How to Install SSL Certificates on Microsoft Servers

Realtime
publishers

Dan Sullivan

Copyright Statement

Chapter 3: Using SSL Certificates in Microsoft Internet Information Server

The goal of this book is to provide readers a step-by-step guide to working with SSL certificates in a Windows environment. In the first chapter, we considered different types of SSL certificates and the reasons for choosing one type over another. In the second chapter, we delved into the Microsoft Certificate Store and reviewed how to use the Microsoft Management Console (MMC) to perform basic certificate operations and management tasks. In this chapter, we turn our attention to one of the most common business drivers for using SSL certificates: providing assurance about the authenticity of our business' Web sites.

Web sites make use of SSL certificates to authenticate themselves to clients and to support encrypted communication with clients. Windows systems administrators responsible for maintaining Web sites will likely have to install and maintain SSL certificates for one or more sites. This chapter provides a detailed explanation of how to install SSL certificates with Internet Information Server (IIS) Manager, including binding certificates to sites, configuring SSL settings, and verifying installation. The role of authenticating clients with SSL certificates is also discussed. We conclude this chapter with a discussion of setting up development and test environments with self-signed certificates.

The chapter is organized around three tasks commonly performed when working with IIS:

- Installing SSL certificates in IIS with the IIS Manager
- Authenticating clients with client certificate mapping
- Setting up SSL-enabled development and test environments

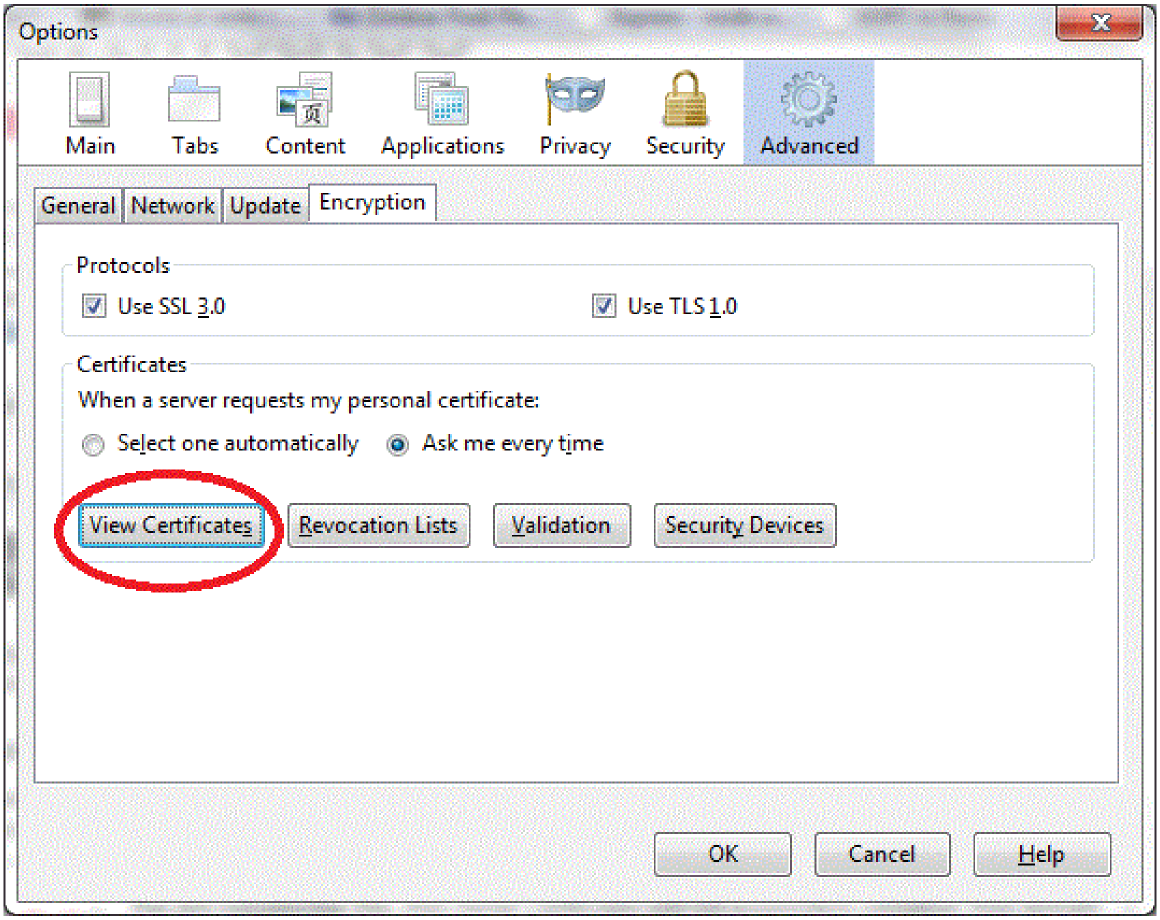
Most of the work involved in these steps occurs within the IIS Manager, but as we will see next, an important step begins with requesting a certificate from a trusted third-party provider.

