



How To... Troubleshoot SSL with SAP Business Planning and Consolidation 10.0, version for the Microsoft Platform

Applicable Releases:

SAP Business Planning and Consolidation 10.0, version for the Microsoft Platform

Version 1.0

April 2014

© Copyright 2012 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.

SAP NetWeaver "How-to" Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer:

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Document History

| Document Version | Description |
|------------------|--------------------------------------|
| 1.00 | First official release of this guide |

Typographic Conventions

| Type Style | Description |
|---------------------|--|
| <i>Example Text</i> | Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation |
| Example text | Emphasized words or phrases in body text, graphic titles, and table titles |
| Example text | File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools. |
| Example text | User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation. |
| <Example text> | Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system. |
| EXAMPLE TEXT | Keys on the keyboard, for example, F2 or ENTER. |

Icons






| Icon | Description |
|---|-----------------------|
|  | Caution |
|  | Important |
|  | Note |
|  | Recommendation or Tip |
|  | Example |

Table of Contents

| | | |
|-----|--|---|
| 1. | Scenario | 1 |
| 2. | Background Information | 1 |
| 3. | Prerequisites | 1 |
| 4. | Step-by-Step Procedure | 2 |
| 4.1 | Checking the Settings of Internet Information Services | 2 |
| 4.2 | Planning and Consolidation web.config files | 4 |
| 4.3 | Planning and Consolidation Server Manager | 5 |
| 4.4 | Planning and Consolidation AppServer Tables..... | 6 |
| 4.5 | Planning and Consolidation Client..... | 6 |
| 4.6 | Checking the Configuration of SQL Server Reporting Services..... | 6 |

1. Scenario

This "How to Guide" will focus on how to troubleshoot a SAP Business Planning and Consolidation 10.0, version for the Microsoft platform environment that is configured with Secure Socket Layers (SSL).

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

- Internet Information Services (IIS)
- The Planning and Consolidation web.config files
- Server Manager
- The Planning and Consolidation Appserver tables
- The Planning and Consolidation client
- Microsoft SQL Server Reporting Services (SSRS) Configuration Tool

2. Background Information

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. Prerequisites

You must have administrative privileges for Planning and Consolidation, Internet Information Services (IIS), Microsoft SQL Server.

4. Step-by-Step Procedure

4.1 Checking the Settings of Internet Information Services

Verifying the Validity of the Server Certificate

1. Open the IIS Manager, by choosing *Start* → *All Programs* → *Administrative Tools* → *Internet Information Services (IIS) Manager*.
2. In the *Connections* panel, choose the server node.
3. In *Features View* double-click *Server Certificates*, as shown in *Figure 1: Server Certificates*.
4. Select the certificate that you are using for your web site and in the *Actions* panel choose *View*.
5. In the *General* tab, check the validity of the certificate.

