HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.50

Hardening Guide

Document Number: BACHAR7.50/01
Document Release Date: February 2009
Software Release Date: May 2008

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.

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

© Copyright 2005 - 2008 Hewlett-Packard Development Company, L.P.

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

This manual's title page 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

Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:
http://h20229.www2.hp.com/passport-registration.html

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 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 57 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 27.

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 19.

➤ **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 27.

➤ **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 57.

➤ **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 95.

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 "Bus Communication and 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:

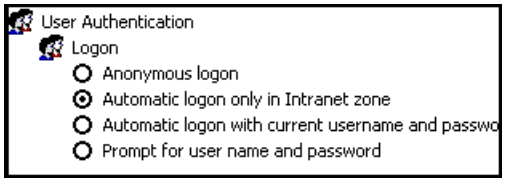
1. In the Internet Explorer Web browser, select **Tools** > **Internet Options**, and click the **Advanced** tab.
2. Scroll down to the **Java (Sun)** section. Select **Use Java2**. Any Java2 version v1.5.x or v1.6x is acceptable.

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.

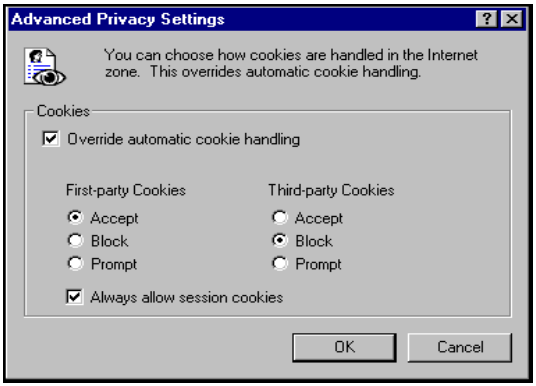
2 In the Settings pane, you can configure cookies in one of two ways:

- ➤ 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 22.

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

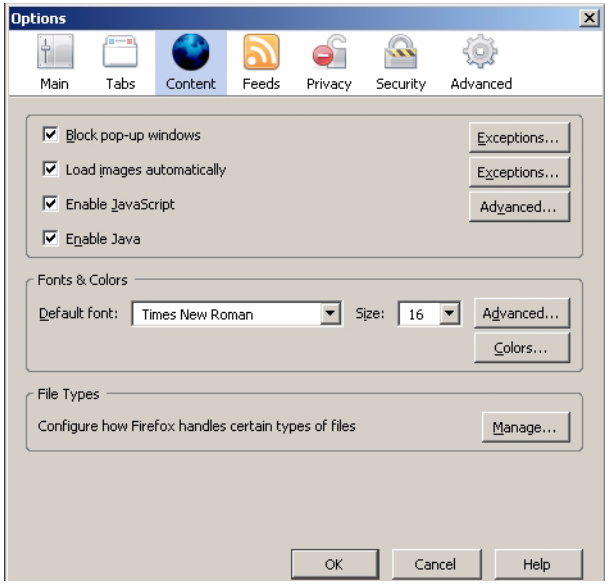
You must configure the FireFox Web browser to connect to HP Business Availability Center.

This section includes the following topics:

To configure Java scripting and applets:

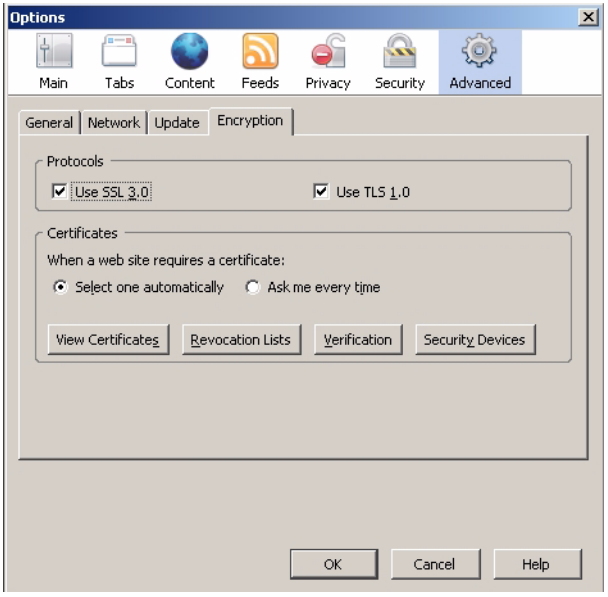
1 In the FireFox Web browser, select **Tools** > **Options** and click the **Content** button.

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**.



