Using Client Certificate Authentication with IIS 6.0 Web Sites

Date: Jun 24, 2004
Section: Articles :: Web Server Security
Author: Thomas Shinder
Printable Version
Rating: 4.6 / 5 - 10 Votes

1 2 3 4 5 ○ ○ ○ ○ ○ Rate this article

In spite of the fact that there's no such thing as a secure network, there are still a lot of things you can do that doesn't require you to take a second mortgage on your home and thousands of man-hours. This is especially true when it comes to providing secure access to Microsoft IIS Web servers.

What methods do you use to control access to your secure Web sites? Do you require authentication? If so, what type of authentication? Are the users' credentials passed in clear text? Do you secure data moving between the Web site and the client, or can anyone with a network sniffer read all the data moving between the Web client and the Web server?

The definition of *secure* is a moving target. If you talk to the security wonks, they'll tell your configuration is not secure, and that you'll have to spend untold number of dollars and administrator hours to correct the security flaws in your network. Meanwhile, if you were to go to the security consultant's home, you'll find he has glass windows and clear glass panes on his doors which are easily breakable. Any run-in-the-mill burglar can make off with his stereo and laptop computer sitting on the desk inside.

When we put together a secure Web site (for employee access, not for e-commerce as e-commerce sites have an entire different set of requirements), we require *two factor* authentication. Two factor authentication requires two methods be used when accessing content on the secure Web site. For example, one factor can be the username and password, and the second factor can be biometric input, such as a fingerprint. The two factor authentication methods typically depend on *what I know* and *what I have*.

Most two-factor authentication schemes require very pricey third party devices that provide the *what I have* component. The most popular two-factor authentication method is RSA SecurID. The SecurID token generates a one time password users use when they authenticate with a secure Web site. SecurID is a very powerful two-factor authentication scheme and I highly recommend it for organizations that can afford it.

Even if you don't have hoards of excess cash, you can still benefit from two factor authentication. If you have a Windows 2000 or Windows Server 2003 Server (such as the domain controller in your Active Directory domain), then you can put together your own two-factor authentication scheme. You can install a Microsoft Certificate Server on the Windows Server machine and issue user certificates to your users. Then you can configure your Web site to require both username and password *and* a user certificate. The user certificate is the *what I have* piece of the two factor authentication scheme.

In this article we'll go over procedures required to make this two-factor authentication method work. You'll need to do the following:

- Install IIS 6.0 on the Windows Server 2003 computer
- Create an offline certificate request file using the Web Site Certificate Wizard
- Submit the offline certificate request to the Certificate Server using the Web Enrollment Site
- Install the Web site certificate
- Install the CA certificate
- Configure the Web site to require a client certificate and use basic authentication
- Request a User Certificate from the Web enrollment site
- Make the connection to the Web site

Our sample network includes a Windows XP client machine, a Windows Server 2003 Web server and a Windows Server 2003 domain controller that has an enterprise CA installed on it. The enterprise CA must be installed on a machine that is a member of an Active Directory domain. We will use the Web enrollment site on the enterprise CA to obtain certificates. Note that you can also use a standalone CA, which does not require an Active Directory domain. The user interface on the standalone CA differs a bit from the enterprise CA's Web enrollment site, but the same principles apply.

Install IIS 6.0 on the Windows Server 2003 Computer

We will use an IIS 6.0 Web server in our example. You can also use IIS 5.0 and the procedures are essentially the same, although the Web Site Certificate Request Wizard looks a little different, the basic functionality and procedures are the same.

The first step is to install the IIS WWW service on the Web server computer. We need to do this because unlike Windows 2000 where the WWW is installed by default, it is not installed by default on a Windows Server 2003 server.

Perform the following steps to install the IIS 6.0 WWW service on the Windows Server 2003 machine that will act as the Web server:

1. Click **Start** and point to **Control Panel**. Click the **Add or Remove Programs** link.

2. In the **Add or Remove Programs** window, click the **Add/Remove Windows Components** button.

3. In the **Windows Components** window, click the **Application Server** entry in the **Components** list and then click **Details**.

4. In the **Application Server** dialog box, put a checkmark in the **Internet Information Services (IIS)** checkbox. Click **OK**.

5. Click **Next** on the **Windows Components** page.

6. Click **OK** on the **Insert Disk** dialog box. In the **Files Needed** dialog box, enter the path to the **i386** folder on the Windows Server 2003 CD in the **Copy files from** text box. Click **OK**.

7. Click **Finish** when the Wizard is completed.

Create an Offline Certificate Request File using the Web Site Certificate Wizard

Now that the Web site is installed, we can create an offline request to obtain a Web site certificate.

There are two ways you can make a request for a certificate from a Microsoft Certificate Server: via an offline request and via the Certificates MMC. The Web site machine must be a member of the same domain as the Certificate Server if you want to use the Certificates MMC. In our example, the Web server is not a member of the domain, so we must first generate an offline certificate request file and then submit this file to the Certificate Server using the Certificate Server's Web enrollment site.

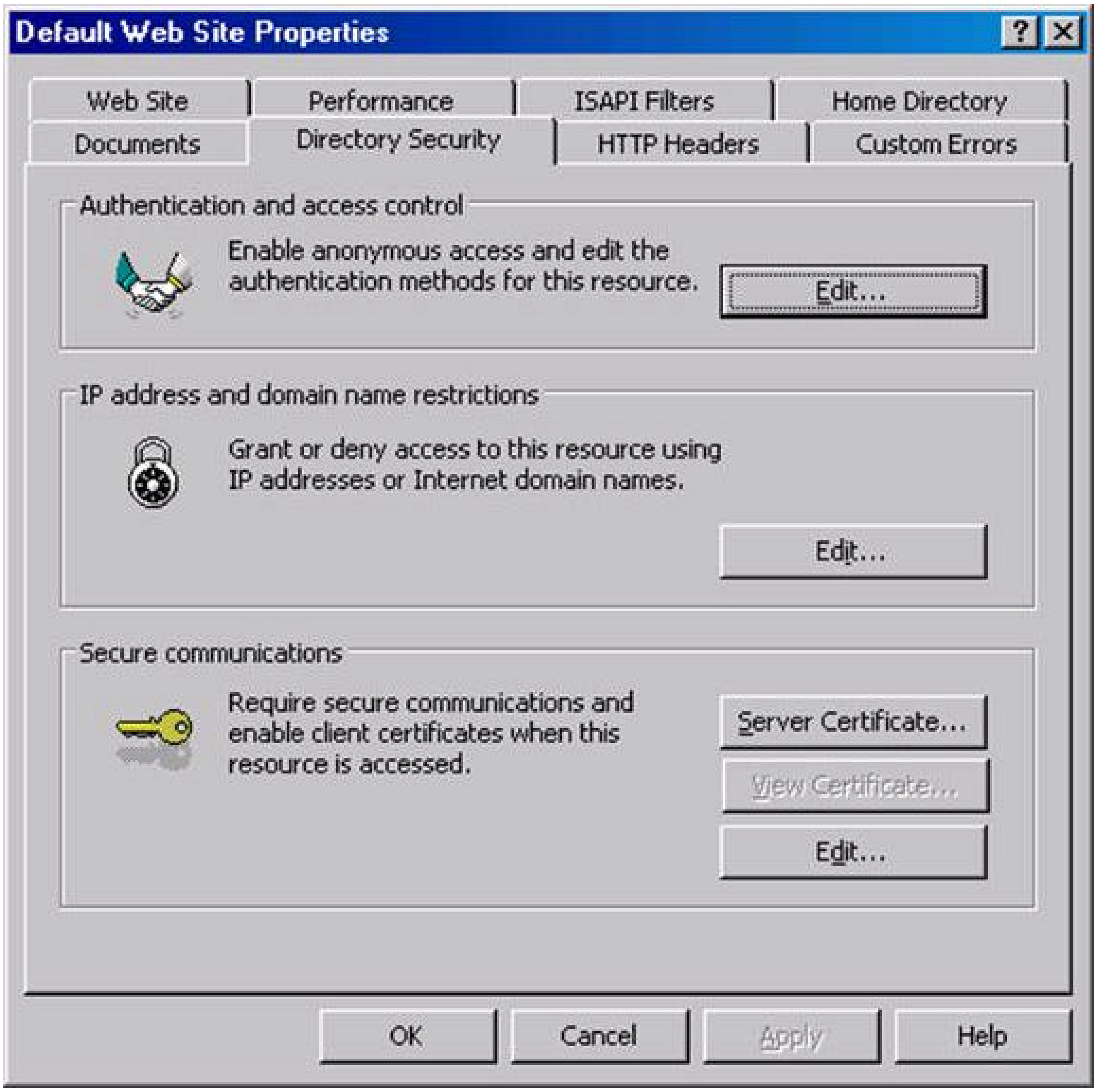
Perform the following steps on the Web server to generate the certificate request file:

1. Click **Start** and then point to **Administrative Tools**. Click the **Internet Information Services (IIS) Manager** link.