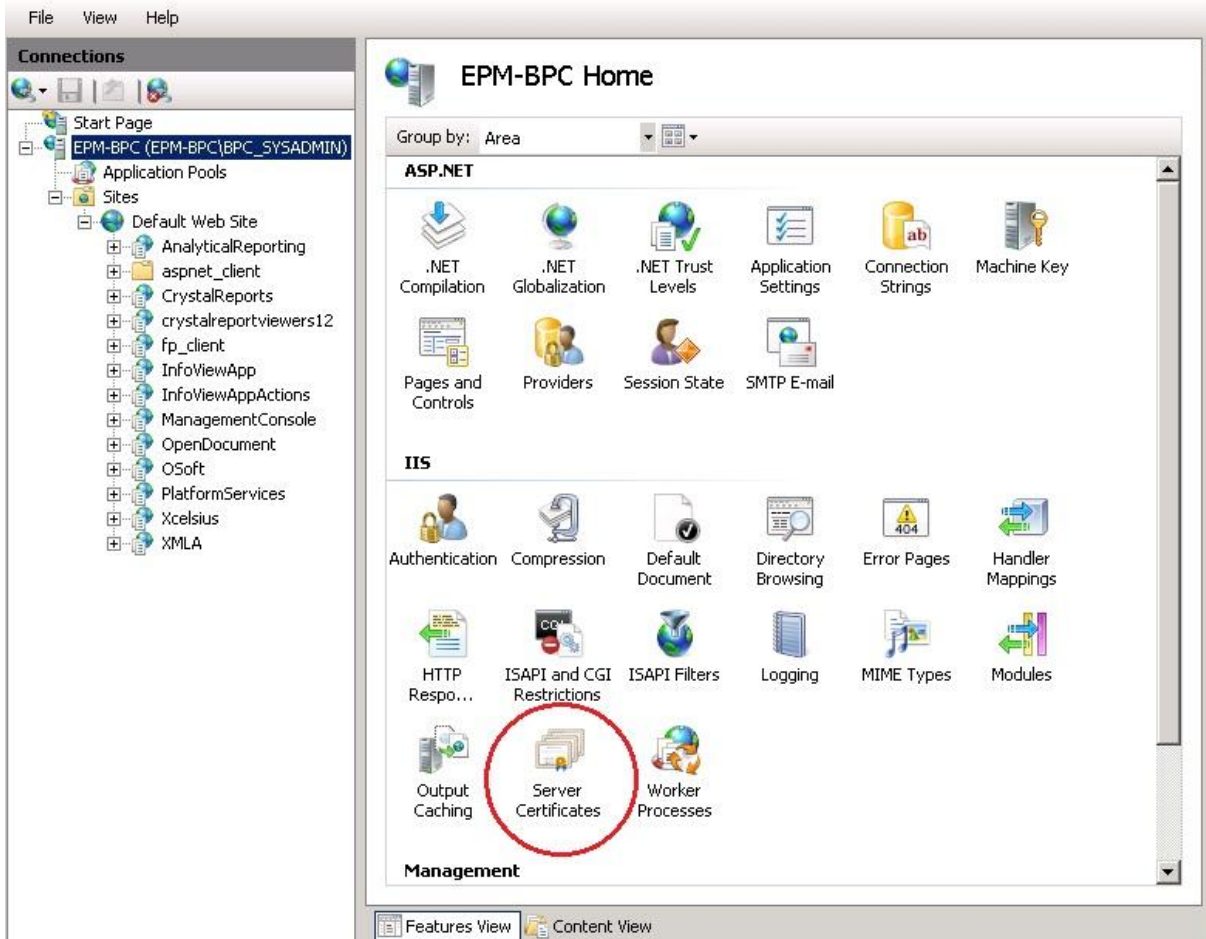


Figure 1: Server Certificates

Checking if SSL Connections are Required

1. In the IIS Manager, under the *IIS* section, choose *SSL Settings*, as shown in *Figure 2: SSL Settings*.
2. Make sure that the *Require SSL* checkbox is selected, as shown in *Figure 3: Require SSL*.