Installing SSL Certificates in IIS with IIS Manager

Installing an SSL certificate is a multistep process that begins with acquiring a certificate, either from a trusted third party or by generating one yourself. We'll consider using a trusted third party here; later in the chapter, we will discuss how to generate a certificate yourself in the section on setting up development and test environments.

A number of trusted third-party providers can create SSL certificates for your Web servers. One quick way to find a list of providers that is trusted by most browsers is to check the lists in Microsoft Internet Explorer or Mozilla Firefox.

In Firefox, click Tools menu, then select Options. When the Options dialog box opens, click the Advanced icon at the top, then click the Encryption tab. Next, click View Certificates to display the Certificate Manager. From here, you can click the Authorities tab to see a list of certificate providers that are trusted by that browser.



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Figure 3.1: One source of SSL certificate providers is your browser. In Firefox, look under the Tools | Options | Advanced tab to View Certificates, including a list of certified authorities.

Another source of information is of course the Internet. Search in Google, Bing, or Yahoo for a list of third-party certificate providers.

> **Note**
>
> Be careful before choosing free or unusually discounted certificates. These may be from providers that are not typically included in the set of trusted authorities. Also, free providers may not offer as much assurance as other SSL certificate providers. Finally, when a client device needs to communicate with a certificate provider, such as for a certificate revocation list (CRL), the response time from free providers may not be comparable to other providers' response times.

The basic steps to installing an SSL certificate with IIS Manager are:

- Requesting a certificate
- Completing a certificate request
- Adding site binding
- Configuring SSL settings
- Verifying installation

We'll go over each of these steps in detail and discuss troubleshooting steps you might find helpful.

Requesting a Certificate

First, we should start the IIS Manager by clicking the Start menu, then selecting Administrative Tools.

