure Sockets Layer (SSL) channel.

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see “Using SSL in HP Business Availability Center” in the *HP Business Availability Center Hardening Guide* PDF.

Enable SSL Between BAC Running an Internal UCMDB and the DDM Probe with Mutual Authentication

You can set up authentication for both the DDM Probe and BAC running an internal UCMDB, with certificates. The certificate for each side is sent and authenticated before the connection is established.

Important: The following method of enabling SSL on the DDM Probe replaces the procedure for basic authentication, which is deprecated. For details on basic authentication, see "Enable SSL on the DDM Probe with Basic Authentication" on page 416.

This section includes the following topics:

Prerequisites

Set up the BAC server with an internal UCMDB, running in SSL. Client certificates are required.

Enable Mutual Certificate Authentication

If the certificate used by the HP Business Availability Center Web server is issued by a well-known Certificate Authority (CA), it is most likely that you do not have to perform the following procedure. To validate trust, try connecting to the Web server using SSL and check whether the certificate is already trusted.

During authentication, BAC running an internal UCMDB sends its certificate to the DDM Probe client machine, and the DDM Probe sends its certificate to BAC running an internal UCMDB.

1. Download the required certificate, encoded in base-64, and save it as **c:\cacert.cer**:
   - ➤ If BAC is using a CA-signed certificate: download the CA certificate.
   - ➤ If BAC is using a self-signed certificate: download the BAC self-signed certificate.
2. Import the Certificate Authority certificate into the DDM Java truststore by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -import -trustcacerts -alias ddmTrustedCA -
keystore ..\lib\security\cacerts -file c:\cacert.cer
```

   - ➤ Type the following keystore password: **changeit**
   - ➤ When asked **Trust this certificate?**, enter **yes**.
3. Create a keystore by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -genkey -keyalg RSA -alias ddmkey -
keystore
C:\hp\DDM\DiscoveryProbe\root\lib\security\client.keystore
```

   - ➤ Choose your password and enter your details.

     Important: Enter the full hostname for **first and last name**.
   - ➤ When asked, **Is CN=... correct?** type **yes**.
   - ➤ Press ENTER to set the same password for the key.
4. Create a certificate request for CA to sign by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -certreq -alias ddmkey -file c:\ddm.csr  -
keystore
C:\hp\DDM\DiscoveryProbe\root\lib\security\client.keystore
```

   - ➤ Enter the keystore password.
5. Submit the **c:\ddm.csr** file to your Certificate Authority and acquire a signed client certificate in base-64 encoding.

6 Import the CA certificate into the keystore by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -import -alias ddmTrustedCA -file
c:\cacert.cer -keystore
C:\hp\DDM\DiscoveryProbe\root\lib\security\client.keystore
```

➤ Enter the keystore password and when asked **Trust this certificate?**, enter **yes**.

7 Import the client certificate into the keystore by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -import -alias ddmkey -file
c:\<SIGNED_CERT> -keystore
C:\hp\DDM\DiscoveryProbe\root\lib\security\client.keystore
```

Note: <**SIGNED_CERT**> is the full path to the certificate acquired in step 5 on page 133 above.

➤ Make sure that the output message is **Certificate** reply **was installed in keystore**.

8 List the contents of the keystore by running the following command:

```
C:\hp\DDM\DiscoveryProbe\jre\bin>keytool -list -keystore
C:\hp\DDM\DiscoveryProbe\root\lib\security\client.keystore
```

➤ Enter the keystore password.

➤ Verify that the output includes both **keyEntry** and **trustedCertEntry**.

9 Change the **ssl.properties** file, located in the **C:\HP\DDM\DiscoveryProbe\root\lib\security** folder:

- Update the keystore and truststore file names to point to the files you created previously:

```
# Path to Keystore and Truststore files
javax.net.ssl.keyStore=C:\\hp\\DDM\\DiscoveryProbe\\root\\lib\\security\\client.keyst
ore
javax.net.ssl.trustStore=C:\\hp\\DDM\\DiscoveryProbe\\jre\\lib\\security\\cacerts
```

  (Note the double backslashes.)

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

    You may have to log in with a user name and password.
  - Locate the **Type=MainProbe** service and click the link to open the JMX MBEAN View page.
  - Locate the **getEncryptedKeyPassword** operation.
  - Enter your keystore or truststore password in the **Key Password** field and click **getEncryptedKeyPassword**.
  - Open the **ssl.properties** file in the following folder: **C:\hp\DDM\DiscoveryProbe\root\lib\security**.
  - Copy and paste the encrypted password (numbers separated by commas, for example, 1,2,3,4,5) into the relevant keystore or truststore line of the **ssl.properties** file.
  - Save the file.

10 Update the C:\hp\DDM\DiscoveryProbe\root\lib\collectors\DiscoveryProbe.properties file:

- Change the **appilog.agent.probe.protocol** parameter to **HTTPS**.
- Make sure the **serverPortHttps** value is **443**.

11 Restart the DDM Probe.

Configure SSL from the Discovery Probe to the Gateway Server

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

To configure the Discovery Probe to connect to the Gateway Server using SSL:

1. Prerequisite: Configure HP Business Availability Center to use SSL.
2. Prerequisite: Install the Discovery Probe. During installation, enter the name of the HP Business Availability Center Gateway server to which the Probe must report results.
3. If you are working with the Certificate Authority, download the current Certificate Authority certificate to your DDM Probe server. Save it to a file, for example, C:\ca.cer.
4. Import this certificate into the DDM Probe JVM: **C:\hp\DDM\DiscoveryProbe\jre\bin** with the following values:

   ```
   keytool -import -trustcacerts -alias <your alias> -keystore ..\lib\security\cacerts -file <file path and name>
   ```

5. Enter the password and click **Yes** to confirm.
6. Set the connection parameters in the DDM Probe.
   - ➤ Open the file **%discovery root%\root\lib\collectors\DiscoveryProbe.properties**.
   - ➤ Configure the URL of the HP Business Availability Center server:

     ```
     serverName = <HP Business Availability Center Gateway server domain name>
     ```

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

➤ Configure the port number to use for HTTPS:

```
# Ports used for HTTP/s traffic
#serverPort = 80
serverPortHttps = 443
```

➤ Set the schema to be used by the Agent to HTTPS:

```
# Can be either HTTP or HTTPS
appilog.agent.probe.protocol = HTTPS
```

➤ Set the name of the HP Business Availability Center server:

```
# Name of the Server machine to which this probe reports
serverName = <server name either of the reverse proxy or the Gateway server>
```

7 Restart the Discovery Probe.

10

Using SSL with the Staging Data Replicator

This chapter describes how to configure your HP Business Availability Center platform with the Staging Data Replicator to support communication using the Secure Sockets Layer (SSL) channel.

This chapter includes:

For introductory and general information on configuring HP Business Availability Center and its data collectors to support SSL, see "Using SSL in HP Business Availability Center" on page 63.

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 an HP Business Availability Center 7.x machine to an HP Business Availability Center 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__&message_subject=topaz_report/samples&request_timeout=30&force_keep_alive=true&send_gd=true"/>

To configure the SDR to trust the HP Business Availability Center certificate:

1. Obtain a copy of the certificate used by the Web Server on the HP Business Availability Center Gateway Server. This file must be a DER encoded binary X.509 (.CER) file.
2. Import HP Business Availability Center's certificate into SDR's KeyStore. For details, see "To import a required certificate to the truststore:" on page 79.
   - Configure SDR to use KeyStore, and add additional options in the file <**BAC 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=<**keystoere path**>

       -Dnet.ssl.trustStorePassword=passphrase

11

Using Basic Authentication in HP Business Availability Center

This chapter describes how to configure your HP Business Availability Center platform to support authentication using the basic authentication protocol.

This chapter includes:

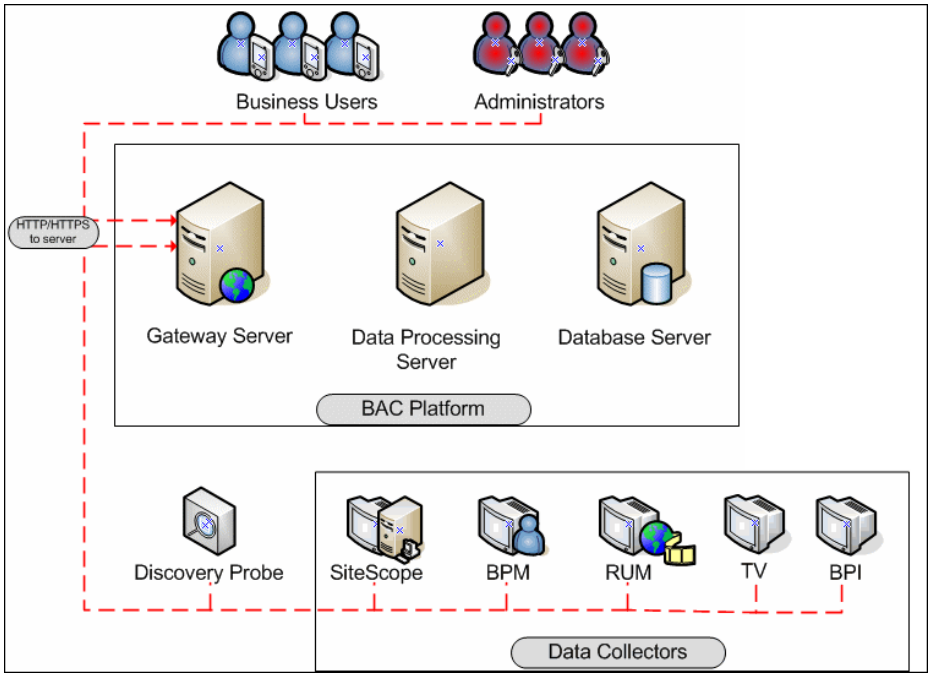
Introducing Basic Authentication Deployment in HP Business Availability Center

The HP Business Availability Center platform fully supports the basic authentication schema, which provides HP Business Availability Center with the ability to authenticate a client communicating with an HP Business Availability Center 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 HP Business Availability Center platform to support SSL communication, see "Using SSL in HP Business Availability Center" on page 63.

Possible basic authentication channels in HP Business Availability Center are illustrated in the following diagram:



Overview of Configuring Basic Authentication in HP Business Availability Center

Before proceeding with the configuration steps, ensure that:

- the HP Business Availability Center 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 HP Business Availability Center server is also relevant for a single machine installation, in which the Gateway Server and Data Processing Server both reside on the same machine.

HP Business Availability Center Components Supporting Basic Authentication

You set an HP Business Availability Center server to support basic authentication by enabling basic authentication support for the Web server installed on the HP Business Availability Center server, and for the Web Guard component on the HP Business Availability Center server.

You configure HP Business Availability Center 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 145
- "HP Business Availability Center Clients Supporting Basic Authentication" on page 145

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.

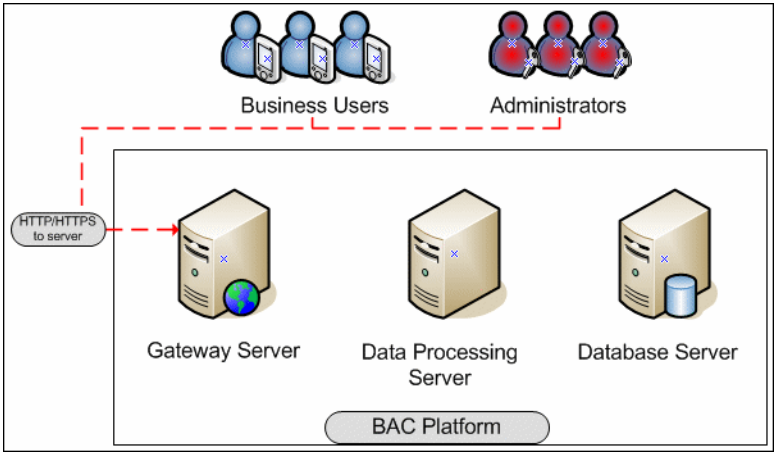
HP Business Availability Center Clients Supporting Basic Authentication

The following HP Business Availability Center clients support basic authentication communication with the HP Business Availability Center servers:

- **Browsers.** When used as HP Business Availability Center machine (when HP Business Availability Center 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 HP Business Availability Center machine (when HP Business Availability Center 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 an HP Business Availability Center 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 147.