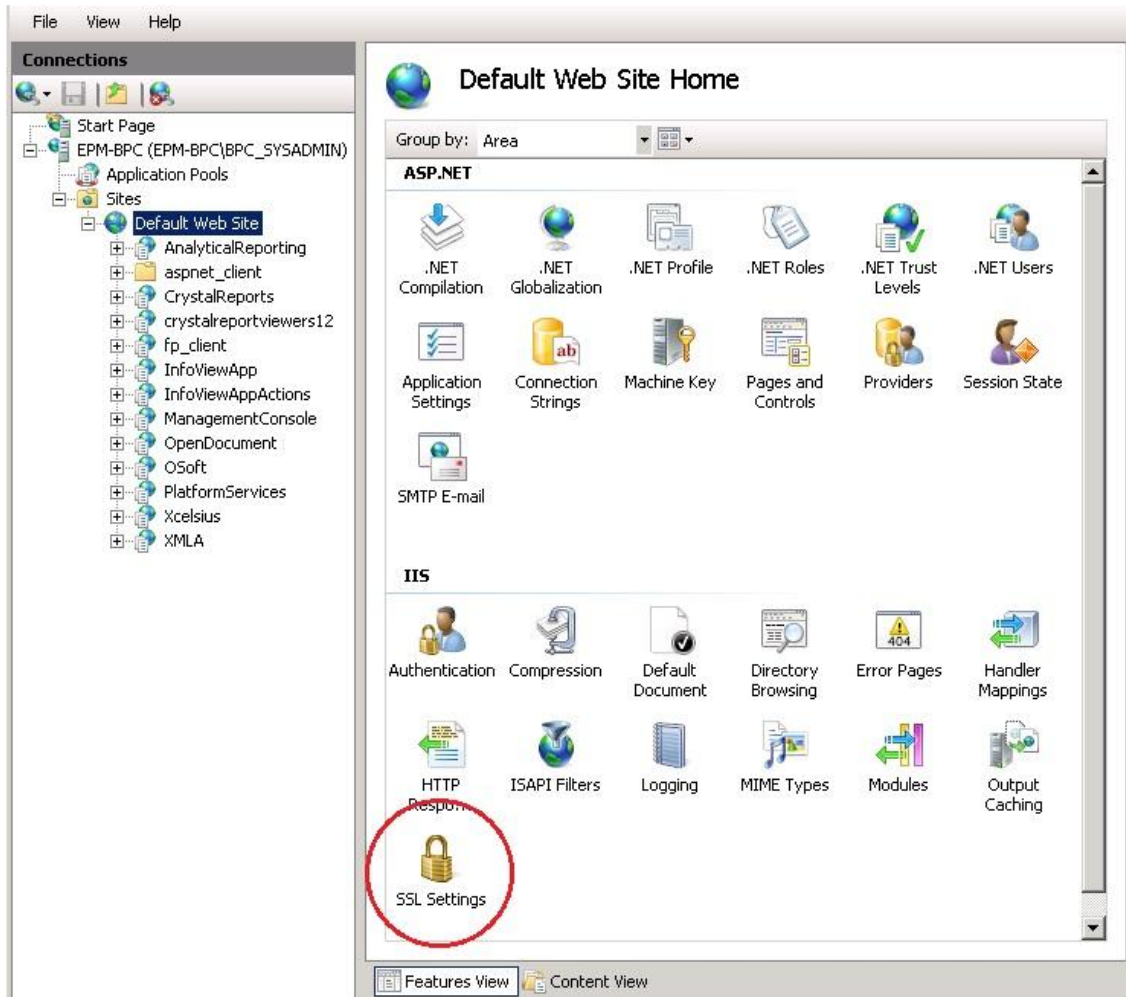


Figure 2: SSL Settings

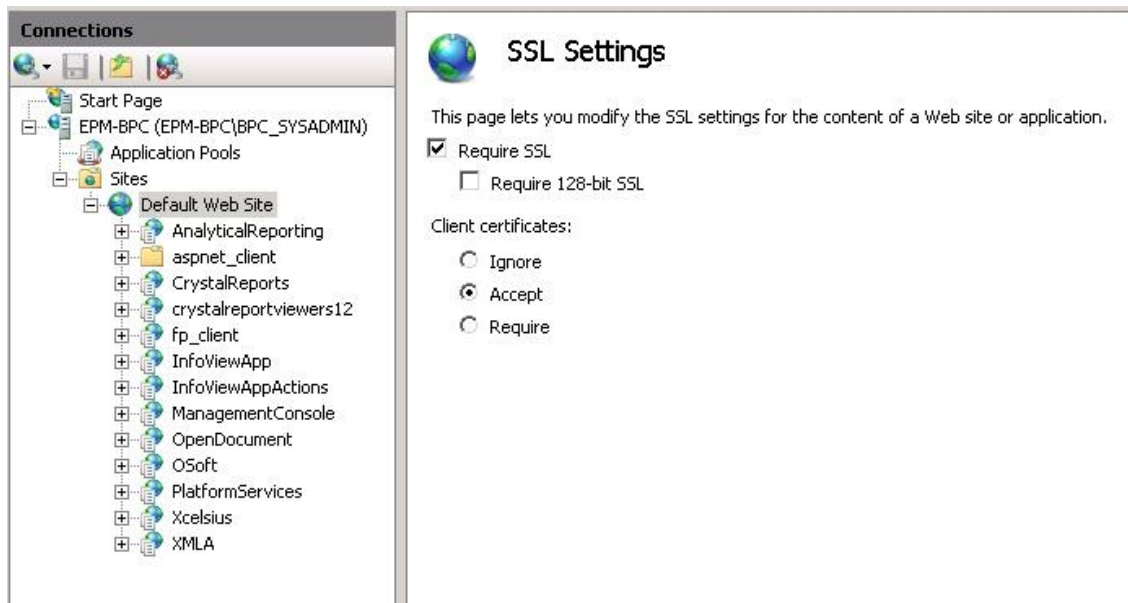


Figure 3: Require SSL

Verifying the Certificate is Bound to the Web Site

The server certificate must be properly bound to the web site for which you want to use SSL. Thus when a client opens the web site, the server will send its certificate and the client can use the certificate to encrypt information and send it to the server.