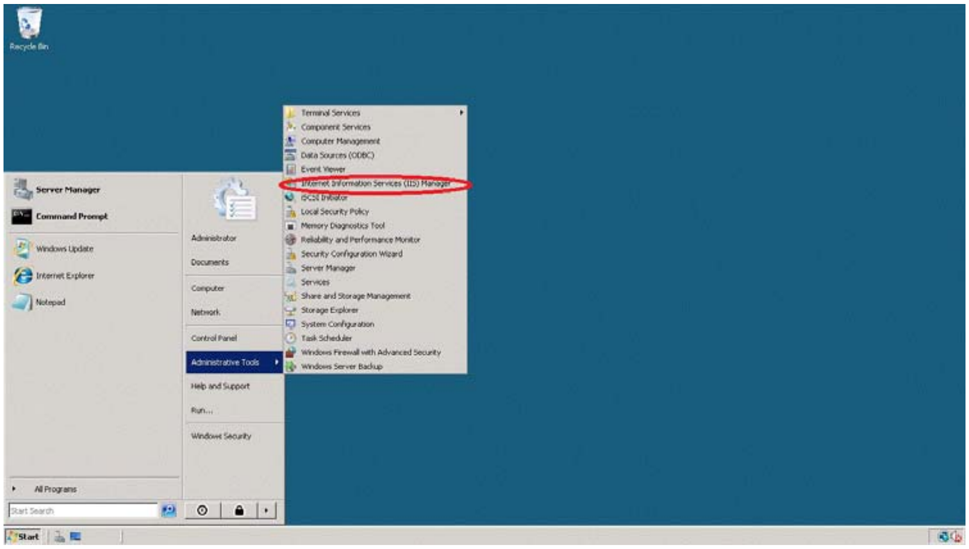
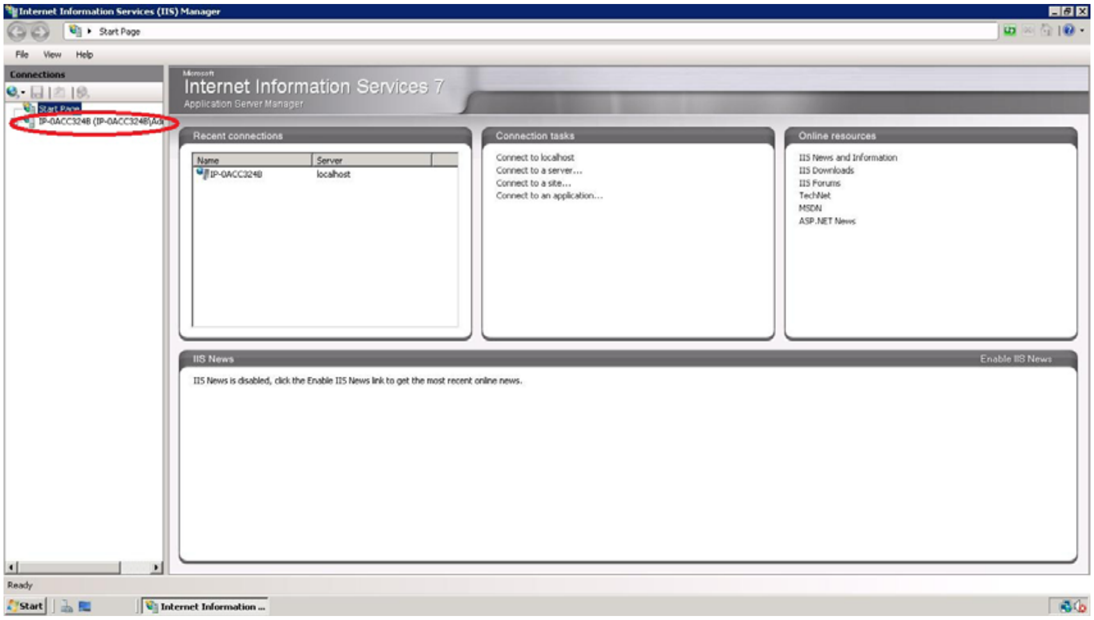


Figure 3.2: Start the IIS Manager from the desktop using Start | Administrative Tools | Internet Information Server (IIS) Manager.

This will start the IIS Manager as Figure 3.3 shows.



IIS News is disabled, click the Enable IIS News link to get the most recent online news.

Figure 3.3: The Connections pane on the left of IIS Manager interface lists Web servers where we can install certificates.

Clicking on the server name shows the list of management operations for a Web server (see Figure 3.4).