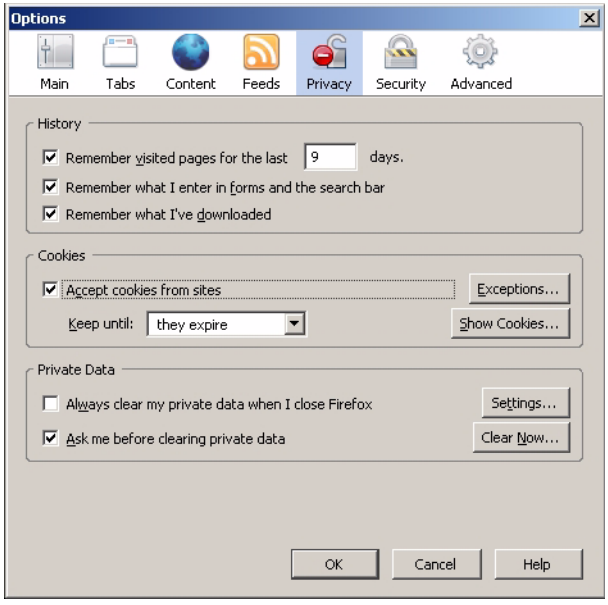
5 Click **OK** to save your settings and close the Options dialog box.

To configure cookies:

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

2 Click the **Privacy** button.

3 Select the **Accept cookies from sites** checkbox.



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.

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 server(s).

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 32.

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" below
- "Generic Mode" on page 31

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.

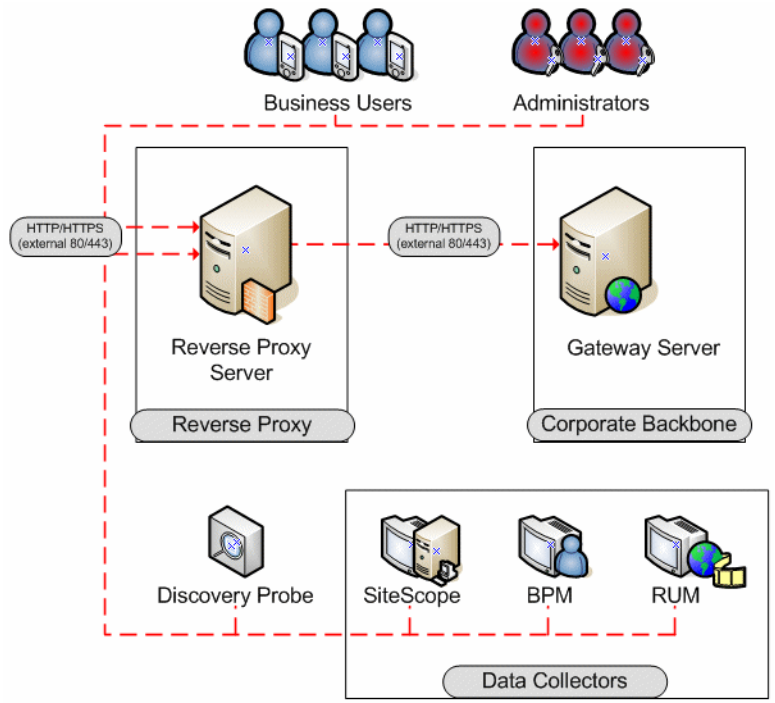
If you are working in this mode, each time an HTTP or HTTPS request causes the HP Business Availability Center application to calculate a base URL, the base URL is replaced with the value defined for either the **Default Virtual Centers Server URL** or the **Local Virtual Centers Server URL** (when defined).

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 42.

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**.

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

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/*

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

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/*

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

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

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 42.

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.