3. In the IIS Manager, in the *Connections* panel, select the web site node
4. In the *Actions* panel, choose *Bindings*.
5. Make sure there is a binding of type *https* and that this binding points to the local server. To do that, select the binding of type *https* and choose *Edit*.
6. Verify that the following parameters are set:
 - a. *Type = https*
 - b. *IP address = [:::1]* - this is a shorthand expression for the local server name
 - c. *Port = 443* – this is the default port that SSL uses
 - d. *SSL Certificate* – this is the certificate that you want to use for SSL connections

4.2 Planning and Consolidation web.config files

Landing Page web.config File

1. Open the web.config file located in the `<drive>:\BPC\Webstrvr\Web` of the Planning and Consolidation web / application server.
2. 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)

Management Console web.config file

1. Open the web.config file located in the <drive>:\BPC\Web\ManagementConsole of the Planning and Consolidation web / application server.
2. 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)

4.3 Planning and Consolidation Server Manager

1. Go to *Server Manager* → *Server* → *Server Options*.
2. Ensure that the values for Reporting Services, Application, and Web Server names match the certificate.
3. 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).

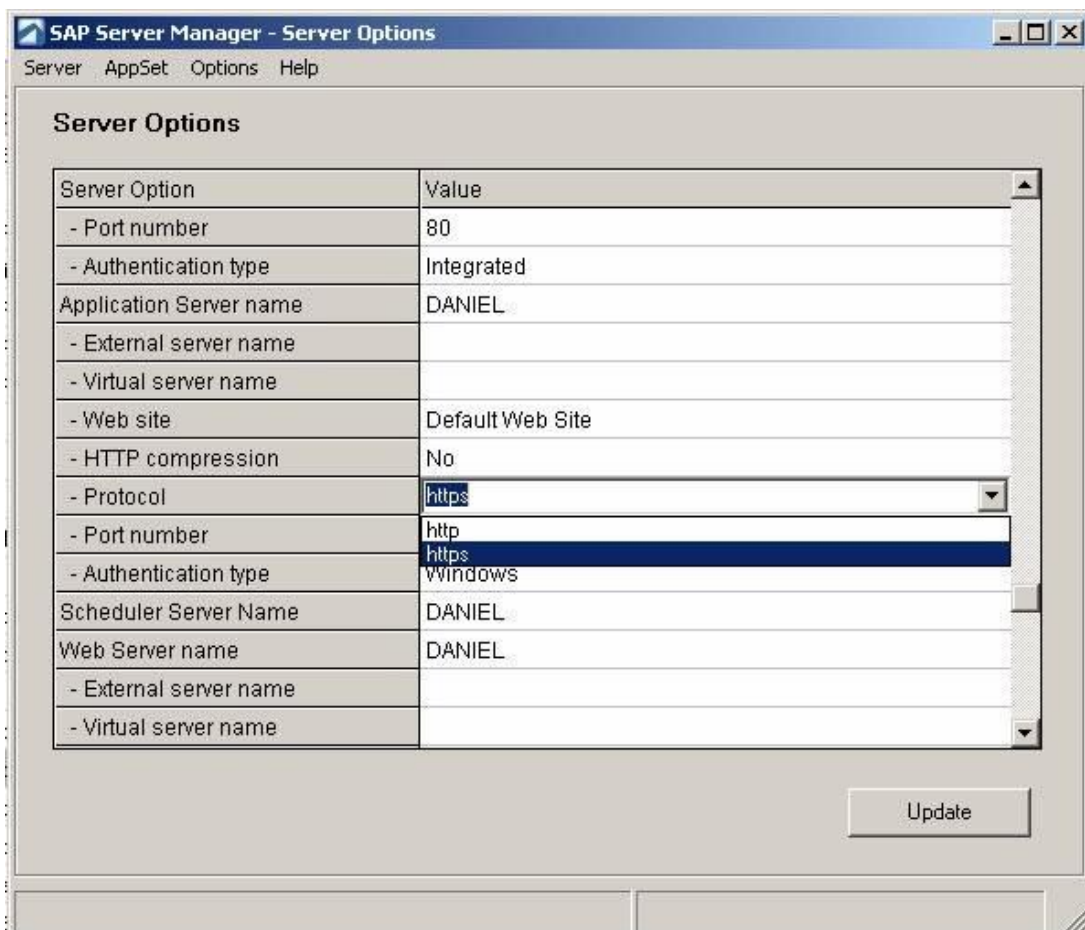


Figure 4: Server Options

4.4 Planning and Consolidation AppServer Tables

The information regarding the server configuration, security and protocol are saved in the table *tblServerInfo*, in the *AppServer* database.



Under normal circumstances you do not need to make any changes directly in the database. All the necessary configurations are done in the Server Manager and then are propagated to the tables and files as needed.

1. Within the *AppServer* database in SQL, open *tblServerInfo*.
2. Ensure that the values match the values in Server Manager from the previous section of this guide.

4.5 Planning and Consolidation Client

When configuring a connection to the Planning and Consolidation server using the Connection Wizard, make sure that you have selected the option to use secure connection. Note that this option only works if SSL has already been enabled on the server side.