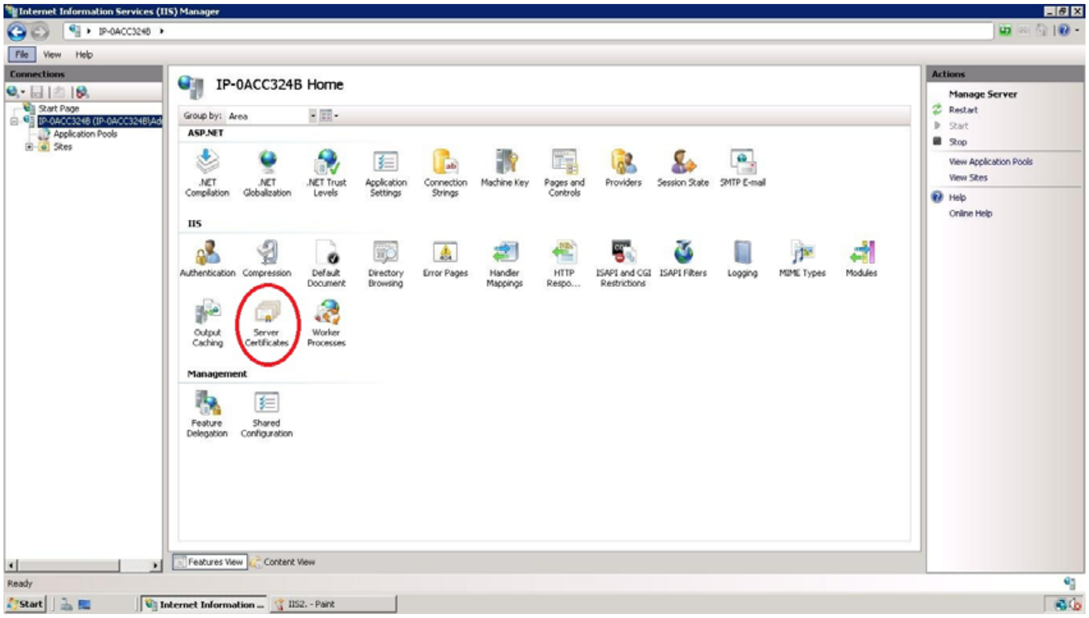
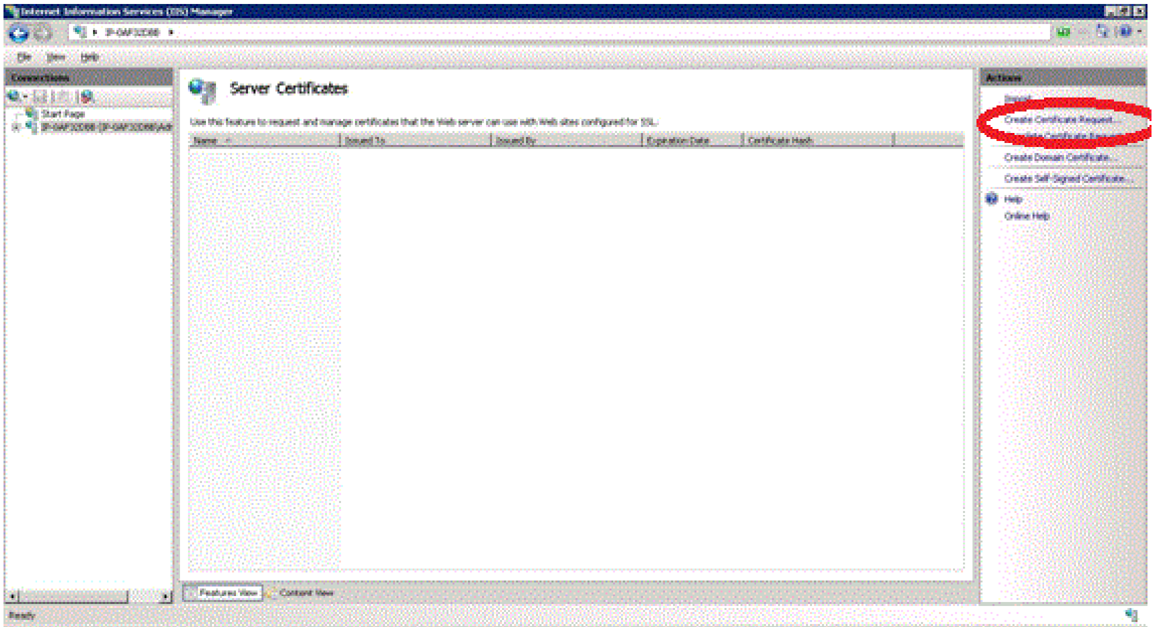


Figure 3.4: Within IIS Manager, we can select a specific server to manage. When we do, this list of server operations is available, including managing Server Certificates (within red circle).