- **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
```

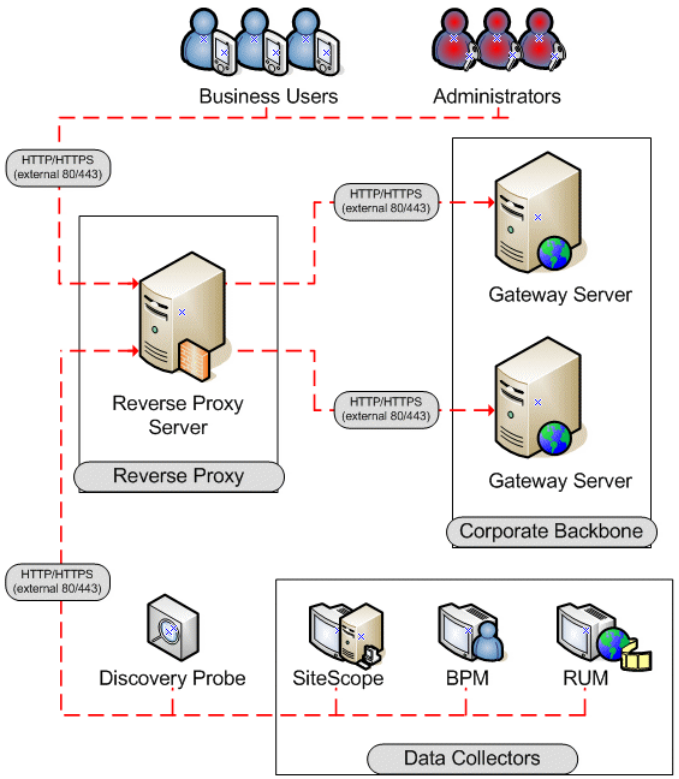
ProxyPass	/HPBAC	http://BAC_server/HPBAC
ProxyPassReverse	/HPBAC	http://BAC_server/HPBAC
ProxyPass	/topaz	http://BAC_server/topaz
ProxyPassReverse	/topaz	http://BAC_server/topaz
ProxyPass	/ext	http://BAC_server/ext
ProxyPassReverse	/ext	http://BAC_server/ext
ProxyPass	/webinfra	http://BAC_server/webinfra
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

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 54.

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/*	http://[Gateway for Data Collectors]/topaz/* https://[Gateway for Data Collectors]/topaz/*
/ext/*	http://[Gateway for Data Collectors]/ext/* https://[Gateway for Data Collectors]/ext/*
/mam-collectors/*	http://[Gateway for Data Collectors]/mam-collectors/* https://[Gateway for Data Collectors]/mam-collectors/*

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://[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/*
/webinfra/*	http://[HP Business Availability Center server] /webinfra/* https://[HP Business Availability Center server] /webinfra/*

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

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 for Data Collectors Server and application users are connecting to the Gateway for Application Users Server via the same reverse proxy:

Note: In an LW-SSO environment, the [Gateway for Application Users Server] 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 for Data Collectors Server]/topaz/topaz_api/* https://[Gateway for Data Collectors Server]/topaz/topaz_api/*
1	/ext/*	http://[Gateway for Data Collectors Server]/ext/* https://[Gateway for Data Collectors]/ext/*
1	/mam-collectors/*	http://[Gateway for Data Collectors Server]/mam-collectors/* https://[Gateway for Data Collectors Server]/mam-collectors/*
2	/HPBAC/*	http://[Gateway for Application Users Server] /HPBAC/* https://[Gateway for Application Users Server] /HPBAC/*
2	/hpbac/*	http://[Gateway for Application Users Server] /hpbac/* https://[Gateway for Application Users Server] /hpbac/*

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

Priority	Requests for... on the Reverse Proxy Server	Proxy Request to be Served by:
2	/mam/*	http://[Gateway for Application Users Server]/mam/* https://[Gateway for Application Users Server]/mam/*
2	/mam_images/*	http://[Gateway for Application Users Server]/mam_images/* https://[Gateway for Application Users Server]/mam_images/*
2	/mcrs/*	http://[Gateway for Application Users Server]/mcrs/* https://[Gateway for Application Users Server]/mcrs/*
2	/rumproxy/*	http://[Gateway for Application Users Server]/rumproxy/* https://[Gateway for Application Users Server]/rumproxy/*

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 54.

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 for Application Users Server 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 for Application Users Server 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

4

Using SSL in HP Business Availability Center

This chapter describes how to configure your HP Business Availability Center platform 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 a client or data collector accesses HP Business Availability Center server, SSL authenticates the server and the client, and establishes an encryption method and a unique certificate for the communication session.

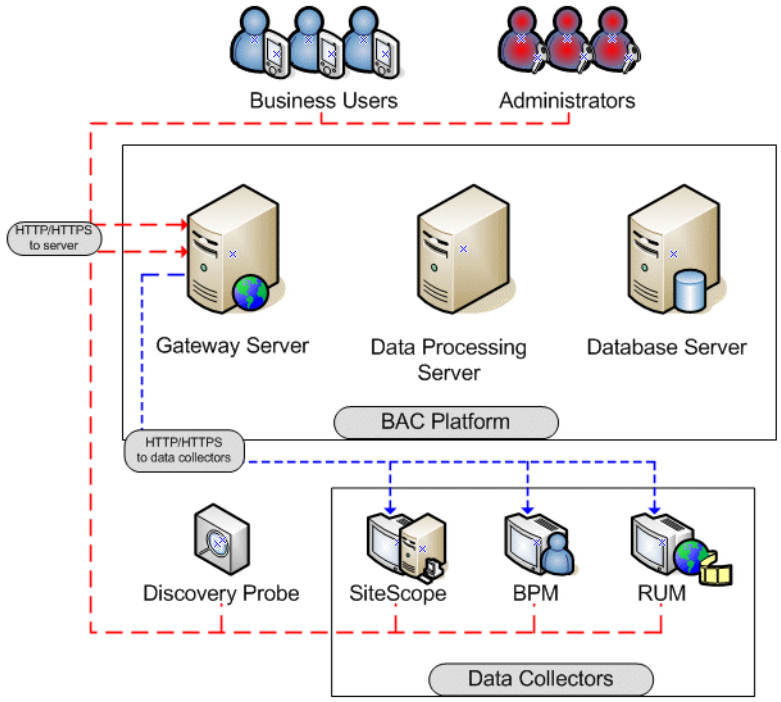