2. In the **Internet Information Services (IIS) Manager** console, expand the **Web Sites** node and click on the **Default Web Site** node. Right click on the **Default Web Site** node and click **Properties**.

3. On the **Default Web Site Properties** dialog box, click the **Directory Security** tab.

4. On the **Directory Security** tab, click the **Server Certificate** button in the **Secure Communications** frame.


Default Web Site Properties
Web Site
Performance
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
Authentication and access control
Enable anonymous access and edit the authentication methods for this resource.
Edit...
IP address and domain name restrictions
Grant or deny access to this resource using IP addresses or Internet domain names.
Edit...
Secure communications
Require secure communications and enable client certificates when this resource is accessed.
Server Certificate...
View Certificate...
Edit...
OK
Cancel
Apply
Help

5. Click **Next** on the **Welcome to the Web Server Certificate Wizard** page.

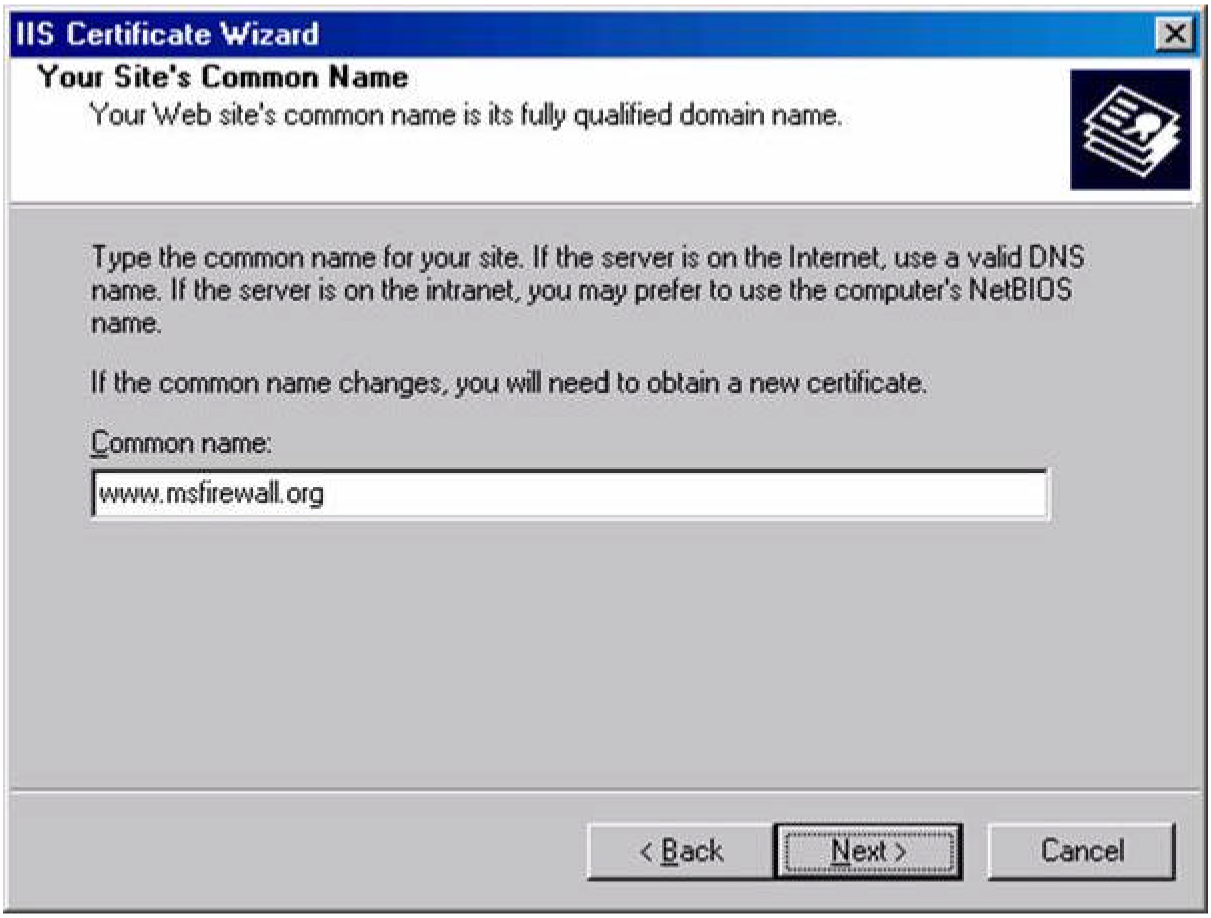
6. On the **Server Certificate** page, select the **Create a new certificate** option and click **Next**.

7. On the **Delayed or Immediate Request** page, note that the only option available to you is the **Prepare the request now, but send it later**. The reason for this is that the Web server is not a member of a domain that has an enterprise CA. Accept the default option and click **Next**.

8. On the **Name and Security Settings** page, accept the default values and click **Next**.

9. On the **Organization Information** page, enter the name of your organization in the **Organization** text box and enter the name of your organizational unit in the **Organizational Unit** text box. Click **Next**.

10. On the **Your Site's Common Name** page, enter the name of the Web site in the **Common name** text box. This is an extremely important entry. The name you put into this text box must be exactly the same as the name the users use to access the Web site. In this example, we will enter **www.msfirewall.org** into the text box. When users access this site, they will enter into their browsers **http://www.msfirewall.org**. Click **Next**.



Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:

www.msfirewall.org

11. On the **Geographical Information** page, enter your **State/Province** and **City/locality** in the text boxes and click **Next**.

12. On the **Certificate Request File Name** page, accept the default location for the **certreq.txt** file and click **Next**. (Note that the file is located in the root of the C:\ drive; we'll retrieve that file later when we make our certificate request to the Certificate Server).

13. Review the information on the **Request File Summary** page and click **Next**.

14. Click **Finish** on the **Completing the Web Server Certificate Wizard** page.

15. Click **OK** on the **Default Web Site Properties** dialog box.

Submit the Offline Certificate Request to the Certificate Server using the Web Enrollment Site

We can use the certificate request file created by the Web Site Certificate Wizard to request a Web site certificate from the enterprise CA we installed on our domain controller. To accomplish this task, we will open the Certificate Server's Web enrollment site and send the request.

Perform the following steps to send the Web site certificate request to the enterprise CA:

1. Open **Internet Explorer** on the Web server machine and enter **http://10.0.0.2/certsrv** in the address bar, where **10.0.0.2** is the IP address of the Certificate Server. Press ENTER.