Figure 3.5 shows the Server Certificates window in IIS Manager. This is where we can start the request certificate process.

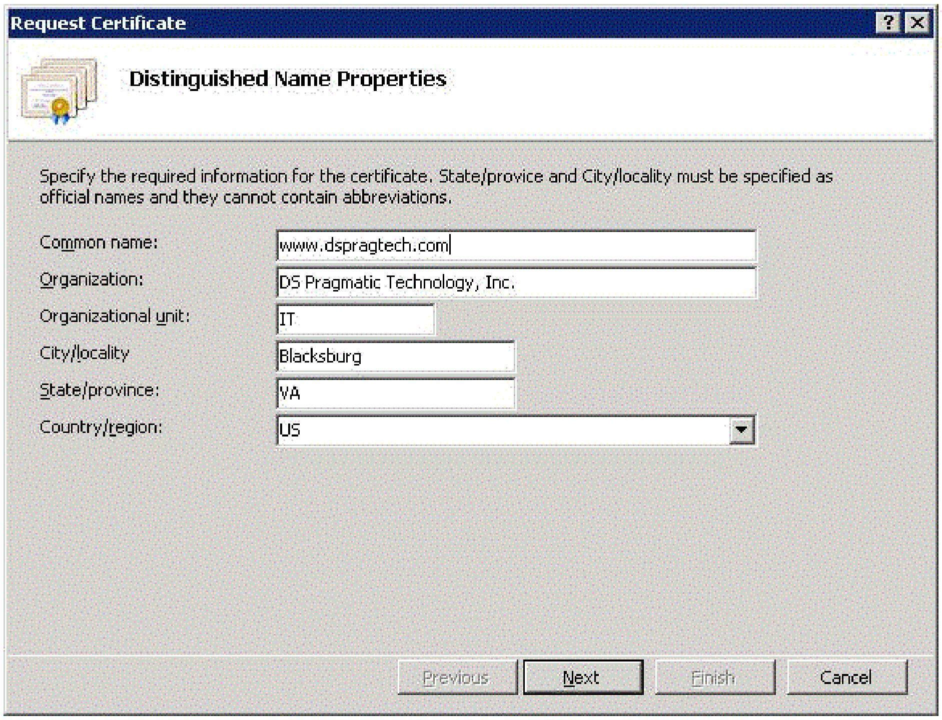

Internet Information Services (IIS) Manager
IP-0AF32D88
File
View
Help
Connections
Start Page
IP-0AF32D88 (IP-0AF32D88\Ad
Server Certificates
Name
Issued To
Issued By
Expiration Date
Certificate Hash
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Features View
Content View
Ready

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Figure 3.5: The Server Certificates window in IIS Manager. This is where we request and install SSL certificates.

In the right panel, click Create Certificate Request. This displays the Distinguished Properties form. Information about your company and the server are entered here. Properties include:

- Domain name of the server, such as a www.mycompanyname.com
- The full, descriptive name of the company
- An organizational unit (OU), such as IT or just about any description you care to use
- Location information