The HP Business Availability Center platform fully supports the SSL version 3.0 protocol. The SSL channel is configured on the HP Business Availability Center servers/clients as required.

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 a user or a data collector such as Business Process Monitor.
- **Encrypted channel.** Encrypts the communication between the client and the server using a variety of ciphers.
- **Data integrity.** Helps ensure that the information sent by one side over SSL is the same information received by the other side.

Possible SSL channels in 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 "Bus Communication and 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 64 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 (only use an SSL channel where necessary)
- you consult the section "SSL-Supported Topologies in HP Business Availability Center" on page 64 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 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 27.

  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 88.

- 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 "Enabling SSL From the Gateway Server to the Business Process Monitor Agent" on page 71.

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.

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

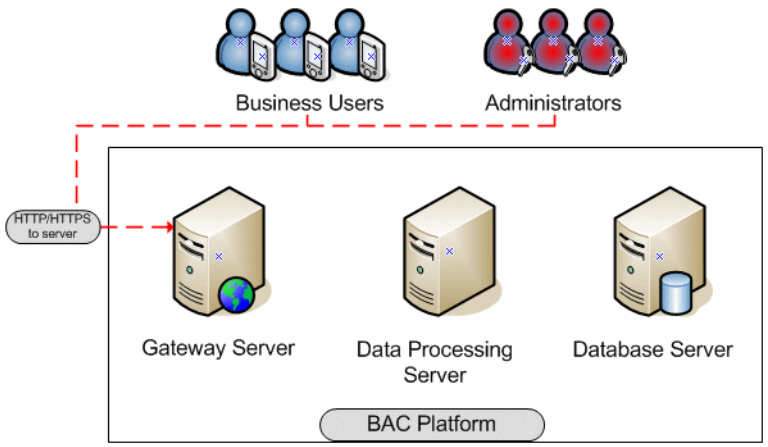
SSL optional topologies in HP Business Availability Center version 6.2 and later are divided into two main categories:

- 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 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.



This section includes the following topics:

- "SSL Configuration for the Gateway Server" below
- "SSL Configuration for the Application Users" on page 66

SSL Configuration for the Gateway Server

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.

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.

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.

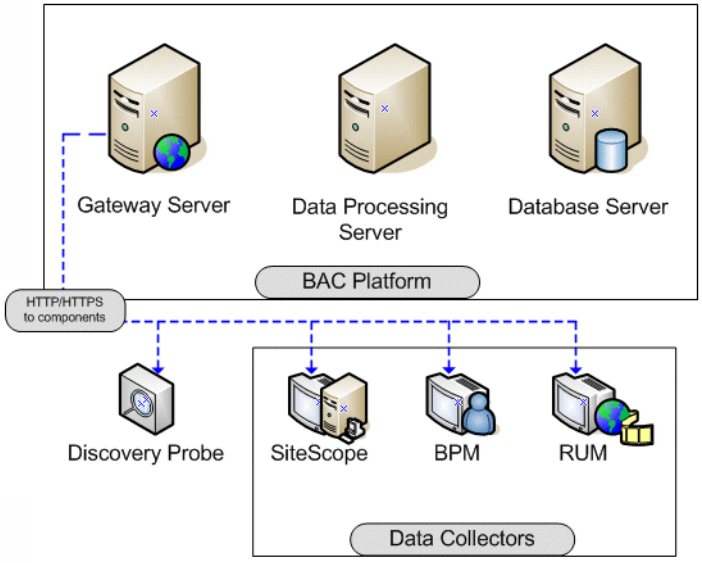
To import a certificate to the truststore used by the browser:

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.

   After importing a certificate to the truststore used by the browser, you must also import it to the truststore used by the Java Runtime Environment (JRE). For details, see "Setting Java Runtime Environment to Work With Client/Server Certificates" on page 89.

Configuring SSL From the Gateway Server to Data Collectors

The instructions in this section describe how to enable SSL from the Gateway Server to Business Process Monitor, SiteScope, Real User Monitor, and Discovery Probe data collectors.



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

This section includes the following topics:

Enabling SSL From the Gateway Server to SiteScope

To enable the Gateway Server to communicate with SiteScope using SSL, you must configure the SiteScope monitor to support SSL, configure the Gateway Server's Java Runtime Environment (JRE) to trust the SiteScope certificate, and set HP Business Availability Center to use HTTPS to connect to the SiteScope monitor. 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.

Configuring the SiteScope Web server to support SSL

To enable a SiteScope monitor to communicate using SSL, you must configure Tomcat 5.0.x to support HTTPS. For detailed information on configuring Tomcat 5.0.x, refer to http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

To configure Tomcat 5.0.x to support HTTPS:

1 Uncomment the following connector element:

```
<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 SiteScope SSL communications, change the port number in the connector element accordingly.

---

2 Add the following attribute to the connector element:

keystoreFile="**myKeyStore**"

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

Note: You can create a self-signed certificate for testing, using the keytool.exe utility, as described in http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

---

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 Restart Tomcat.

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 the SiteScope Web server. For details, see "Setting JRE to Trust a Client/Server Certificate" on page 89.

You must import the SiteScope 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.

Tip: You can use the keytool.exe utility to import the SiteScope server-side certificate.

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 the SiteScope Web server has been configured to force client-side authentication you must add a client-side certificate that can be sent to SiteScope, to HP Business Availability Center's keystore.

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 89.

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 89.

---

2 Configure SiteScope to trust HP Business Availability Center's client-side certificate.

To configure SiteScope to trust HP Business Availability Center's client-side certificate, you must set the Tomcat used by SiteScope 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:

```
<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**="**your truststore**"
- **truststorePass**="**truststore password**" (if different to the keystore password)

The default truststore used by Tomcat is **<SiteScope 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 89.

A sample command for importing a client-side certificate is:

```
keytool -import -keystore <SiteScope root directory>\JRE\lib\security\cacerts -
storepass changeit -alias "Gateway Server Client Certificate" -trustcacerts -file
myGatewayServerClientCertificate.pem
```

where **myGatewayServerClientCertificate.pem** is the Gateway Server client certificate sent by HP Business Availability Center JVM for client-side authentication, or the Certification Authority (CA) certificate issued it.

Enabling 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 configure the Business Process Monitor to support SSL, set HP Business Availability Center to use HTTPS to connect to the Business Process Monitor, and configure the Gateway Server's Java Runtime Environment (JRE) to trust the Business Process Monitor certificate.

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 className="org.apache.catalina.connector.http.HttpConnector"
   port="2696" minProcessors="5" maxProcessors="75" enableLookups="true"
   redirectPort="8443" acceptCount="10" debug="0" connectionTimeout="60000"/>
   ```

   to:

   ```
   <!--<Connector className="org.apache.catalina.connector.http.HttpConnector"
   port="2696" minProcessors="5" maxProcessors="75" enableLookups="true"
   redirectPort="8443" acceptCount="10" debug="0"
   connectionTimeout="60000"/>-->
   ```

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

   ```
   <!--<Connector className="org.apache.catalina.connector.http.HttpConnector"
   port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
   acceptCount="10" debug="0" scheme="https" secure="true">
   <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
   clientAuth="false" protocol="TLS"/>
   </Connector>-->
   ```

   to:

   ```
   <Connector className="org.apache.catalina.connector.http.HttpConnector"
   port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
   acceptCount="10" debug="0" scheme="https" secure="true">
   <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
   clientAuth="false" protocol="TLS"/>
   </Connector>
   ```

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 http://tomcat.apache.org/tomcat-5.5-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 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 (by default, the **default** user in Windows, the **root** user in UNIX).

11 If you are working on a Windows platform, do the following:

a Go to directory **\Documents and Settings\All Users\Start Menu\Programs\HP Business Process Monitor.**

b Delete **Business Process Monitor Admin** shortcut.

c Left-click the directory **\Documents and Settings\All Users\StartMenu\Programs\HP Business Process Monitor** to highlight it.

d In the top menu bar, select **File** > **New** > **Shortcut**. The Create Shortcut dialog window opens.

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

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

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

12 Restart Business Process Monitor.

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.

Note: The certificate at the Business Process Monitor must be issued to the IP of the Business Process Monitor Web server and not to the Web server name.

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 89.

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.

Tip: You can use the keytool.exe utility to import the Business Process Monitor server-side certificate.

Enabling 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 configure Real User Monitor to support SSL, configure the Gateway Server's Java Runtime Environment (JRE) to trust the Real User Monitor certificate, and set HP Business Availability Center to use HTTPS to connect to Real User Monitor.