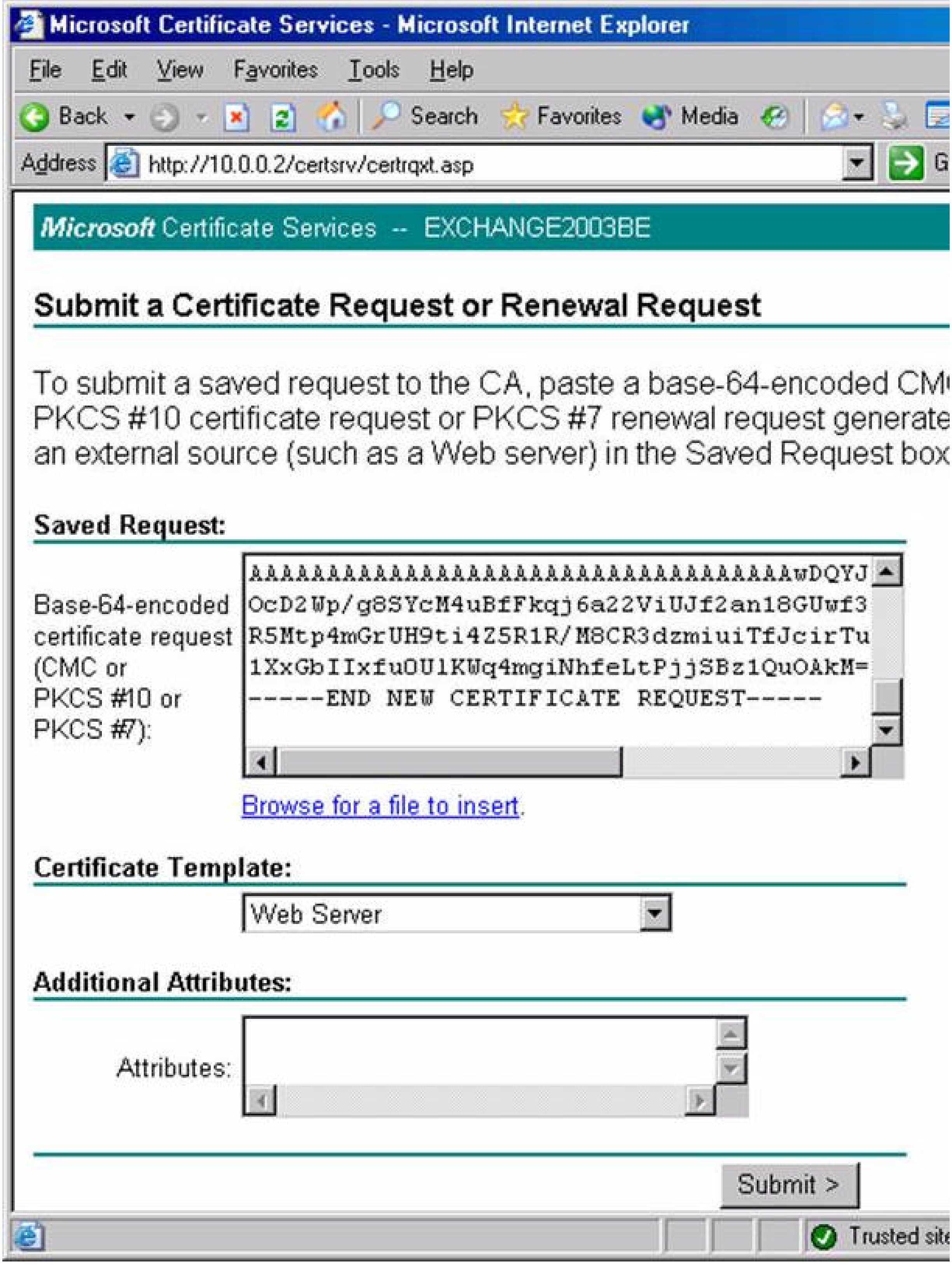
2. Enter domain administrator credentials in the authentication dialog box and click **OK**.

3. On the **Welcome** page of the Web enrollment site, click the **Request a certificate** link at the bottom of the page.

4. On the **Request a Certificate** page, click the **advanced certificate request** link.

5. On the **Advanced Certificate Request** page, click the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** link.

6. On the **Submit a Certificate Request or Renewal Request** page, copy the contents of the **certreq.txt** file into the **Saved Request** text box. Open the **certreq.txt** file and then press **CTRL+A** to select all the text. Then press **CTRL+C** to copy all the text to the clipboard. Go to the Web browser windows and click in the **Saved Request** text box and press **CTRL+V** to paste the contents of the **certreq.txt** file into the text box. Select the **Web Server** template from the **Certificate Template** list. Click the **Submit** button.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://10.0.0.2/certsrv/certrqxt.asp
G
Microsoft Certificate Services -- EXCHANGE2003BE
Browse for a file to insert.
Submit >
Trusted site

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM
PKCS #10 certificate request or PKCS #7 renewal request generate
an external source (such as a Web server) in the Saved Request box

