SSL Certificate – SAP

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for SAP Web Application Server

Installation Instructions for SAP Web Dispatcher

Installation Instructions for SAP Web Application Server

Obtain and Install SSL certificate

Method 1. Download and install the SSL in PKCS#7 format

1. Download the certificate from your Symantec Trust Center account by following the steps here.

   NOTE: When downloading the certificate, please select **PKCS#7** as a certificate format and save it as **SSL.p7b**
2. From **Trust Manager** expand the **SSL server PSE node**.
3. Double click to select the appropriate application server. The application server's SSL server PSE is displayed in the PSE maintenance section.
4. In the PSE maintenance section, choose Import Cert. Response. The dialog for the certificate request response will be displayed.
5. Paste the contents of the **SSL.p7b** into the dialog's text box or select the response from the file system by using Load local file.
6. The signed public-key certificate is imported into the server's SSL server PSE, which is displayed in the PSE maintenance section.
7. You can view the certificate by selecting it with a double click. The certificate information is then shown in the certificate maintenance section.
8. Save the data.

   NOTE: If you are using Method 1 you don't need to download and install the Intermediate CA Certificate as the PKCS#7 format contains your SSL certificate and the Intermediate CA certificate.

Method 2. Obtain the SSL Certificate sent via e-mail

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

-----END CERTIFICATE-----

3. Save the file as **SSL.pem**
4. From **Trust Manager** expand the **SSL server PSE node**.
5. Double click to select the appropriate application server. The application server's SSL server PSE is displayed in the PSE maintenance section.
6. In the PSE maintenance section, choose Import Cert. Response. The dialog for the certificate request response will be displayed.
7. Paste the contents of the **SSL.pem** into the dialog's text box or select the response from the file system by using Load local file.
8. The signed public-key certificate is imported into the server's SSL server PSE, which is displayed in the PSE maintenance section.
9. You can view the certificate by selecting it with a double click. The certificate information is then shown in the certificate maintenance section.
10. Save the data.
11. Download and install the Intermediate CA certificate by following the steps here.
12. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for SAP Web Dispatcher

Step 1. Obtain the Symantec Intermediate CA Certificate

1. Download the **Intermediate CA certificate** from this link:
   Select the appropriate Intermediate CA certificate for your SSL Certificate type..
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **intermediate.pem**

Step 2. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   Do not use Microsoft Word or other word processing programs that may add characters.

   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the as **SSL.pem**

Step 3. Install the SSL Certificate

To install an SSL certificate on a SAP Web Dispatcher, follow either **one** of the following **methods**:

Method 1. Install the SSL Certificate Using the Trust Manager

1. If the certificate request dialog is still open, then close it.
2. If the SAP Web Dispatcher's PSE is not loaded in the PSE maintenance section, then load it by selecting the File node with a double-click and selecting the PSE from the file system.
3. In the PSE maintenance section, choose Import Cert. Response. The dialog for the certificate response appears.

4. Insert the contents of the certificate request response into the dialog's text box either using Copy & Paste or by loading the file from the file system.
5. The signed public-key certificate is imported into the SAP Web Dispatcher's PSE, which is displayed in the PSE maintenance section.
6. You can view the certificate by selecting it with a double-click. The certificate information is then shown in the certificate maintenance section.
7. Create a PIN for the PSE.

   NOTE: It is recommended using a PIN to protect the PSE, especially if the SAP Web Dispatcher is located in your demilitarized zone.
8. Save the data in the trust manager.
9. You are prompted for the location to which to save the PSE. Replace the PSE that you created earlier.
10. If you saved the PSE to a local file on the application server, then copy it to the SECUDIR directory on the SAP Web Dispatcher.

Method 2. Install the SSL Certificate Using SAPGENPSE

1. Use configuration tool sapgenpse to import the certificate request response into the PSEs.
2. Run the following command:

   Example: sapgenpse import_own_cert <Additional_options> -p <PSE_file> -c <Cert_file> -r <RootCA_cert_file> -x <PIN>

   -p <PSE_Name> Path and file name of the PSE. The path is the SECUDIR directory and the file name is SAPSSLS.pse.
   for the SSL server PSE or SAPSSLC.pse for the SSL client PSE (if it exists). Path description (in quotation marks, if spaces exist)

   -c <Cert_file> Path and file name of the certificate request response. Path description (in quotation marks, if spaces exist)

   -r <RootCA_cert_file> File containing both the Root CA certificate and the Intermediate CA certificate. The Intermediate CA
   certificate is to be first followed by the Root CA certificate. Path description (in

quotation marks, if spaces exist)

-x <PIN> PIN that protects the PSE Character string

3. Verify certificate installation using the Symantec Installation Checker.