How To
Troubleshoot
SSL with BPC
Version 1.01 - May 2009

Applicable Releases:
SAP BPC 7 Microsoft
1 Scenario

This “How to Guide” will focus on how to troubleshoot a SAP BPC 7M environment that is configured with Secure Socket Layers (SSL).

There are several areas to investigate when troubleshooting SSL, which include:

- Internet Information Services (IIS)
- BPC web.config files
- Server Manager
- BPC Appserver tables
- BPC client
- SQL Server Reporting Services (SSRS) Configuration Tool

2 Introduction

This How-To guide leverages BPC 7 for the Microsoft Platform.

This guide will also be using a single BPC server named vmw2330.wdf.sap.corp.

SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL.

SSL encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted. Only the user's computer and the secure server are able to recognize the data. SSL keeps your name, address, and credit card information between you and merchant to which you are providing it. When you visit a Web address starting with "https," the "s" after the "http" indicates the website is secure. These websites often use SSL certificates to verify their authenticity.

While SSL is most commonly seen on the Web (HTTP), it is also used to secure other Internet protocols, such as SMTP for sending e-mail and NNTP for newsgroups. Early implementations of SSL were limited to 40-bit encryption, but now most SSL secured protocols use 128-bit encryption or higher.
### 3 IIS

#### 3.1 Default Web Site’s Properties – Web Site tab

Ensure that an SSL port is assigned. Most likely it will be 443.

![Default Web Site Properties](image)

<table>
<thead>
<tr>
<th>Directory Security</th>
<th>HTTP Headers</th>
<th>Custom Errors</th>
<th>ASP.NET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Site</td>
<td>Performance</td>
<td>ISAPI Filters</td>
<td>Home Directory</td>
</tr>
</tbody>
</table>

#### Web site identification

- **Description:** Default Web Site
- **IP address:** (All Unassigned)
- **TCP port:** 80, **SSL port:** 443

#### Connections

- **Connection timeout:** 120 seconds
- **Enable HTTP Keep-Alives**

#### Enable logging

- **Active log format:**
  - CDRC Logging

![Buttons](image)
3.2 Default Web Site’s Properties – Directory Security tab

Under Secure communications, click the View Certificate… button
3.2 Default Web Site’s Properties – Directory Security tab continued

Ensure that the certificate is active and has not expired (as in example below).

Take note of the name of the certificate. In the below example, it is vmw2330.wdf.sap.corp.

Best practice is to issue the certificate in the fully qualified domain name (FQDN) of the server.
3.2 Default Web Site’s Properties – Directory Security tab continued

Under Secure communications, click the Edit… button.

Ensure that Require secure channel (SSL) is checked.
4  BPC Web.config files

4.1 Landing Page Web.config file

Using Notepad, open the Web.config file located in the X:\BPC\Websrvr\Web of the BPC web / application server.

Scroll to the bottom and ensure that the file is configured to use:

- HTTPS
- the name of the SSL certificate
- designated SSL port (usually 443)

```xml
<!-- base locations of servers -->
<add key="AppServer_AUTH" value="1"/>
</appSettings>
</configuration>
```

4.2 Management Console Web.config file

Using Notepad, open the Web.config file located in the X:\BPC\Websrvr\Web\ManagementConsole of the BPC web / application server.

Scroll to the bottom and ensure that the file is configured to use:

- HTTPS
- the name of the SSL certificate
- designated SSL port (usually 443)

```xml
<appSettings>
  <add key="mp_server" value="vmw2330"/>
  <add key="msiserver" value="vmw2330"/>
  <add key="logServer" value="vmw2330.wdf.sap.corp:443"/>
  <add key="systemConfig" value="https://vmw2330.wdf.sap.corp:443/osoft/app/Service/SystemConfigService"/>
</appSettings>
</system.web>
```
5 BPC Server Manager

5.1 Server Options

Open Server Manager>Server>Server Options. Ensure that the values for Reporting Services, Application, and Web Server names match the certificate.

For the Reporting Services, Application, and Web Servers, ensure that the Protocol parameter is set to HTTPS and that the Port number is set to the designated port (usually 443).

![Server Options](image)

<table>
<thead>
<tr>
<th>Server Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Web site</td>
<td>Default Web Site</td>
</tr>
<tr>
<td>- HTTP compression</td>
<td>No</td>
</tr>
<tr>
<td>- Protocol</td>
<td>https</td>
</tr>
<tr>
<td>- Port number</td>
<td>443</td>
</tr>
<tr>
<td>- Authentication type</td>
<td>Windows</td>
</tr>
<tr>
<td>Scheduler Server Name</td>
<td>VMW2330.wdf.sap.corp</td>
</tr>
<tr>
<td>Web Server name</td>
<td>VMW2330.wdf.sap.corp</td>
</tr>
<tr>
<td>- External server name</td>
<td></td>
</tr>
<tr>
<td>- Virtual server name</td>
<td></td>
</tr>
<tr>
<td>- Web site</td>
<td>Default Web Site</td>
</tr>
<tr>
<td>- HTTP compression</td>
<td>No</td>
</tr>
<tr>
<td>- Protocol</td>
<td>https</td>
</tr>
<tr>
<td>- Port number</td>
<td>443</td>
</tr>
<tr>
<td>- Authentication type</td>
<td>Windows</td>
</tr>
</tbody>
</table>
6 BPC Appserver Tables

6.1 tblServerInfo

Within the AppServer database in SQL, open tblServerInfo. Ensure that the values match that were checked in Server Manager in section 5.

<table>
<thead>
<tr>
<th>ServerType</th>
<th>ServerName</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>AppAuthType</td>
<td>Windows</td>
</tr>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>AppPort</td>
<td>443</td>
</tr>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>AppProtocol</td>
<td>https</td>
</tr>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>AppServer</td>
<td>VMW2330</td>
</tr>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>AppWebSite</td>
<td>1</td>
</tr>
<tr>
<td>AppServer</td>
<td>AppServer1</td>
<td>ExtAppServer</td>
<td>VMW2330.wdf.sap.corp</td>
</tr>
</tbody>
</table>

6.2 tblAppSetInfo

Within the AppServer database in SQL, open tblAppsetInfo. Ensure that the values correspond to the ServerName values that are in tblserverinfo.

<table>
<thead>
<tr>
<th>ReportServer</th>
<th>AppServer</th>
<th>WebServer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReportServer1</td>
<td>AppServer1</td>
<td>WebServer1</td>
</tr>
</tbody>
</table>
7 BPC Client

7.1 SSL Connection Wizard Option

Ensure that the Use secure port (only if web server is SSL-enabled) radio button is checked.
8 SQL Server Reporting Services

Navigate to Reporting Services Configuration Manager by the following:
Start>Programs>Microsoft SQL Server 2008>Configuration Tools.

8.1 Checking Reporting Services Web Service URL

Ensure that the correct SSL Certificate and SSL Port are designated.
(At time of writing this guide, the current SSL certificate was expired and is shown as "Unknown").
8.2 Report Manager URL

Ensure that the Report Manager URL has HTTPS and the SSL Port designated.