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwDQYJ
OcD2Wp/g8SYcM4uBfFkqj6a22ViUJf2an18GUwf3
R5Mtp4mGrUH9ti4Z5R1R/M8CR3dzmiuiTfJcirTu
1XxGbIIxfuOU1KWq4mgiNhfeLtPjjSBz1QuOAkM=
-----END NEW CERTIFICATE REQUEST-----
```

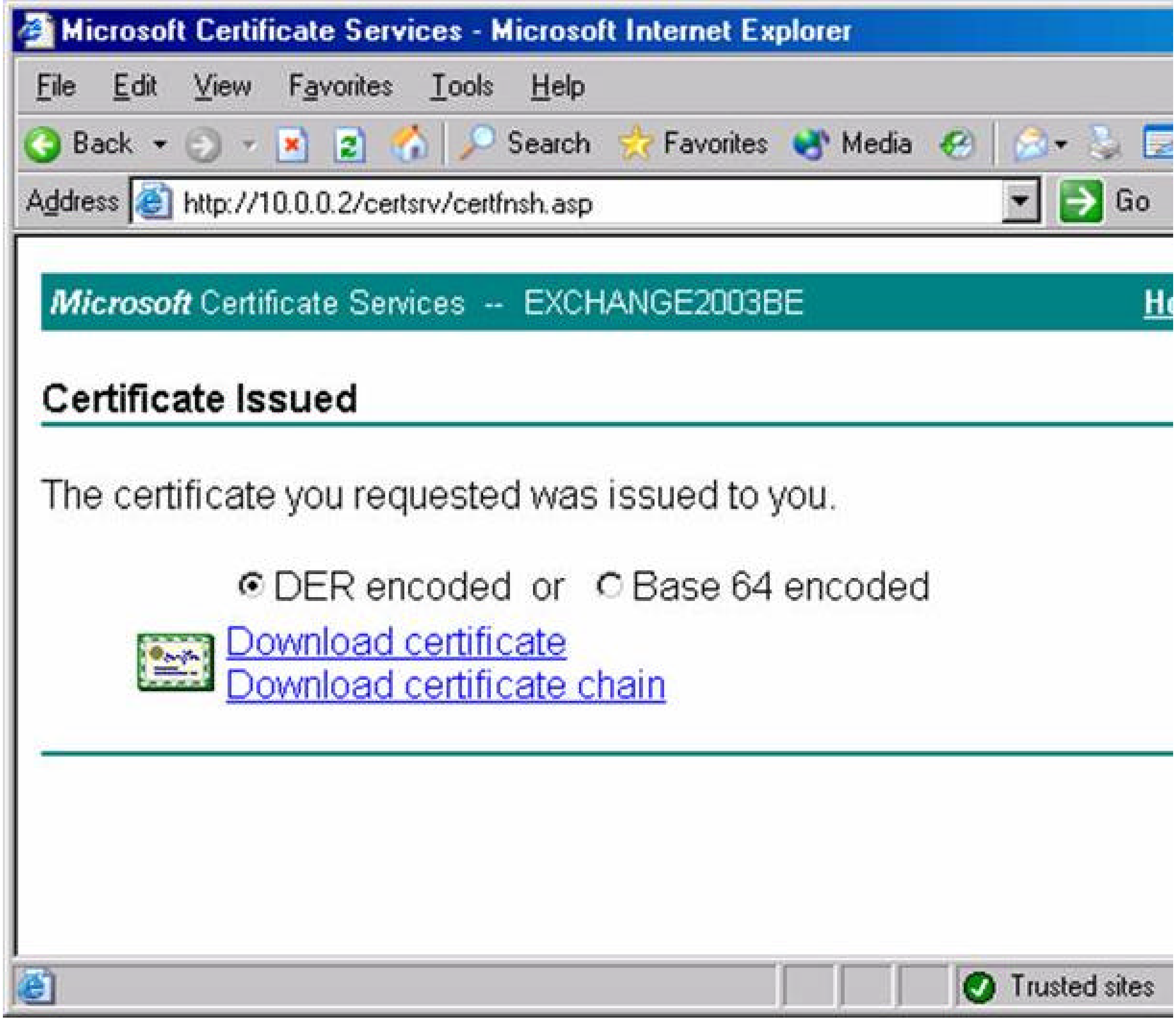
Certificate Template:

Web Server

Additional Attributes:

Attributes:

7. On the **Certificate Issued** page, click the **Download certificate** link.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.0.2/certsrv/certfnsh.asp
Go
Microsoft Certificate Services -- EXCHANGE2003BE
Trusted sites

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

8. In the **File Download** dialog box, click the **Save** button. Save the file to the Desktop. Click the **Close** button.

9. On the **Certificate Issued** page, click the **Download certificate chain** link.

10. In the **File Download** dialog box, click the **Save** button. Save the file to the Desktop. Click the **Close** button.

11. Close **Internet Explorer**.

Install the Web Site Certificate

We've downloaded the Web site certificate and CA certificate files from the Web enrollment site. The next step is install these certificates on the Web server. We'll begin by installing the Web site certificate and then we'll install the CA certificate.

Perform the following steps to install the Web site certificate on the Web server:

1. At the Web server machine, click **Start** and point to **Administrative Tools**. Click the **Internet Information Services (IIS) Manager** link.

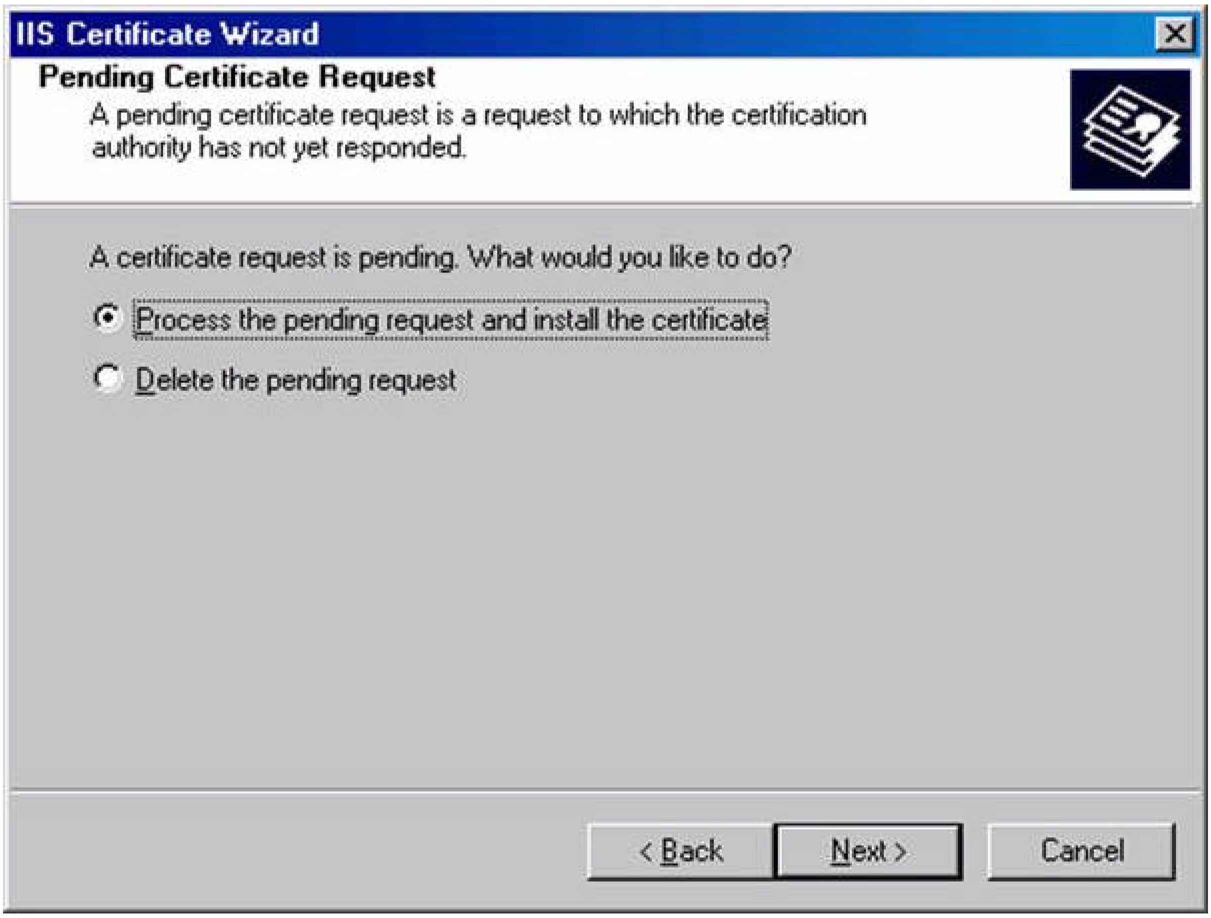
2. Expand the **Web Sites** node in the left pane of the console and then click on the **Default Web Site**. Right click on the **Default Web Site** and click **Properties**.

3. In the **Default Web Site Properties** dialog box, click the **Directory Security** tab.

4. On the **Directory Security** tab, click the **Server Certificate** button.

5. Click **Next** on the **Welcome to the Web Server Certificate Wizard** page.

6. On the **Pending Certificate Request** page, select the **Process the pending request and install the certificate** option and click **Next**.



IIS Certificate Wizard

Pending Certificate Request

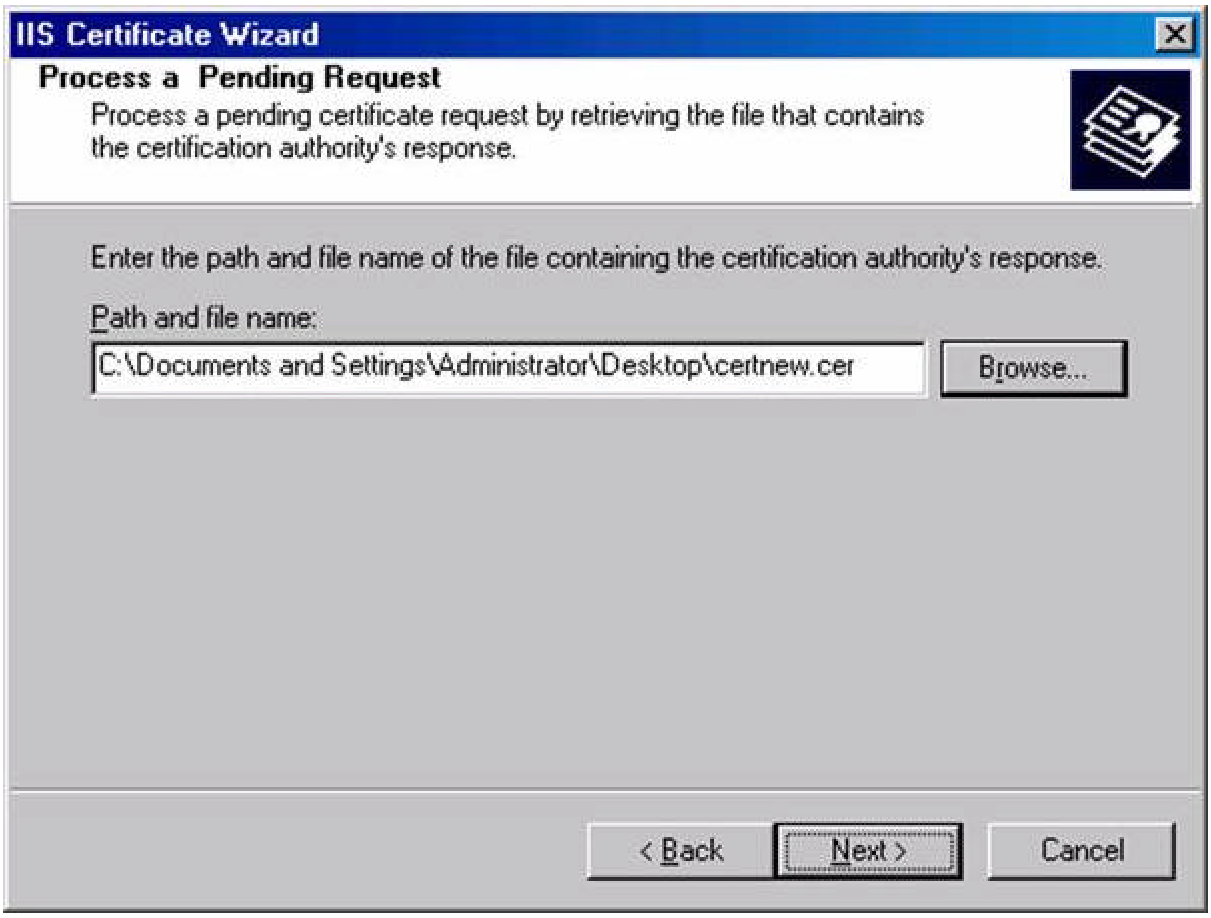
A pending certificate request is a request to which the certification authority has not yet responded.

A certificate request is pending. What would you like to do?

● Process the pending request and install the certificate

○ Delete the pending request

7. On the **Process a Pending Request** page, click the **Browse** button and locate the **.cer** file for the Web site certificate.



Process a Pending Request

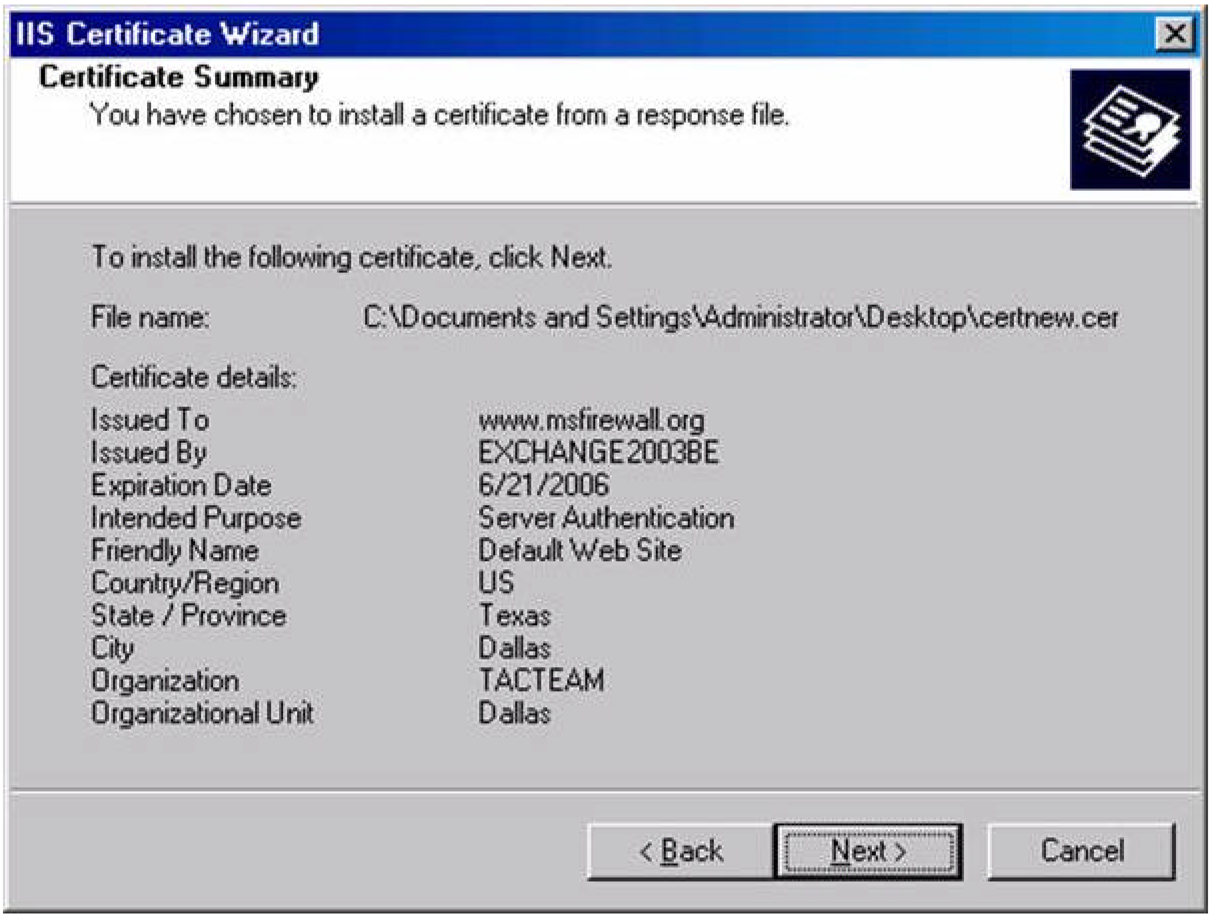
Process a pending certificate request by retrieving the file that contains the certification authority's response.