- "Basic Authentication Configuration for the Application Users" on page 150.

Basic Authentication Configuration for the Gateway Server

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

Important: Some JREs request an additional username and password confirmation when accessing applets imbedded in HP Business Availability Center, such as the Dashboard Topology Map, System Health, and IT Universe Manager.

This section contains the following topics:

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 an HP Business Availability Center 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 HP Business Availability Center 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 HP Business Availability Center have the required NTFS permissions required for the Users connecting to HP Business Availability Center.

Enable Basic Authentication Support for the Gateway Server Web Guard

Web Guard is a component in each HP Business Availability Center server that tracks the validity of the HP Business Availability Center components using HTTP/HTTPS. If you configured your Web server to use basic authentication, the Web Guard must also be configured to use basic authentication.

To configure the Web Guard to use basic authentication:

1. Double-click the **<HP Business Availability Center root directory>\tools\setsiteauthentication\bin\setsiteauthentication.exe** utility.
2. Select the **Using basic authentication** check box.
3. Enter the following 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
4. Copy the file **<HP Business Availability Center root directory>\tools\setsiteauthentication\bin\SiteSecurity.dat** to **<HP Business Availability Center root directory>\dat.**

Note for Solaris users: Perform steps 1-3 in a Windows environment and then copy **SiteSecurity.dat** to **<HP Business Availability Center root directory>/dat** on your Solaris Gateway Server machine.

---

5. Restart the HP Business Availability Center service on the Gateway Server.

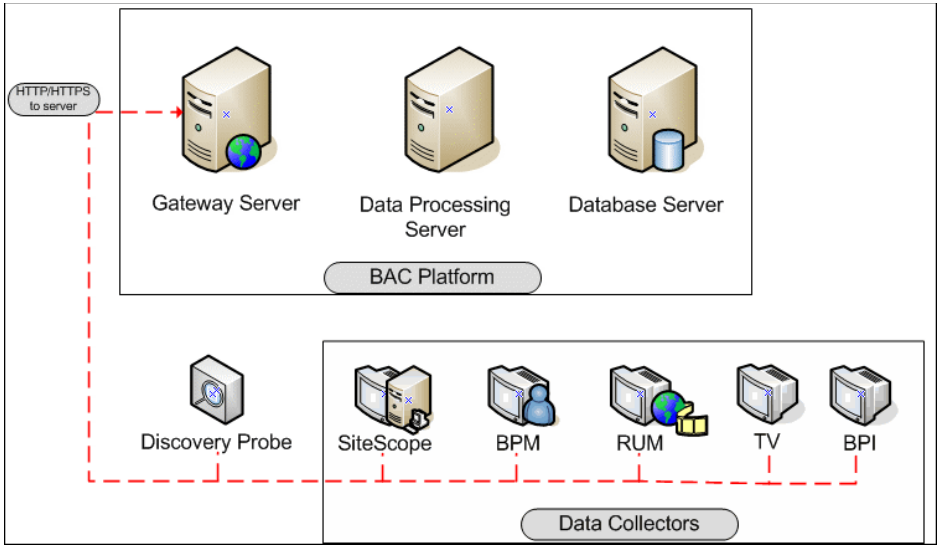
Basic Authentication Configuration for the Application Users

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

To connect as an application user to an HP Business Availability Center server that requires basic authentication, it is only necessary for you to know the credentials of the user permitted to log in to the HP Business Availability Center 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 HP Business Availability Center 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 HP Business Availability Center data collectors connecting to it using HTTP/S.



This section describes the following topics:

➤ "Basic Authentication Configuration for the Gateway Server" on page 152.

➤ "Basic Authentication Configuration for the Data Collectors" on page 154.

Basic Authentication Configuration for the Gateway Server

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

This section contains the following topics:

➤ "Enable Basic Authentication Support on the Web Server" on page 152.

➤ "Enable Basic Authentication Support for the Gateway Server Web Guard" on page 153.

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 an HP Business Availability Center 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 HP Business Availability Center 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 HP Business Availability Center has the required NTFS permissions required for the Users connecting to HP Business Availability Center.

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

Enable Basic Authentication Support for the Gateway Server Web Guard

Web Guard is a component in each HP Business Availability Center server that tracks the validity of the HP Business Availability Center components using HTTP/HTTPS. If you configured your Web server to use basic authentication, the Web Guard must also be configured to use basic authentication.

