How to Configure SSL in IIS 6

Last Modified on 12/21/2021 1:04 pm EST

How to Configure SSL in IIS 6

Procedure Steps

Not sure which version of IIS you have? IIS 6 is included on Windows Server 2003 and Windows XP Professional x64 Edition.

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 6 for SSL. There two primary steps in doing so: obtaining a certificate and configuring the web site 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. IIS 6 provides built-in options to obtain certificates from an internet or external certificate authority. Additional tools can be used to create self-signed certificates.

Requesting Certificates from an a Certificate Authority

To request a certificate from an internal or external certificate authority then you can use the **Web Server Certificate Wizard** provided in IIS 6. To get there:

1. Open Internet Information Services (IIS) Manager by running **inetmgr**.
2. Expand the server node and the **Web Sites** folder.
3. Right click on the desired website and select **Properties**.
4. In the properties dialog, go to the **Directory Security** tab.
5. Next, click [Server Certificate] under the **Secure communications** section. This will open the **Web Server Certificate Wizard**.

Once this wizard has started, you will have the option to **Create a new certificate** amongst other options. Unless you already have an existing certificate, choose the option to create a new certificate. Next, you are provided the options to either **Prepare the request now, but send it later** or **Send the request immediately to an online certificate authority**.

Both options require that you enter information such as the organization's name and geographical

information as well as the certificate's common name. The common name must match the **site's** fully qualified domain name for internet use, or for intranet use it can also be the NetBIOS name.

Prepare the request now, but send it later

This option should be used if you do not have an enterprise certificate authority, if the server requesting the certificate does not belong to the same domain as the enterprise certificate authority or does not trust that domain, if you are using a standalone certificate authority, or if you are obtaining a certificate from a third-party certificate authority.

With this option, a Base64-encoded certificate request file will be generated. This file should then be used to submit a request to the certificate authority. Once the request has been complete, you will receive the certificate which you can then import. To import the certificate, then simply return back to the **Web Server Certificate Wizard** as described in the steps above. However, when starting this wizard after generate the certificate request file, you will be given two new options: **Process the pending request and install the certificate** and **Delete the pending request**. Simply select the first option to process the request, and then provide the path to the certificate that you received the from external certificate authority. Once this wizard is complete, you will now have a server certificate installed.

Send the request immediately to an online 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. With this option, instead of generating a certificate request file, you will be able to select an internal certificate authority. When the certificate request completes, the server certificate is installed and bound to the web site.

Create a Self-Signed Certificate

A self-signed certificate is a certificate that is issued by your server and to your server instead of by 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. IIS 6, unfortunately, does not have an option to create self-signed certificates. However, the **IIS 6.0 Resource Kit Tools** provides an application, called **SelfSSL**, that can be used to automatically generate and install a self-signed certificate. See http://support.microsoft.com/kb/840671 for more details.

Configure the Web Site to Require SSL

After installing the server certificate, you should configure the web site require SSL. If skip this step and do not configure the site to require SSL, then the site can be accessed with **or without** a secure connection. To configure the site to *require* SSL, then following these instructions:

1. Open Internet Information Services (IIS) Manager by running **inetmgr**.
2. Expand the server node and the **Web Sites** folder.
3. Right click on the desired website and select **Properties**. Select or directory or page within the

site if you want to secure only a portion of the site, instead of the whole thing.
4. In the properties dialog, go to the **Directory Security** tab.
5. Under the **Secure communications** section, click [Edit].
6. Place a checkmark by **Require secure channel (SSL)**.

Test the SSL Configuration

To test the SSL configuration, then you can simply navigate to the website in your browser. If you browse to the site using **http** and you have made SSL required for the site, then you should get an **HTTP 403.4 - Forbidden error**. Using **https**, you should be able to view your web site*.

*If you are using a self-signed certificate, you may receive a message saying: **There is a problem with this website's security certificate**. You can safely press the **Continue to this website (not recommend)** link to continue.

Applies To

Browser-Based Applications
OnGuard (All versions)
Windows Server 2003
Windows XP

Additional Information