How to configure SSL in Internet Information Services 7 (IIS 7)

Last Modified on 05/28/2024 5:44 pm EDT

How to configure SSL in Internet Information Services 7 (IIS 7)

Procedure Steps

Summary

HTTP traffic sent between web servers and clients is sent in clear text. This can present a security risk when sending passwords and other sensitive information across the network. Fortunately, the transmission of this data can be encrypted by setting up SSL (Secure Sockets Layer). This article explains how to configure web servers running IIS 7 for SSL. There are three primary steps in doing so: obtaining a certificate, creating an HTTPS binding on the site, and configuring the application to require SSL.

Obtain a Server Certificate

Server certificates can be obtained using an external certificate authority, an internal certificate authority, or by creating a self-signed certificate. Conveniently, IIS 7 provides options to easily obtain a certificate. These options are available in the Server Certificates feature of the Internet Information Services (IIS) Manager. To get there:

1) Open Internet Information Services (IIS) Manager by running the command inetmgr.

2) In the **Connections** pane on the left, select the root server node.

3) Double-click on the **Server Certificates** icon in the **IIS** section.

You will then see the following options in the **Actions** pane on the right:

Create Certificate Request

Use the **Create Certificate Request** option to request a certificate from an external certificate authority. You will be asked to provide the common name for the certificate which must match the site name (i.e. mysite.com). After providing additional information such as your organization's name and address, and after completing the request, a Base64-encoded certificate request file will be generated. This file should then be used to submit a request to the external certificate authority. Once the request has been complete, you will receive the certificate which you can then import using the **Complete Certificate Request** option. See http://technet.microsoft.com/en-us/library/cc731977%28WS.10%29.aspx for more details.

Create Domain Certificate

Use the **Create Domain Certificate** option to request a certificate from an internal certificate authority. If your Windows domain has a server that acts as a certificate authority, then you can use this option to ease certificate deployment and reduce the cost of issuing certificates. You will be asked to provide the common name for the certificate which must match the site name (i.e. mysite.com). After providing additional information such as your organization's name and address, you will be asked to choose the Online Certificate Authority. Your certificate will then be installed after entering the friendly name. See http://technet.microsoft.com/en-us/library/cc731014%28WS.10%29.aspx for more details.

Create Self-Signed Certificate

Use the **Create Self-Signed Certificate** option to create a self-signed certificate. This option issues a certificate to your server and by your server instead of a trusted certificate authority. Therefore this certificate will not be trusted by any clients unless the server's certificate is added to the client **Trusted Root Certification Authorities** certificate store. This option is intended to be used for testing or in scenarios where there is a limited, known group of users. See http://technet.microsoft.com/en-us/library/cc753127%28WS.10%29.aspx for more details.

After you have obtained a server certificate, the certificate must be installed. When using the **Create Domain Certificate** or **Create Self-Signed Certificate** option, this will happen automatically. However, if using the **Create Certificate Request** option, you must install the certificate manually by using the **Complete Certificate Request** option. Once installed, the certificate will be listed in the **Server Certificates** feature of the server connection.

Create an HTTPS Binding on the Site

After installing the server certificate, you then need to configure a protocol binding for SSL for the appropriate website. To do this, follow the steps below.

1) Open Internet Information Services (IIS) Manager by running the command inetmgr.

2) In the **Connections** pane on the left, select the desired website.

3) In the **Actions** pane on the right, select the **Bindings...** link.

4) The **Site Bindings** dialog will appear. Click [Add...].

5) Choose the Type **https**, choose the SSL certificate that you installed in the previous step, then click [OK], then [Close].

Configure the Application to Require SSL

After creating an HTTPS binding for your site, you then should configure the desired application(s) to require SSL. If you skip the steps below and do not configure the application(s) to require SSL, then the application(s) can be accessed with or without a secure connection.

1) Open Internet Information Services (IIS) Manager by running the command inetmgr.

2) In the **Connections** pane on the left, expand the desired website.

3) Click on the desired application in the **Connections** pane.

4) In the **Features** View, double click on **SSL Settings** under the **IIS** section.

5) Select **Require SSL** under **SSL Settings**.

6) Click the **Apply** link in the **Actions** pane on the right.

Test the SSL Configuration

To test the SSL configuration, then you can simply connect to the website using the browse application links provided in IIS. Follow these instructions:

1) Open Internet Information Services (IIS) Manager by running the command inetmgr.

2) In the **Connections** pane on the left, expand the desired website.

3) Click on the desired application in the **Connections** pane.

4) In the **Actions** pane on the right, click the **Browse *:80 (http)** link. If SSL is required for this application, an HTTP 403.4 - Forbidden error should be returned.

5) In the **Actions** pane on the right, click the **Browse *:443 (https)** link. This should load the web site using SSL.*

*If you are using a self-signed certificate, you may receive the following message:
"There is a problem with this website's security certificate."

Also, if you encounter any errors during the configuration, please refer to Installation Guide, Configure SSL.

This is how IIS 7 responds when using a self-signed certificate and accessing the web site using localhost. You can safely click the **Continue to this website (not recommended)** link to continue.

Applies To

OnGuard (All versions)
Browser-based VideoViewer
Browser-based Area Access Manager
Browser-based Visitor Management
Windows Vista
Windows 7
Windows Server 2008

Additional Information

IIS 7 is included on Windows Server 2008, Windows Server 2008 R2, and some editions of Windows Vista and Windows 7.

For additional help, a great video can be found at http://learn.iis.net/page.aspx/378/configuring-ssl-in-iis-manager/ that walks through the configuration using a self-signed certificate and issuing a certificate using an external certificate authority.