Enter the path and file name of the file containing the certification authority's response.

Path and file name: C:\Documents and Settings\Administrator\Desktop\certnew.cer

8. On the **SSL Port** page, accept the default SSL port, which is **443**. Click **Next**.

9. On the **Certificate Summary** page, review your settings and click **Next**.



You have chosen to install a certificate from a response file.

To install the following certificate, click Next.

File name: C:\Documents and Settings\Administrator\Desktop\certnew.cer

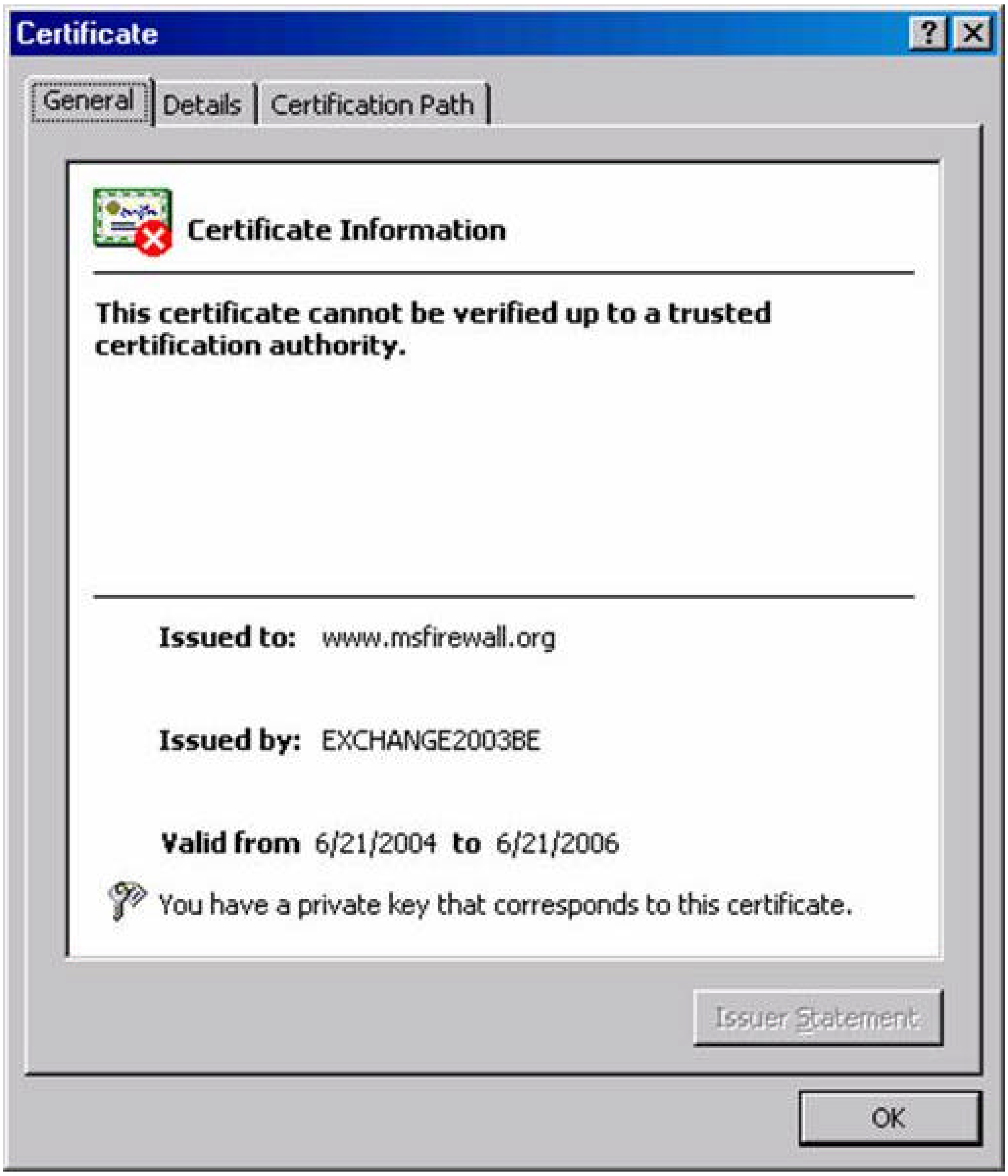
Certificate details:

Issued To	www.msfirewall.org
Issued By	EXCHANGE2003BE
Expiration Date	6/21/2006
Intended Purpose	Server Authentication
Friendly Name	Default Web Site
Country/Region	US
State / Province	Texas
City	Dallas
Organization	TACTEAM
Organizational Unit	Dallas

10. Click **Finish** on the **Completing the Web Server Certificate Wizard** page.

11. On the **Directory Security** tab, click the **View Certificate** button.

12. In the **Certificate** dialog box, click the **General** tab. Note that the **Issued to** name is **www.msfirewall.org**. This is the common name on the certificate. Notice that there is a red “X” on the certificate at the top of the dialog box.



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: www.msfirewall.org

Issued by: EXCHANGE2003BE

Valid from 6/21/2004 to 6/21/2006

You have a private key that corresponds to this certificate.

13. Click on the **Certification Path** tab. Notice that there is a red “X” on the root CA. This indicates that the CA certificate of the root CA is not in the **Trusted Root Certification Authorities** list on the Web server. We will fix this problem in the next procedure.

14. Click **OK** in the **Certificate** dialog box.

15. Click **OK** in the **Default Web Site Properties** dialog box.

Install the CA Certificate

We need to install the Root CA certificate in the **Trusted Root Certification Authorities** store on the Web server machine. This allows the Web server to trust the Web site certificate installed on the IIS Web site.

Perform the following steps to install the root CA certificate into the machine’s certificate store:

1. Click **Start** and then click the **Run** command.

2. In the **Run** dialog box, enter **mmc** in the **Open** text box and click **OK**.

3. In the **Console1** window, click the **File** menu and click the **Add/Remove Snap-in** command.

4. In the **Add/Remove Snap-in** dialog box, click the **Add** button.

5. In the **Add Standalone Snap-in** dialog box, select the **Certificates** entry in the **Available Standalone Snap-ins** dialog box and click **Add**.

6. On the **Certificates snap-in** page, select the **Computer account** option and click **Next**.

