Installing Internet Information Services (IIS) and Creating Certificates

Table of Contents

[Installing Internet Information Services (IIS) and Creating Certificates 3](#_Toc8647747)

[Step 1 - Installing IIS 3](#_Toc8647748)

[Step 2 - Creating Certificate Request 4](#_Toc8647749)

[Step 3 – Request Response 4](#_Toc8647750)

[Step 4 – Completing Certificate Request 4](#_Toc8647751)

[Step 5 – Exporting .pfx File 4](#_Toc8647752)

[Step 6 - Separating private key from certificate for use with .pem extensions 5](#_Toc8647753)

# Installing Internet Information Services (IIS) and Creating Certificates

## Step 1 - Installing IIS

In server manager, use the **add roles and features** option using role-based and feature-based installation. Select the server from the pool. On the Server Roles page, select Web Server (IIS).

Ensure the following options are selected:

Under Common HTTP Features:

* Default Document
* Directory Browsing
* HTTP Errors
* Static Content
* Optional tools: HTTP Redirection, WebDAV Publishing

Under Health and Diagnostics:

* HTTP Logging
* Request Monitor
* Tracing
* Optional tools: Custom Logging, Logging Tools, ODBC Logging

Under Performance:

* Static Content Compression
* Optional tool: Dynamic Content Compression

Under Security:

* Request Filtering
* Optional tools: Basic Authentication, Centralized SSL Certificate Support, Client Certificate Mapping Authentication. Digest Authentication, IIS Client Certificate Mapping Authentication. IP and Domain Restrictions, URL Authorization, Windows Authentication

Under Application Development:

* .NET Extensibility 3.5
* .NET Extensibility 4.6
* ASP.NET 3.5
* ISAPI Extensions
* ISAPI Filters

Under Management Tools:

* IIS Management Console
* Optional Tools: IIS 6 Management Compatibility, IIS Management Scripts and Tools, Management Service

No features on the features page are vital to install. Leave the **Include management tools** box checked.

## Step 2 - Creating Certificate Request

In the start menu, type **Manage computer certificates**. In this certificate manager window, hover over the **Actions** tab, followed by **All tasks**, **Advanced Operations**, then **Create Custom Request**. Select this option.

Ensure **Active Directory Enrollment Policy** is selected and press **Next**.

Under **Template**, select **Web Server** and leave the rest as default.

At the Certificate Information section, press the **arrow next to Details**, then select **Properties**

In the Subject tab, under **Subject name**, select the dropdown menu for Type and select “**Common name**”. For the value, enter the name of the server that hosts the site requiring the certificate, for example: server-01

Under **Alternative name**, select **DNS** and also enter the server’s name there.

Under the **Private Key** tab, under **Key options**, make sure the **Make private key exportable** option is selected.

Press OK and it will prompt you to choose a save location and file name. By default, it will save with no file extension, so **make sure you add .req at the end of the name** so the request will show up in the search later.

## Step 3 – Request Response

In the start menu, type “**certreq**”. You will first be prompted to select the file, then the certification authority, then the name and save location of your new .cer file. **This is not the final certificate.**

## Step 4 – Completing Certificate Request

In **IIS**, select on the local host so the Home page shows up. Under this page, under IIS, there should be a **Server Certificates** option. Select this.

Under **Actions** in the column to the right, select the **Complete Certificate Request** option. The file name containing the certification authority’s response will be the **.cer file created with certreq.** Choose a friendly name and leave the certificate store as Personal. The certificate should show up under Server Certificates.

## Step 5 – Exporting .pfx File

Select the certificate under Server Certificates in IIS. Right click and click Export. Under Export to, navigate to the desired location, and create a password for the .pfx file. **This will be needed later**.

## Step 6 - Separating private key from certificate for use with .pem extensions

To do this task, OpenSSL will need to be installed. Though originally for Linux, there are modified Windows versions available. OpenSSL is a command line based tool, so **command prompt** will need to be opened. To use it, **cd** to the location of the OpenSSL bin files, for example, “C:\Program Files\OpenSSL-Win64\bin”.

Next, use the following commands to change the .pfx file to two .pem files. You may be required to enter the password set for the certificate

To create what will later be turned into the private key file, use: openssl pkcs12 -in \path\certname.pfx -nocerts -out \pathDestination\key.pem – nodes

To create the .pem file, use: openssl pkcs12 -in \path\certname.pfx -nokeys -out \pathDestination\cert.pem

To complete the creation of the key by removing the passphrase from the key and turning it into a key file, use: openssl rsa -in \path\key.pem -out \path\finalkey.key