4.6 Checking the Configuration of SQL Server Reporting Services

Open the *Reporting Services Configuration Manager* program. To do this, open the Windows *Start* menu and navigate to *All Programs* → *Microsoft SQL Server <version>* → *Configuration Tools* → *Reporting Services Configuration Manager*.

Checking Reporting Services Web Service URL

1. In the *Connect* panel, choose *Web Service URL*.
2. Verify that the correct SSL port and SSL Certificate are assigned. For more information, see *Figure 4: Web Service URL*.

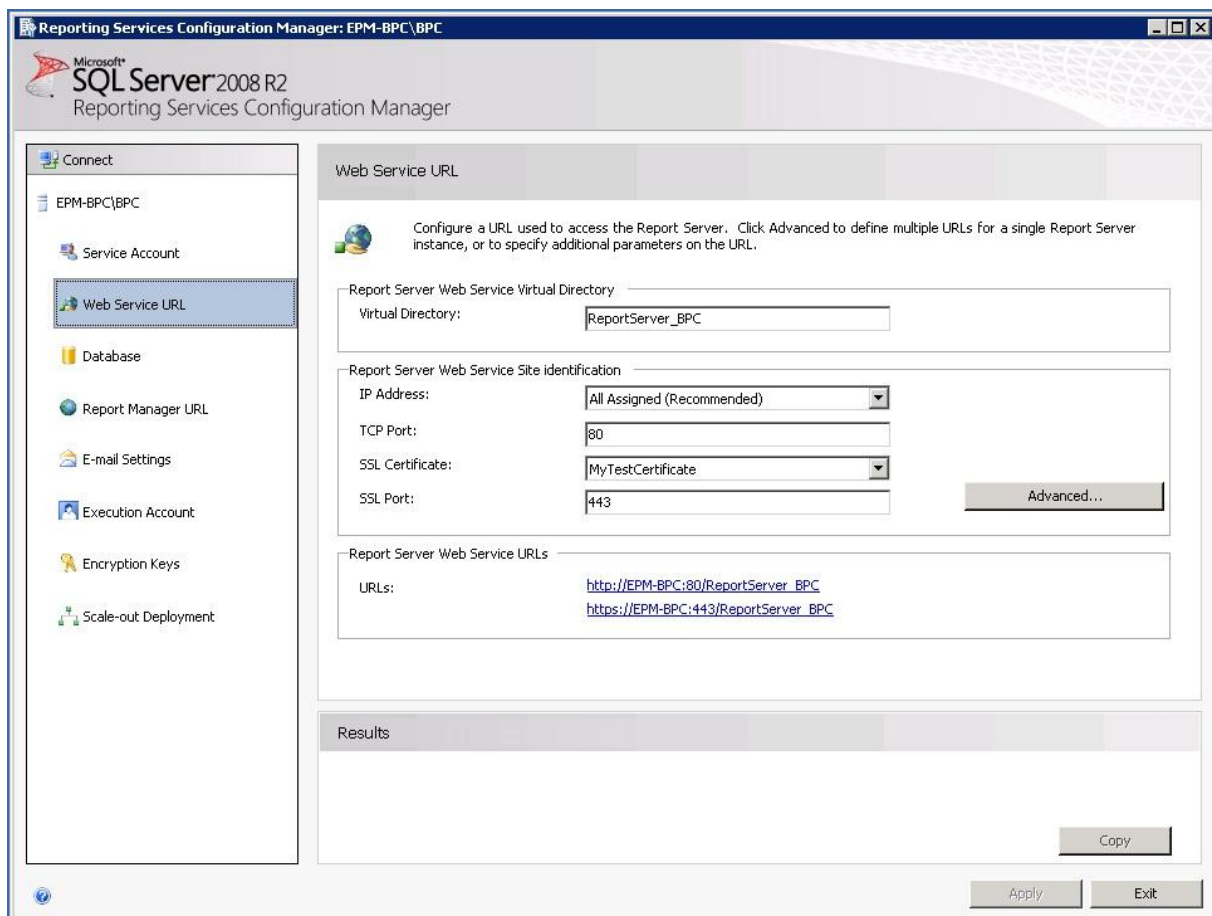


Figure 5: Web Service URL

Checking Reporting Services Report Manager URL

1. In the *Connect* panel, choose *Report Manager URL*.
2. Choose *Advanced*.
3. Verify that in the section *Multiple SSL Identities for Report Manager* the correct SSL port and SSL Certificate are assigned.