7. On the **Select Computer** page, select the **Local computer** option and click **Finish**.

8. Click **Close** in the **Add Standalone Snap-in** dialog box.

9. Click **OK** in the **Add/Remove Snap-in** dialog box.

10. Expand the **Certificates** node and then expand the **Trusted Root Certification Authorities** node and click on the **Certificates** node. Right click on the **Certificates** node, point to **All Tasks** and click **Import**.

11. Click **Next** on the **Welcome to the Certificate Import Wizard** page.

12. On the **File to Import** page, click the **Browse** button and locate the **certnew.p7b** file you downloaded from the Web enrollment site. Click **Next**.

13. On the **Certificate Store** page, accept the default setting, **Place all certificates in the following store** and click **Next**.

14. Click **Finish** on the **Completing the Certificate Import** page.

15. Click **OK** in the **Certificate Import Wizard** dialog box informing you that the import was successful.

Configure the Web Site to Require a Client Certificate and use Basic Authentication

Now that our certificates are in place, we can configure the Web server's authentication and SSL settings. Since we want a secure Web server, we'll force users to use SSL when connecting to the site. SSL will encrypt the user credentials and data moving between the Web client and the Web server. We will also force Integrated authentication, which is more secure than basic authentication. However, the type of authentication used is not so important in this scenario, since the user credentials are protected by SSL. Finally we will configure the Web site to require a user certificate.

Perform the following steps to configure the security settings on the Web site:

1. Click **Start** and point to **Administrative Tools**. Click **Internet Information Services (IIS) Manager**.

2. In the **Internet Information Services (IIS) Manager** console, expand the server name and expand the **Web Sites** node. Click on **Default Web Site** and right click on it. Click **Properties**.

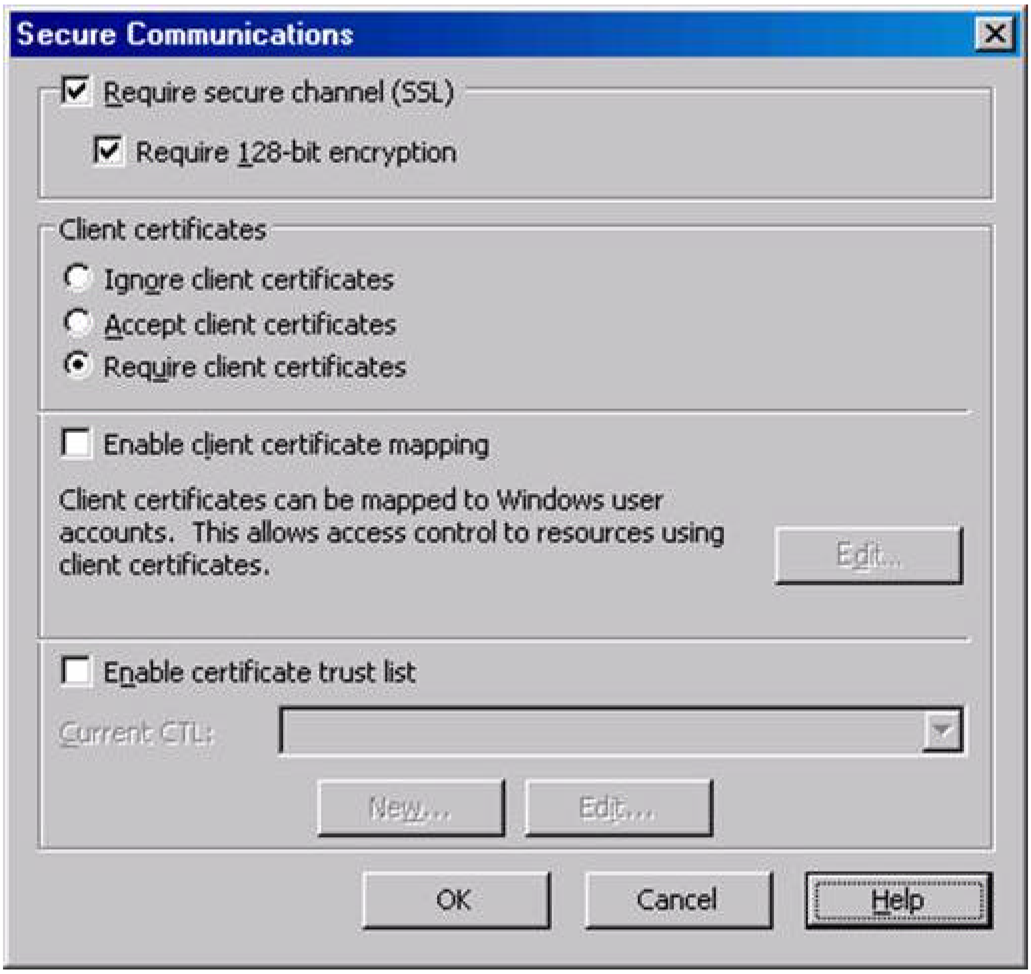
3. In the **Default Web Site Properties** dialog box, click the **Directory Security** tab.

4. On the **Directory Security** tab, click the **Edit** button in the **Authentication and access control** frame.

5. In the **Authentication Methods** dialog box, remove the checkmark from the **Enable anonymous access** checkbox. The only checkbox that should be selected is the **Integrated Windows authentication** checkbox. Click **OK**.

6. On the **Directory Security** tab, click the **Edit** button in the **Secure communications** frame.

7. Place a checkmark in the **Require secure channel (SSL)** checkbox and put a checkmark in the **Require 128-bit encryption** checkbox. Select the **Require client certificates** option in the **Client certificates** frame. Click **OK** in the **Secure Communications** dialog box.