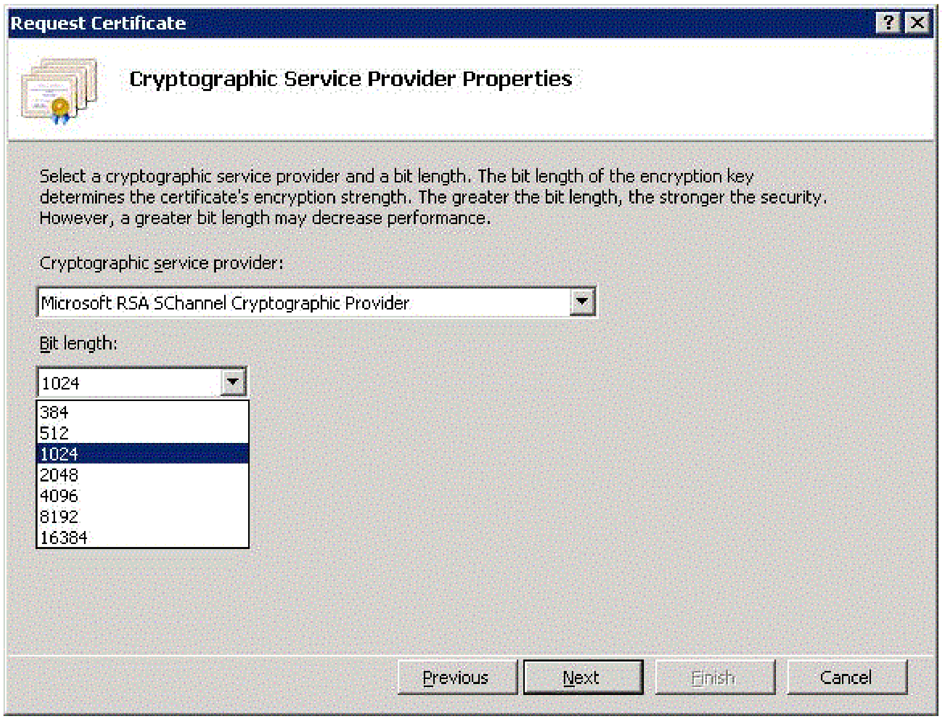
Distinguished Name Properties

Specify the required information for the certificate. State/provice and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: www.dspragtech.com
Organization: DS Pragmatic Technology, Inc.
Organizational unit: IT
City/locality Blacksburg
State/province: VA
Country/region: US

Figure 3.6: The first part of the Certificate Request process is to specify details about the server and company requesting the certificate.

Click Next. The cryptographic properties dialog box displays next.



Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

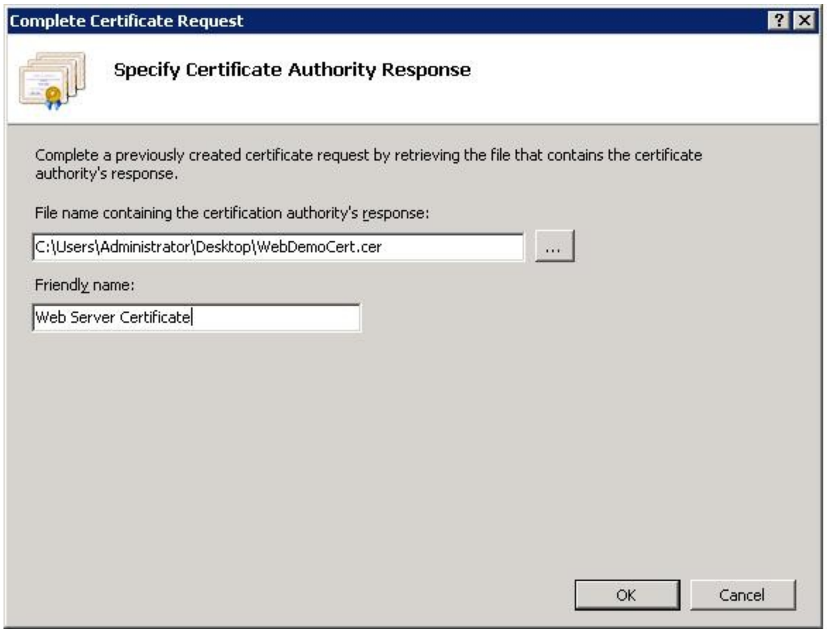
Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 1024

Figure 3.7: In this form, we enter basic cryptographic information, such as cryptographic service provider and key length.

Choose Microsoft RSA Channel Cryptographic Provider unless your certificate provider specifies something else. Key length should be at least 1024 and 2048 is even better, in terms of cryptographic strength.

