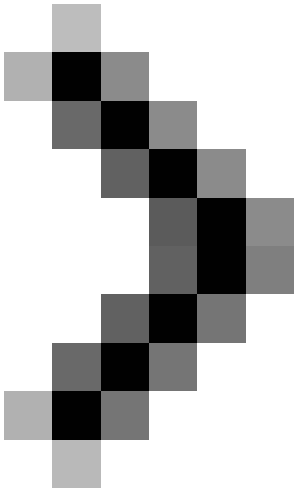
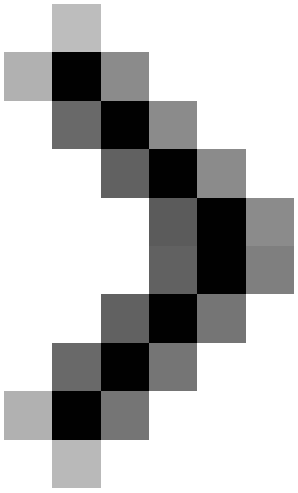
Configure IIS for an FTP Site - Part 3

In this article, I will continue the discussion by showing you how to configure IIS for an FTP site by enabling SSL encryption.



Configure IIS for an FTP Site - Part 1



Configure IIS for an FTP Site - Part 2
Brien M. Posey

In this article, I will continue the discussion by showing you how to configure IIS for an FTP site by enabling SSL encryption.

Introduce

In the previous article of this series, I showed you how to get IIS 7.0. In this section, we will show you how to add SSL encryption to the FTP site.

Collect SSL certificates

Before the FTP server can provide SSL encryption, you need to have an X.509 certificate. You can purchase a certificate from a commercial certificate authority (CA), such as VeriSign or Thawte, or you can use an organization's CA to issue certificates.

For the purposes of the article, we will assume that you have a configured Windows 2008 server to act as an enterprise CA. We will then show you how to issue a certificate request and how to download the necessary certificate in the next section. If you have obtained an SSL certificate from a commercial certificate authority, then you can skip this section and move on to the next section.

To use SSL encryption, we need to issue a request to the enterprise CA. For the purpose of the article, we assume that your FTP server is a member of the Active Directory forest.

To request a certificate, open Internet Explorer, enter the URL associated with your Enterprise Certificate Authority. By default, the URL will be **https: /// CertSrv** . When entering this URL, you usually have to enter the full domain name of the Enterprise Certificate Authority instead of entering the server's NetBIOS name.

When you enter the Enterprise Certificate Authority URL, log into Active Directory Certificate Services, the Web site adds the domain administrator (if needed). After doing so, click on the ' **Request a Certificate** ' link. You will see a screen appear asking you to choose between requesting a user certificate or submitting an advanced certificate request. Click on the second option, **Advanced Certificate Request** .

The following screen will allow you to issue a request directly to the certificate authority or upload a certificate request file that is encrypted in Base-64 or PKCS # 10 format. Click on the ' **Create and Submit a Request to This CA** ' link.

Here, you will be prompted to install the ActiveX control. If you encounter this prompt, go ahead and perform the control installation.

You will then be taken to the **Advanced Certificate Request** main screen. Select the **Web Server** option from the **Certificate Template** drop-down list. You must now enter some basic identifying information to be included in your certificate. This information includes: your name, email address, and phone number.

In the Key Options section, select the **Create a New Key Set option.** You should verify that the **Cryptographic Service Provider (CSP)** is set to **Microsoft RSA SChannel Cryptographic Provider** , and that the **Key Size** is set to **1024** , as shown in Figure A.

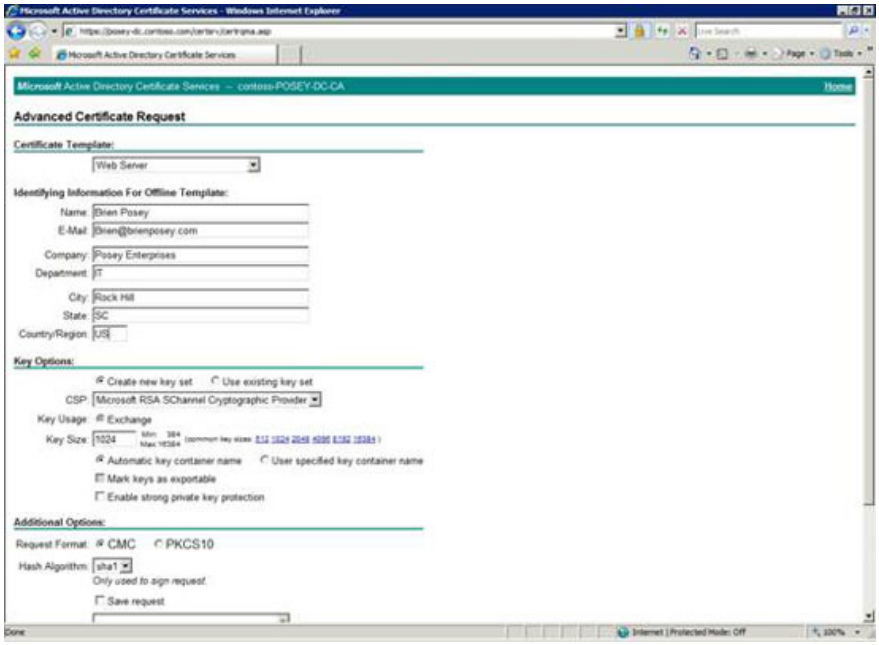


Figure A: You must ensure that the Cryptographic Service Provider (CSP) is set to Microsoft RSA SChannel Cryptographic Provider and Key Size is set to 1024