Secure Communications

☑ Require secure channel (SSL)

☑ Require 128-bit encryption

Client certificates

○ Ignore client certificates

○ Accept client certificates

● Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

8. Click **Apply** and then click **OK** in the **Default Web Site Properties** dialog box.

Request a User Certificate from the Web Enrollment Site

The client computer must present a user certificate to the Web server before the Web server will accept the user's credentials. Users can log on to the Web enrollment site and request a user certificate. The user does *not* need to be an administrator in the domain or on the Certificate Server computer. The user only needs to have legitimate user credentials that the enterprise CA recognizes.

Perform the following steps on the client computer to obtain the user certificate"

1. On the Web client computer, open Internet Explorer and enter **http://10.0.0.2/certsrv** in the address bar, where **10.0.0.2** is the IP address of the Certificate Server. Press ENTER.

2. In the log on dialog box, enter the credentials of a non-administrator user. This will demonstrate that a non-admin can obtain a user certificate. Click **OK**.

3. On the **Welcome** page of the Web enrollment site, click the **Request a certificate** link.

4. On the **Request a Certificate** page, click the **User Certificate** link.

5. On the **User Certificate – Identifying Information** page, click **Submit**.

6. Click **Yes** on the **Potential Scripting Violation** dialog box informing you that the Web site is requesting a certificate on your behalf.

7. On the **Certificate Issued** page, click the **Install this certificate** link.

8. Click **Yes** on the **Potential Scripting Violation** page informing you that the Web site is adding a certificate to the machine.

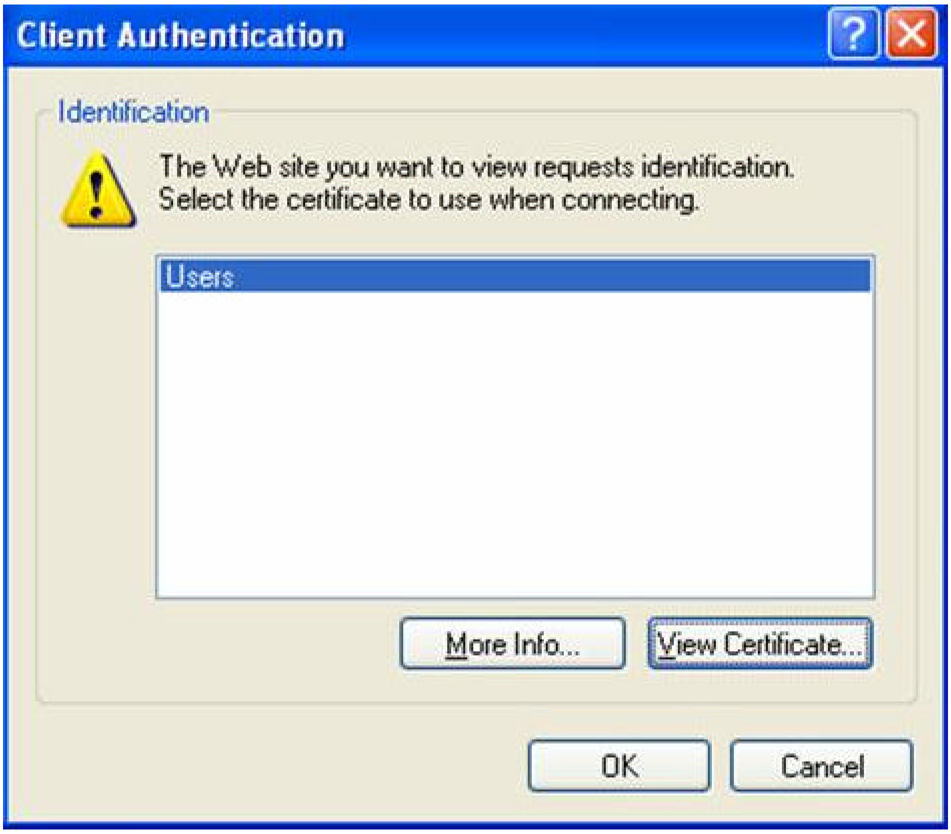
9. Close **Internet Explorer** after you see the **Certificate Installed** page.

Make the Connection to the Web Site

Now we're ready to see if our settings actually work! Perform the following steps to connect to the secure Web site:

1. Open **Internet Explorer** and enter **https://www.msfirewall.org** into the Address bar, where **www.msfirewall.org** resolves to the IP address of the Web server.

2. A **Client Authentication** dialog box appears and shows a **Users** certificate in the list. Click the **View Certificate** button.



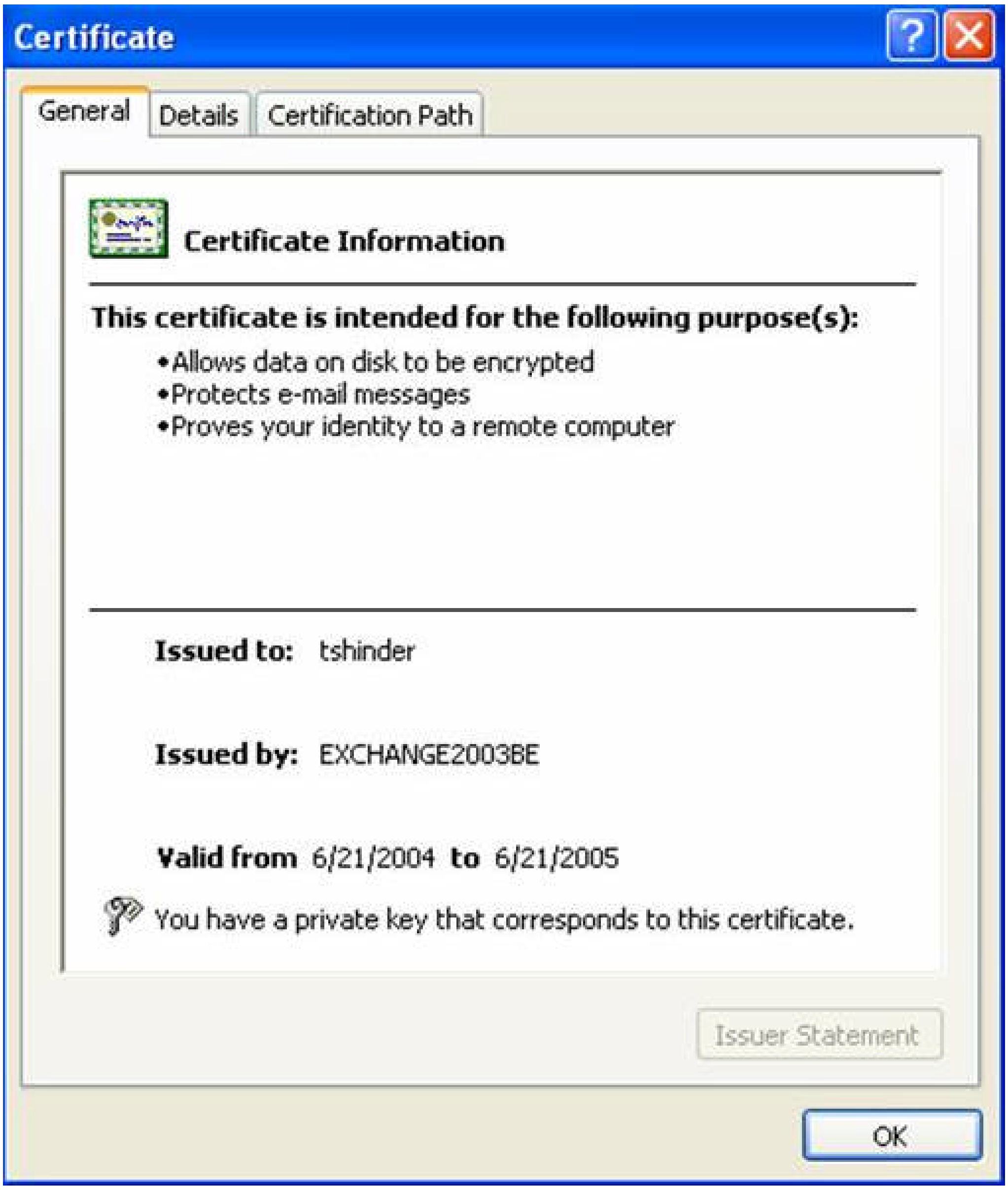
Client Authentication

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

Users

3. In the **Certificate** dialog box you can see the **Issued to** name is the name of the user who requested the certificate. Click **OK**.