To configure the Web Guard to use basic authentication:

1. Double-click the **<HP Business Availability Center root directory>\tools\setsiteauthentication\bin\setsiteauthentication.exe** utility.
2. Select the **Using basic authentication** check box.
3. Enter the following 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.

4 Copy the file **<HP Business Availability Center root directory>\tools\setsiteauthentication\bin\SiteSecurity.dat** to **<HP Business Availability Center root directory>\dat**.

Note for Solaris users: Perform steps 1-3 in a Windows environment and then copy the file **SiteSecurity.dat** to **<HP Business Availability Center root directory>/dat** on your Solaris Gateway Server machine.

---

5 Restart the HP Business Availability Center service on the Gateway Server.

Basic Authentication Configuration for the Data Collectors

This section provides instructions for configuring the following HP Business Availability Center data collectors to support basic authentication:

➤ "Business Process Monitor" on page 155

➤ "SiteScope" on page 156

➤ "Real User Monitor" on page 157

➤ "Discovery Probe" on page 157

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 HP Business Availability Center 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 HP Business Availability Center 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 HP Business Availability Center>**
   - **appilog.agent.Probe.BasicAuth.User = <username used to log into HP Business Availability Center>**
   - **appilog.agent.Probe.BasicAuth.Pwd = <password used to log into HP Business Availability Center>**

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 HP Business Availability Center 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

You harden the JMX console by changing the default JMX user's password. The default user's credentials are: Login name = **admin** Password = **admin**

To change the JMX or MX4J JMX password:

1. Stop the HP Business Availability Center Gateway or Data Processing server.
2. Run the appropriate file, depending on the operating system in use, on either the Gateway or Data Processing server:

Operating System	File Name
Windows	<HP Business Availability Center root directory>\tools\jmx\changeCredentials.bat
Solaris	<HP Business Availability Center root directory>\tools\jmx\changeCredentials.sh

The Change Password dialog box opens, where you enter and confirm your new password. The password change is registered and encrypted in the following files, located on either the Gateway or Data Processing server:

- **\<HP Business Availability Center root directory>\EJBContainer\server\mercury\conf\props\jmx-console-users.properties**

  The syntax in this file appears as **username=password**.

- **\<HP Business Availability Center root directory>\conf\jmxsecurity.txt**

  The syntax in this file appears as **username password**.

3. Restart HP Business Availability Center.

Note: The login name cannot be changed.

For details on configuring the JMX Console to work with SSL, see "Configuring the Application Server JMX Console to Work With SSL" on page 160, and "Configuring the JMX Console to Work With SSL in Other Processes" on page 161.

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 <**HP Business Availability Center 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 <**HP Business Availability Center 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 HP Business Availability Center.

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 HP Business Availability Center processes.

To configure the JMX console to work with SSL in other HP Business Availability Center processes:

1 Open the following files:

- **\<HP Business Availability Center root directory>\conf\spring\jmx-html-adaptor-spring.xml**
- **\<HP Business Availability Center 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 79.

Index

T

W