At this point, scroll down and find below the interface, click the **Submit** button. You will see a warning message telling you that the Web site is creating a certificate request. Click Yes to allow that request to pass. When the

process is complete, you will see a message, indicating that the certificate has been issued to you and asking if you want to install it. Please continue to click on the ' **Install This Certificate** ' link. Next, you will see a message telling you that the Web site is installing the certificate. Click **Yes** to allow that operation.

You will see a message saying that the certificate has been successfully created, but we need to make sure that. To do so, enter the **MMC** command at the **Run** prompt on your FTP server. Windows will then open an empty instance for Microsoft Management Console. Here, you must select the **Add / Remove Snap-In** command from the console's File menu. Windows will then display the **Add or Remove Snap-ins** dialog box.

Select the Certificates option from the list of available snap-ins. You will be asked whether the console is used to manage certificates for your user account, service account or computer account. Select the **Computer Account** option and click the **Next** button.

The next screen will ask if you want to manage certificates for your local computer or manage certificates for client computers on the network. Make sure the **Local Computer** option is checked, then click the **Finish** button and **OK** .

The console will now load the **Certificates snap-in** . You must navigate through the console tree to enter **Console Root | Certificates (Local Computer) | Personal | Certificates.** When choosing **Certificates** , the Details panel will show you the certificate that has been issued.

Enable SSL for FTP Server

At this point, we have an SSL certificate, this is where we can enable SSL encryption for our FTP server. Open **Internet Information Services (IIS) Manager** . Navigate through the interface tree to look to **| Sites | .** With your FTP site selected, double-click the **FTP SSL settings** icon in the Details section.

The console will now display the FTP SSL Settings page. Select the **SSL certificate** from the SSL Certificate drop-down list, as shown in Figure B. You can then choose to allow SSL connections or SSL connection requests. 128 bit encryption can also be selected for stronger security features. Click the **Apply** button to save your changes.

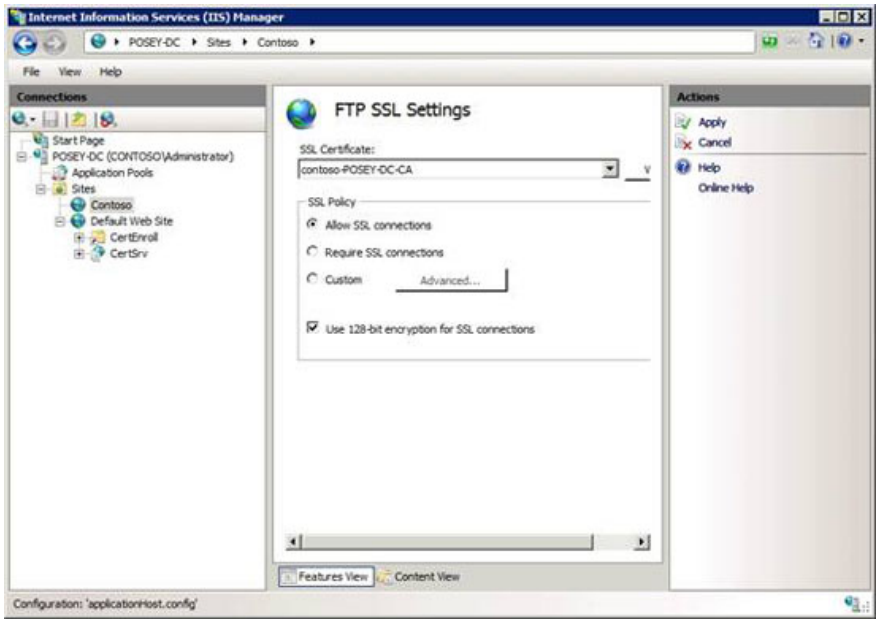


Figure B: Select the certificate from the SSL Certificates list

Use SSL or not use SSL?

One of the drawbacks to using SSL encryption is that this encryption process will increase the CPU's workload. The extended workload will be worth it if you are transmitting or receiving sensitive information or if the FTP site is only used occasionally. If you avoid the FTP site being used too heavily, you need to perform a test to ensure that the encryption process does not cause performance problems for the server.

We recommend that you check the Performance Monitor Processor /% Processor Time counter before and after SSL encryption is enabled. The spikes in the CPU action are perfectly normal, but the average use efficiency needs to be maintained below 80% or your CPU is having problems serving its demanding needs.

Conclude

The ability to encrypt FTP sites must be an interesting thing, but that's not all because you can still log in to the FTP site anonymously without security, even if SSL encryption is enabled. . In Part 4 of this series, I will talk about authentication for FTP sites.