

How to Setup HTTPS

Document revision 1.2

Description

This Manage for TEOS How to Setup HTTPS will explain how you can switch your TEOS 3.0 installation to HTTPS. This guide is meant for server administrators as it requires admin access to the TEOS web and SQL Server.

SSL certificate is not provided by Sony and needs to be generated based on customer domain setup.

Requirements

- Manage for TEOS server from version 3.0
- SSL Certificate for a wildcard or multiple websites on IIS Server is not anymore requested a simple SSL certificate for a web hosting is enough
- SSL certificate is not provided by Sony for on premise server
- SSL Certificate for https must be a public
- Access to the Manage for TEOS server with admin rights

Content

Requirements	2
1. Pre-requirements	3
1.1. Generate a certificate – Example.....	3
1.1.1. IIS - Generate CSR	3
1.1.2 IIS - Certificate Installation	5
1.1.3 Certificate Installation.....	5
2. Setup IIS	7
2.1. Import your certificate	7
2.2. Adding the bindings	7
3. Running TEOS http switching wizard	9

1. Pre-requirements

Before you can generate your SSL Certificate, the certificate requester must create a Certificate Signing Request (CSR) for a domain name or hostname on your web server. The CSR is a standardized way to send the issuing Certificate Authority (CA) your public key, which is paired with a secret private key on the server, and provides relevant information about the requester as indicated below:

Common Name (CN): This is the Fully Qualified Domain Name (FQDN) of your server (i.e. www.pro.sony). This must match exactly what you type in your web browser or you may receive a security error.

Organization Name (O): The legal name of your company/organization (i.e. Google, Inc.). Do not abbreviate your company name and it should include the corporate identifier such as Inc., Corp, or LLC (if applicable). For DV orders, you can use your personal name (i.e. John Doe).

Organization Unit (OU): The unit or division of the company/organization managing the certificate (i.e. IT Department).

Locality (L): The city that you are located in (i.e. Basingstoke)

State or Province Name (ST): The state or province in which you are located in (i.e. London)

Country (C): The country in which you are located in (i.e. United Kingdom or UK)

Email Address: An email address associated with the company (i.e. webmaster@sony.com)

Make sure the certificate is a wildcard, or multidomain certificate to support all the websites within TEOS.

If you request a wildcard certificate (*.teos.domaincompany.com) please make sure the hostname (TEOS domain name which is entered the browser for opening the TEOS web interface) is also included in the wildcard certificate.

Please see this example manual concerning generating the CSR:

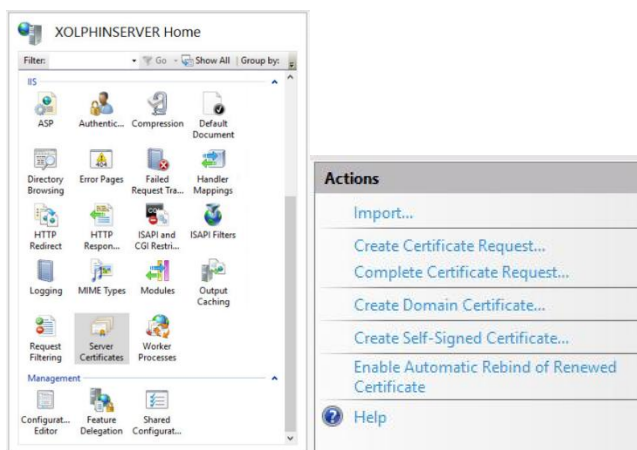
1.1. Generate a certificate – Example

1.1.1. IIS - Generate CSR

This manual applies to IIS 7, 8, 8.5 and 10. A different manual is available for IIS 5 and 6, and Exchange 2000 and 2003.

A Certificate Signing Request (CSR) is required when applying for an SSL certificate. This CSR (and private key) can be generated on your webserver. To request a wildcard certificate, fill in an * (asterisk) for the subdomain, for example *.sslcertificaten.nl (instead of www.sslcertificates.nl). Open the IIS Manager via Start? Administrative Tools? IIS Manager. Choose the server name and then click Features (middle field)

Double-click Server Certificates under Security.




Open the Properties page of the site which must be secured.

Right-click Create Certificate Request under Actions panel to create a CSR.