Certificate Information

This certificate is intended for the following purpose(s):

- Allows data on disk to be encrypted
- Protects e-mail messages
- Proves your identity to a remote computer

Issued to: tshinder

Issued by: EXCHANGE2003BE

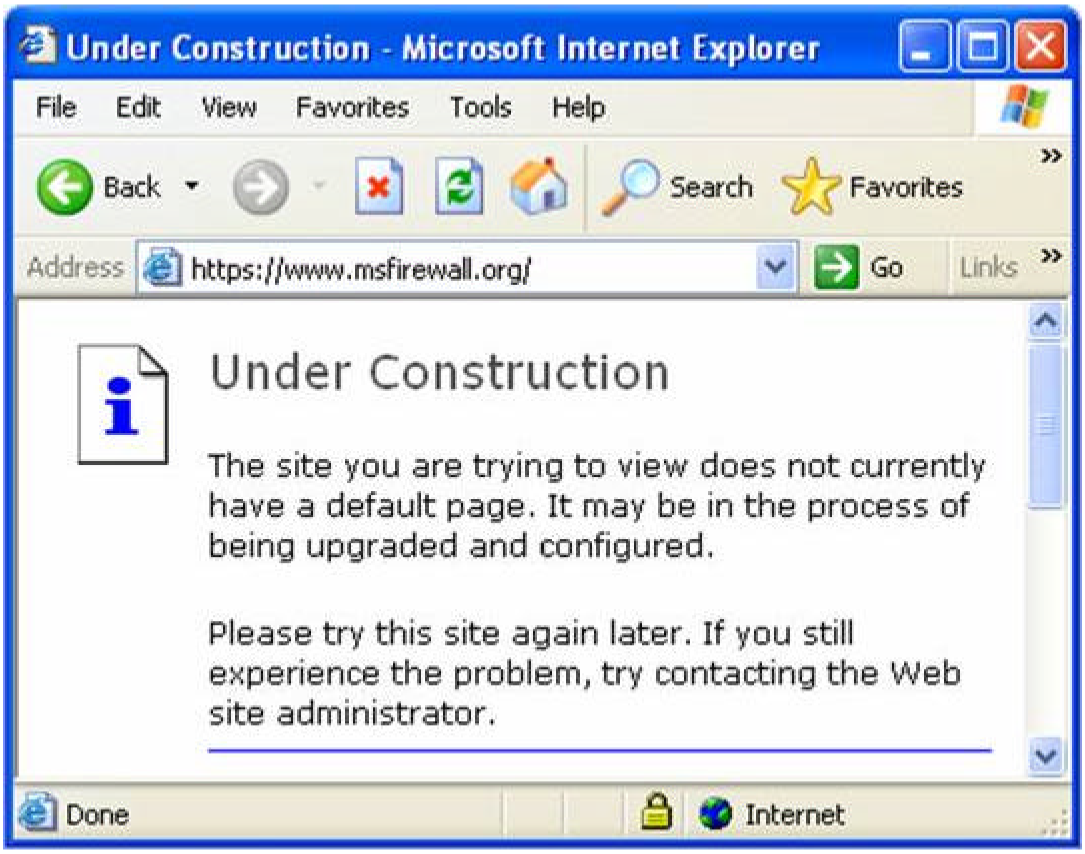
Valid from 6/21/2004 to 6/21/2005

You have a private key that corresponds to this certificate.

4. Click **OK** on the **Client Authentication** dialog box.

5. Enter valid user credentials in the authentication dialog box. These credentials must be valid on the Web server computer. Click **OK**.

6. You can see the default page on the Web site. I haven't added anything to this Web site, so we see the **Under Construction** page. Notice the lock icon in the status bar indicating the we have a secure connection to the Web site.


Under Construction - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://www.msfirewall.org/
Go
Links
Done
Internet

Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

In this example we connected to the secure Web site by first providing a user certificate. Only after the user certificate was submitted were we offered the opportunity to present user credentials. It's important to realize in this example that the user certificate is not mapped to a particular user account. The only requirement for the user certificate is that it comes from a Certificate Authority that the Web server trusts. Trust is based on the CA certificate entries in the Web server 's **Trusted Root Certification Authorities** *machine* certificate store.

You do have the option to map user certificates to user accounts. This provides an even stronger level of security, because not only must the user submit a user certificate from a trusted Certificate Authority, the user certificate must be mapped to a user account that has permission to access the Web site. If you're interested in user certificate mapping and how to make it work with your IIS Web server, send me a note at tshinder@isaserver.org.

Summary

In this article we went over the procedures required to secure a Web site using SSL encryption, user certificate authentication and user credentials. The only requirements are that you have a Windows IIS 5 or 6 Web server, a Microsoft Certificate Server and a browser client that supports user certificates. In future articles we may cover how you can map user certificates to user accounts so that you can further enhance the level of security provided by two-factor authentication using user certificates.

If you would like us to email you when Thomas Shinder releases another article on WindowSecurity.com, subscribe to our 'Real-Time Article Update' by clicking here. Please note that we do NOT sell or rent the email addresses belonging to our subscribers; we respect your privacy!