Configuring the Real User Monitor Web server to support SSL

To enable a Real User Monitor engine to support SSL communication, you must configure Tomcat 5.0.x to support HTTPS. For detailed information on configuring Tomcat 5.0.x, refer to http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

To configure Tomcat 5.0.x to support HTTPS:

1 Uncomment the following connector element:

```
<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 Real User Monitor SSL communications, change the port number in the connector element accordingly.

---

2 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.

Note: You can create a self-signed certificate for testing, using the keytool.exe utility, as described http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

---

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 Restart Tomcat.

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 89.

You must import the Real User 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.

Tip: You can use the keytool.exe utility to import the Real User Monitor server-side certificate.

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 Database URL to:

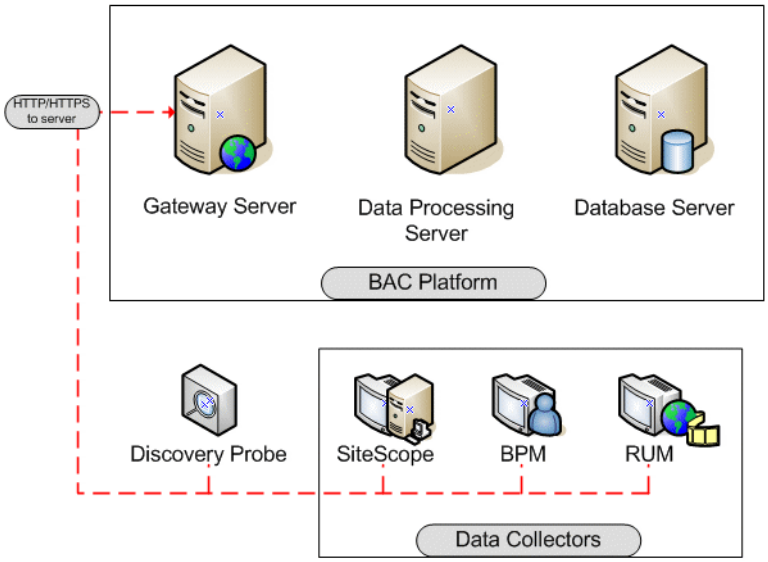
   https://<RUM domain name>:<HTTPS port number>

   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 Data Collectors to the Gateway Server

The instructions in this section describe how to enable SSL from the data collectors to the HP Business Availability Center Gateway Server.



This section includes the following topics:

SSL Configuration for the Gateway Server

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.

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 the entire directories in use by HP Business Availability Center as configured in the Apache configuration file (**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.

SSL Configuration for the Data Collectors

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

- "Business Process Monitor" on page 80
- "SiteScope" on page 81
- "Real User Monitor" on page 83
- "Discovery Probe" on page 85

Note: These instructions are necessary only if the Gateway Server with which the data collector is communicating requires SSL.

Business Process Monitor

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

- **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 CA and to communicate via SSL.
- **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 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. The file must be in PEM format and base64 encoded.
6. Click **Save Changes and Restart 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**.

SiteScope

If the SiteScope machine is required to communicate with the Gateway Server via SSL, the SiteScope machine must be configured 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.

To import a required certificate:

1. Ensure that the certificate to import is in PEM encoding.
2. Use the **keytool.exe** utility, located in the **<HP Business Availability Center server root directory>\JRE\bin** directory.

   The import command should be similar to the following:

   ```
   keytool -import -keystore <SiteScope root directory>\JRE\lib\security\cacerts -storepass changeit -alias myGatewayServerCertificate -trustcacerts -file GatewayServerCert.pem
   ```

   where **GatewayServerCert.pem** is the Gateway Server certificate sent by the Web server for server-side authentication, or the CA certificate that issued it.

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.

To configure SiteScope for SSL using the classic SiteScope interface:

1 Select **Preferences** > **HP BAC**.

2 In the HP Business Availability Center Server Registration page, in the **Optional Settings** section, select the **Use SSL (HTTPS protocol)** check box.

3 Click the **Update** button at the bottom of the page.

4 Restart the SiteScope instance.

Real User Monitor

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

➤ "Configuring a Connection to the Gateway Server Using SSL" – see below

➤ "Configuring an SSL Client-Side Certificate" on page 84

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 CA 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** check boxes.

Configuring an SSL Client-Side Certificate

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

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

1. Open the Real User Monitor Web Console (**http://<Real User Monitor engine name>:8180**).
2. Click the **Configuration** tab.
3. Select **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. Enter the following SSL parameter values:
   - **SSL client certificate file.** The path of the PEM base64 encoded file that holds the client-side certificate.
   - **SSL private key file.** The path of the PEM base64 encoded 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.
7. Click **Save Configuration**.

Discovery Probe

When a session is started between the Discovery Probe and the Gateway Server, the Gateway Server sends the Agent 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 CA and to communicate via SSL.

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

1 Set the Discovery Probe JRE to trust the Gateway Server certificate.

The Discovery Probe truststore file is located at:

%discovery root%\jre\lib\security\cacerts

If the certificate used by the HP Business Availability Center server was not issued by a known CA, you need to import the certificate, or the CA's certificate, to the truststore.

The certificate imported should be in PEM format, base64 encoded.

A sample command, all on the same line, for importing a server-side certificate is:

```
keytool -import -keystore %discovery root%\jre\lib\security\cacerts
-storepass <password>
-alias "Gateway Server certificate"
-file myGatewayServerCertificate.pem
```

where:

- <**password**> is, by default, changeit.
- **myGatewayServerCertificate.pem** is the Gateway server certificate sent by HP Business Availability Center JVM to the Agent, or the Certification Authority (CA) certificate issued it.

2 Set the new connection parameters in the Discovery Probe.

- Open the file **%discovery root%\root\lib\collectors\ DiscoveryProbe.properties**.
- Configure the URL of the HP Business Availability Center server:

  serverIP = <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:

serverPortHttps = <HTTPS port number>

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

appilog.agent.probe.protocol = HTTPS

3 Restart the Discovery Probe.

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 7.0x machine to an HP Business Availability Center 7.50 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 http**s**.

<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 Web server (IIS/Apache) 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.

a keytool -import -trustcacerts -alias bacAlias [-keystore <keystore path>\serverKeystore] -file baccert.cer

---

Note: If [-keystore ..] is omitted, the certificate stored in user's default profile directory is **<%USERPROFILE%>\.keystore**.

---

b Configure SDR to use KeyStore, and add additional options to the process launcher in the file **<BAC Install dir>\SDR\6.x\bin\sdreplicator_run.bat**.

- If the KeyStore was specified, add: **net.ssl.trustStore=<keystoere path>\serverKeystore**
- If [-keystore ..] was omitted when the certificate was imported, and the certificate was stored in default user's KeyStore, add: **net.ssl.trustStore=<%USERPROFILE%>\.keystore**

then add: **net.ssl.trustStorePassword=passphrase**

3 Restart the SDR for the changes to take effect.

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\Gateway\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 89.

To enable the JRE, validate the certificate used by the HP Business Availability Center Web server.

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, see "Setting JRE to Use Client/Server-Side Authentication" on page 91.

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

When the JRE is used to connect to an SSL Web server, or whenever it accepts a client-side 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.

If the JRE is trying to validate a self-signed certificate (a certificate that is issued by itself), it must import the specific certificate into the JRE truststore.

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 the certificate chain, to the truststore used by your JRE.

To import a required certificate to the truststore:

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

The import command should be similar to the following:

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

Note: The certificate imported to the truststore should be in PEM encoding.

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 d:\mycacert -keystore
c:\jre142\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/Server-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:

  ```
  /> keytool -genkey -dname "CN=your name, OU=organization
  unitO=organization" -validity <365> -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

5

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:

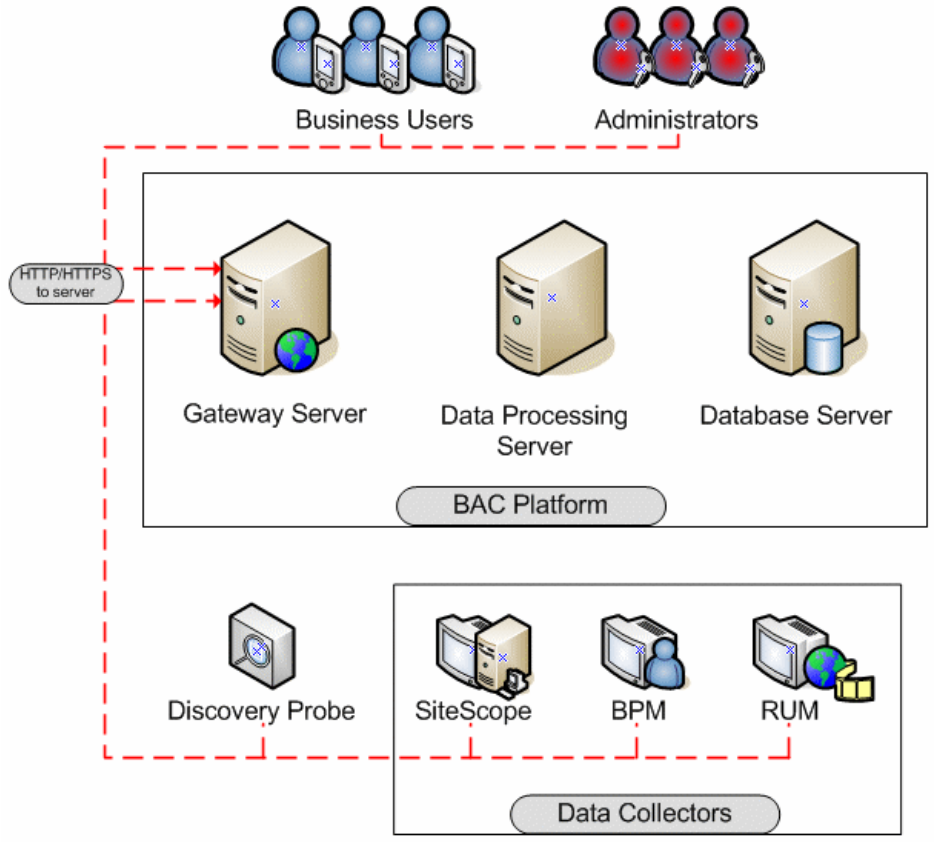
Introducing Basic Authentication Deployment in HP Business Availability Center