Click the Server Certificate button to start the wizard.

In the first screen of the wizard you will be asked to fill in data concerning your organization. Please do so and click Next to go further.

Request Certificate ? X

 **Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:


City/locality:

State/province:

Country/region:

In the next screen of the wizard, the cryptography-settings are set. You can leave this at the standard setting (Microsoft RSA Channel Cryptography Provider). A Bit Length of 1024 bits is the default option; change this to 2048 bits as this is currently the minimum requirement. Please click Next to go to the next screen.

Request Certificate ? X

 **Cryptographic Service Provider Properties**


Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

Enter a file name and path to the location where the CSR must be stored (for instance c:\documents and settings\administrator\desktop\sslcertificaten.nl.csr). This information will be needed again when requesting the CSR later. Click Finish. The CSR has now been saved.

Request Certificate ? X

 **File Name**

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

Example manual for installing certificate here:

1.1.2 IIS - Certificate Installation

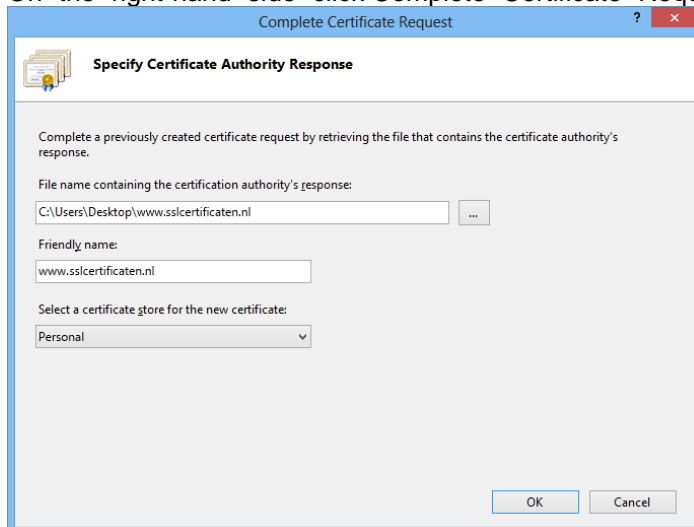
This manual applies to IIS 7, 8, 8.5 and 10. A different manual is available for IIS 5 and 6, and Exchange 2000 and 2003.

Immediately after being issued, your SSL certificate will be sent to you by email. It is also possible to download the certificate from the Control Panel. The file containing the certificate will have the same name as the domain name it is meant for (for example: www_sslcertificaten_nl.crt).

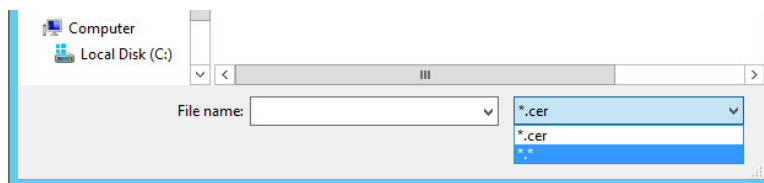
1.1.3 Certificate Installation

Save the certificate files that were sent, so that they are accessible from the server. Click the Start menu? Administrative Tools? IIS Manager. Choose the server name and then click Features (middle field). Double-click Server Certificates under Security.

On the right-hand side click Complete Certificate Request under Actions. A new window will open.



Navigate to the saved certificate; the standard file name follows this structure your_domain_com.crt. Note: If you have purchased a certificate for which a root and intermediate certificate must be installed, it is practical to use the .p7b-file, as this installs both the root and intermediate certificates.



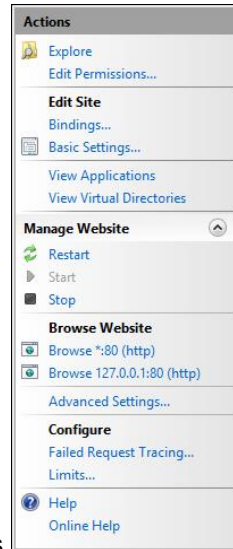
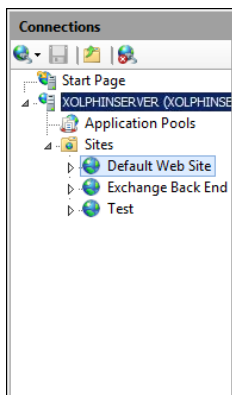
Enter a practical name for the Friendly name - such as the domain name - and click OK. The certificate is now installed and ready to be bound to the website.

Bind certificate to the website

The certificate can now be activated. To do this the website first has to be bound to the HTTPS protocol, after which the certificate can be assigned to the website. To bind the certificate to the website via the user interface follow the steps below. Other options are to use the Powershell or Command Prompt.

Click the Start menu? Administrative Tools? IIS Manager.

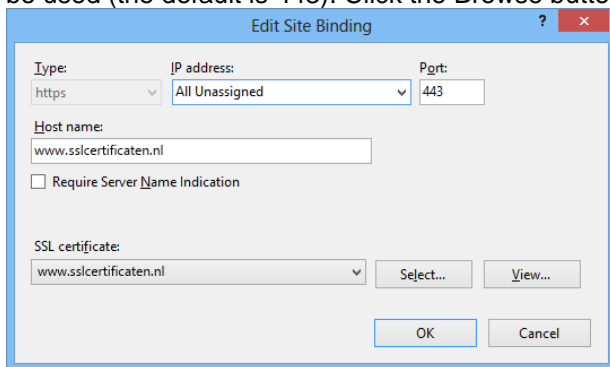
In the IIS Manager use the left menu to browse to the server that hosts the website that must be secured, go to Sites and select the website which must be secured using the new certificate.



Action panel to the right, click Bindings.

In the Site Bindings window click Add... to open the Add Site Binding window.

Enter https as Type, the IP-address of the server through which the website is accessed, and the port to be used (the default is 443). Click the Browse button, select the just installed certificate and click OK.



All necessary steps to install your web server certificate have now been completed. Please make sure to adequately secure your certificate files, and to store a backup of your private key and web server certificate in a safe location. You should also install the root and intermediate certificates. Check whether the certificate is correctly installed with the SSLCheck and ensure an optimal configuration with these tips and settings.

Please do not hesitate to contact us if you encounter problems or error messages.

Importing/exporting SSL certificates:

In case you did not request the CSR on the TEOS server you will not be able to import the .crt file on the TEOS server, in this case please complete the certificate request on the server where the CSR has been generated. Once the certificate is available create an export inside IIS to create a .PFX file, this .PFX file can then be imported on the TEOS server using IIS.

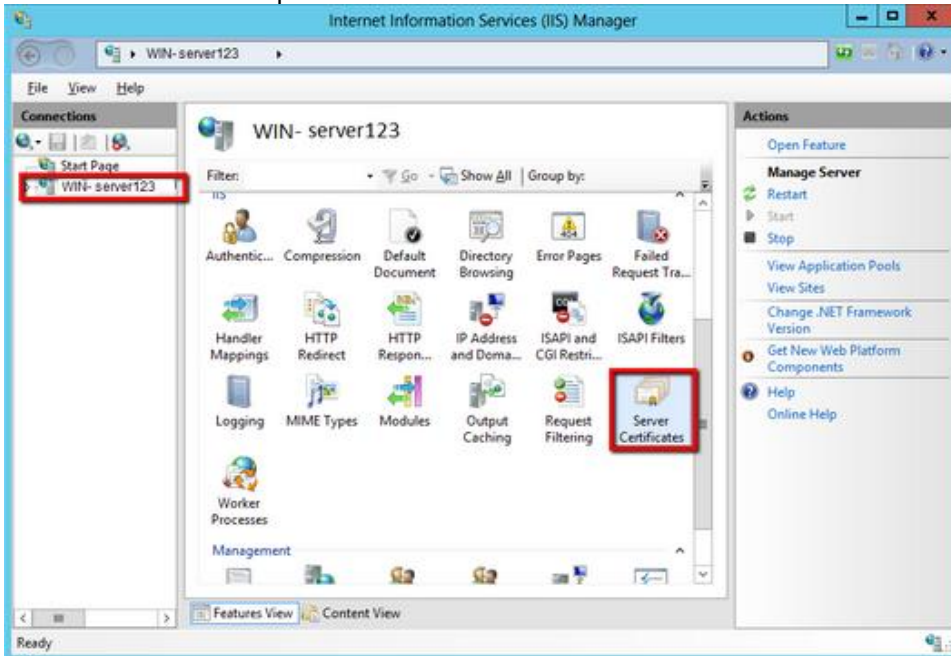
Please see the manual below for exporting an SSL certificate to a .PFX file within IIS:

<https://www.ssldesktop.com/export-certificate-internet-information-services-iis-manager/>

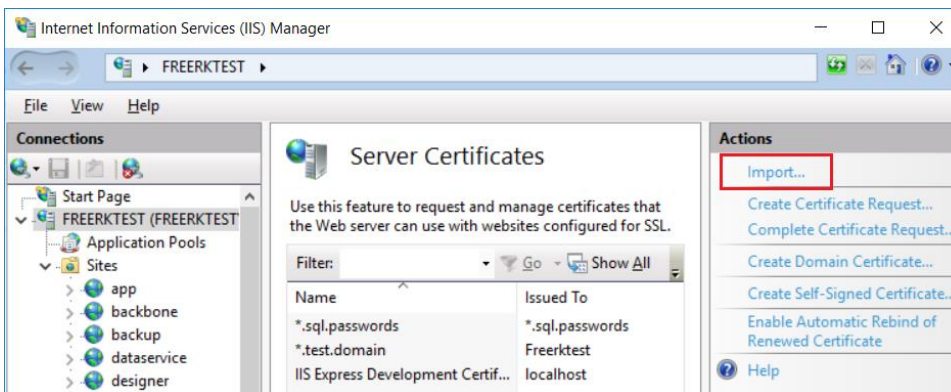
2. Setup IIS

2.1. Import your certificate

The first step is to import your certificate in IIS. Open IIS Manager, in the left side click on the main server and then open the “Server Certificates section”.

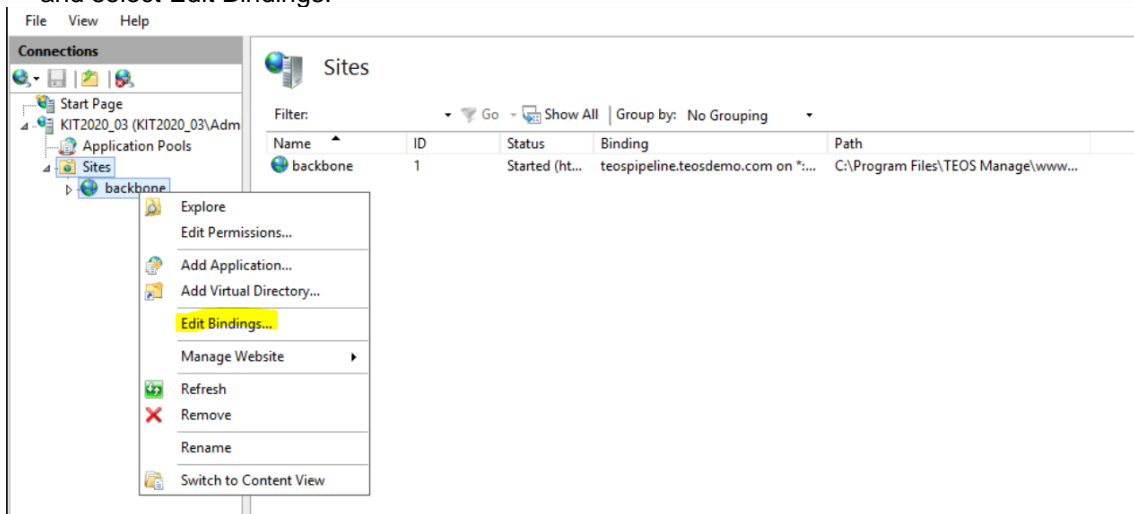


Next import your certificate, or you can create a certificate request if you want to purchase a new certificate. Make sure the certificate is a web hosting to make sure you can support all the websites within TEOS.