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 57.

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.

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.

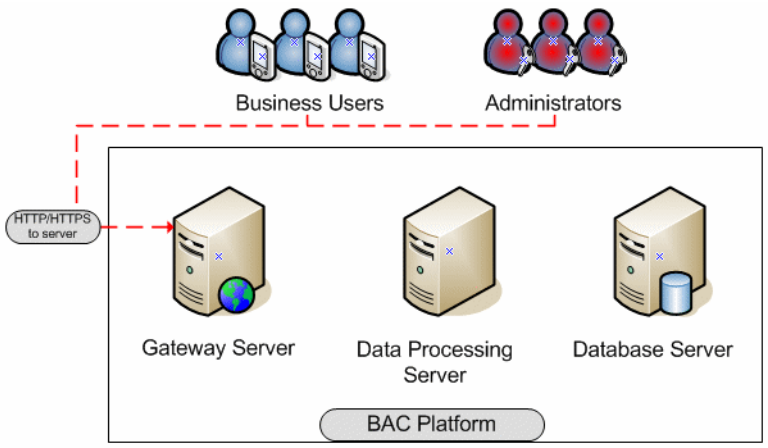
HP Business Availability Center Clients Supporting Basic Authentication

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

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.

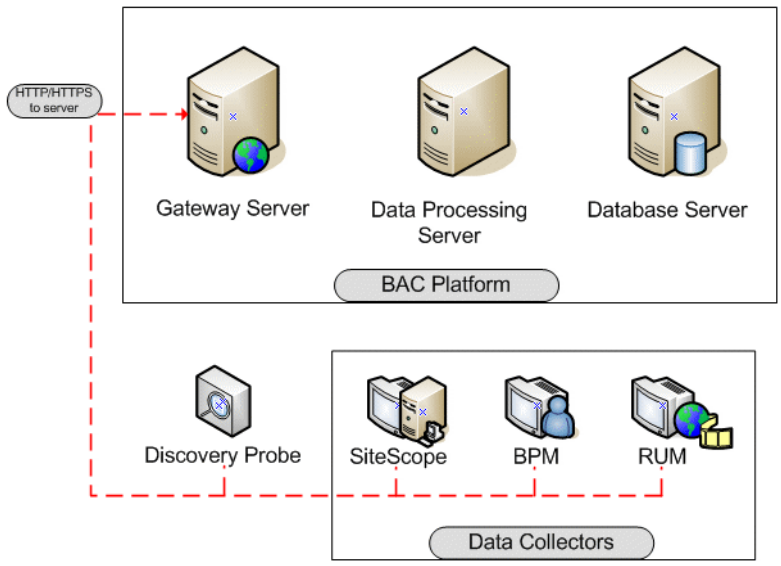
Basic Authentication Configuration for the Application Users

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

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

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 – see below
- "SiteScope" on page 109
- "Real User Monitor" on page 110
- "Discovery Probe" on page 110

Note: The Staging Data Replicator (used during the staging part of the upgrade to repeat samples from an HP Business Availability Center 7.0x machine to an HP Business Availability Center 7.50 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

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

To harden the JBoss JMX console:

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

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

The default JMX user's credentials are:

Login name = **admin**

Password = **admin**

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

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

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

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

To harden the MX4J JMX console:

1 Open the file **<HP Business Availability Center root directory>\conf\jmxsecurity.txt**

2 Add the following line:

<username> <password>

For example: myuser mypassword

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

Index

M

R

S

W