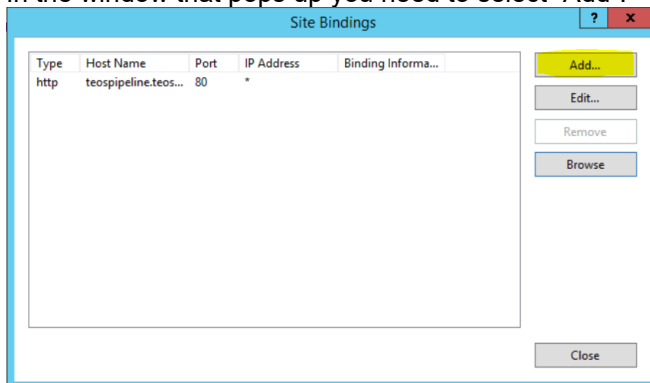


2.2. Adding the bindings

Next you need to bind the certificate to the websites. To do this you need to right click each of the sites and select Edit Bindings.

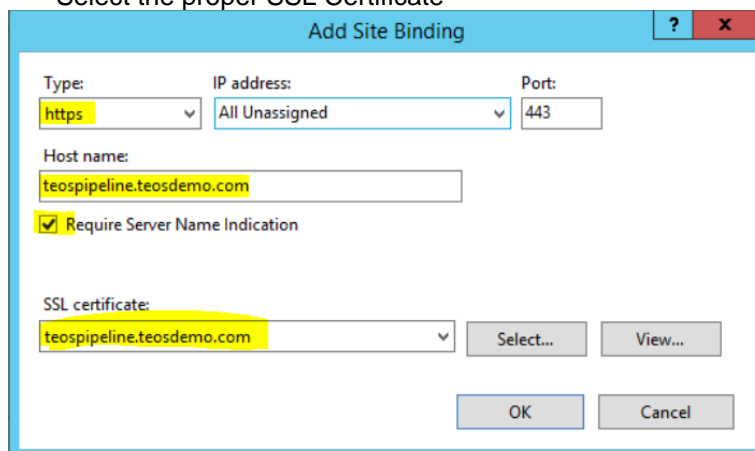


In the window that pops up you need to select “Add”.



For most of the sites you need to add 1 binding with the certificate. Make sure for each binding you add you:

- Select Type https
- Enable the checkbox “Require Server Name Indication”
- Select the proper SSL Certificate



3. Running TEOS http switching wizard

After IIS has been configured, you can run the wizard for the final configurations.

When you start the wizard, you can choose to either switch TEOS to HTTPS, or to switch back to HTTP. After you have chosen, click on Next. The latest version compatible with Manage for TEOS 3.0 is the **version 3.0**, please ensure to run the correct version.

TEOS Setup - TEOS HTTPtoHTTPSSwitcher 1.1.0

Switch protocols
http // https

Please select if you want to switch your installation to http or to https

☒ Switch from http to https

☐ Switch from https back to http

Next > Cancel

TEOS Setup - TEOS HTTPtoHTTPSSwitcher 1.1.0

License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

License info TEOS Manager
Unlicensed use of this software is prohibited.

☒ I accept the agreement

☐ I do not accept the agreement

< Back Next > Cancel

In the next screen accept the agreement and click on next.

TEOS Setup - TEOS HTTPtoHTTPSSwitcher 1.0.0

Ready to Install
Setup is now ready to begin installing TEOS HTTPtoHTTPSSwitcher on your computer.

Click Install to continue with the installation.

< Back Install Cancel

TEOS Setup - TEOS HTTPtoHTTPSSwitcher 1.0.0

Database Connection Information
This information is required for installation

Please specify the server and the connection credentials, then click Next.

Server:
localhost

User name:
sa

Password:

< Back Next > Cancel

You now need to fill in the credentials to connect to the databases. This setup requires a **SQL User with sysadmin privileges**. After clicking Next all configuration changes will be executed.

TEOS Setup - TEOS HTTPtoHTTPSSwitcher 1.0.0

Completing the TEOS HTTPtoHTTPSSwitcher Setup Wizard

Setup has finished installing TEOS HTTPtoHTTPSSwitcher on your computer.

Click Finish to exit Setup.

Finish

The configuration is now completed, and you can click Finish.

You can now access to Manage for TEOS web interface using <https://yourcompany.com>

SONY



For more information
visit **pro.sony/TEOS**

© 2021 Sony Corporation