Click Next. A dialog box appears to save the Certificate Signing Request (CSR) to a file. Enter a file name and a descriptive name for the certificate. If you are working with multiple servers, be sure to use an easy-to-remember naming convention.



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

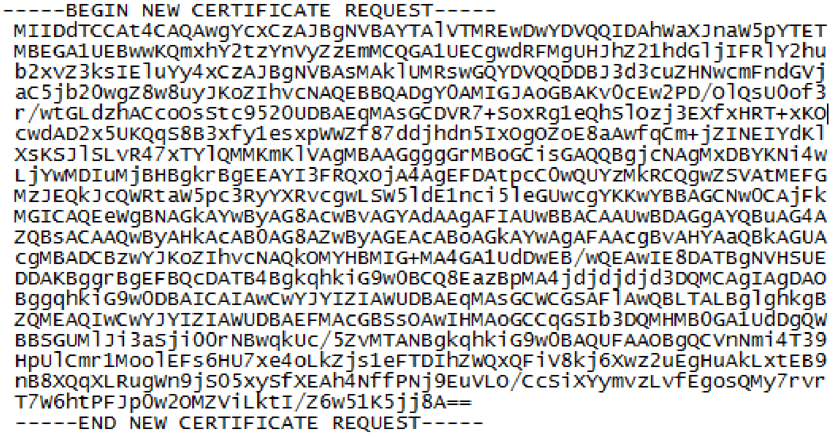
C:\Users\Administrator\Desktop\WebDemoCert.cer

Friendly name:

Web Server Certificate

Figure 3.8: The CSR is saved to a text file and sent to the SSL certificate provider.

The contents of the CSR file are encrypted and look similar to the contents of Figure 3.9.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
 MIIDdTCCAt4CAQAwgYcxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhWaXJnaW5pYTET
 MBEGA1UEBwwKQmxhY2tzYnVyZzEmMCQGA1UECgwdRFMgUHJhz21hdGljIFRlY2hu
 b2xvZ3ksIEluYy4xCzAJBgNVBAsMAklUMRswGQYDVQQDDBJ3d3cuZHNwcmFndGVj
 aC5jb20wgZ8w8uyJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKv0cEw2PD/olQsU0of3
 r/wtGLdzhACcoOsStc952OUDBAEgMAsGCDVR7+SoxRg1eQhslOzj3EXfxHRT+xKO
 cwdAD2x5UKQqS8B3xfy1esxpWWZf87ddjhdn5IxOgOZoE8aAwfqCm+jZINEIYdKl
 XsKSJlSLvR47xTYlQMMKmKlVAgMBAAGgggGrMBoGCisGAQQBgjcNAgMxDBYKNi4w
 LjYwMDIuMjBHBgkrBgEEAYI3FRQxOjA4AgEFDAtpcC0wQUYzMkRCQgwZSVAtMEFG
 MzJEQkJcQWRtaW5pc3RyYXRvcgwLSW5ldE1nci5leGUwcgYKKwYBBAGCNw0CAjFk
 MGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4A
 ZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUA
 cgMBADCBzwYJKoZIhvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUE
 DDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4jdjdjdjd3DQMCAgIAgDAO
 BggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMAsGCWCGSAFlAwQBLTALBglghkgB
 ZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQW
 BBSGUMlJi3asji0OrNBwqkUc/5ZvMTANBgkqhkiG9w0BAQUFAAOBgQCVnNmi4T39
 HpUlCmr1MoolEFs6HU7xe4oLkZjs1eFTDIhZWQxQFiV8kj6Xwz2uEgHuAkLxtEB9
 nB8XQqXLRugWn9jS05xySfXEAh4NffPNj9EuVLO/CcSiXYymvzLvfEgosQMy7rvr
 T7W6htPFJpOw2OMZViLktI/Z6w51K5jj8A==
 -----END NEW CERTIFICATE REQUEST-----
```

Figure 3.9: A CSR file is a text file with encrypted certificate request information. (Not actually a valid request; the text has been altered).

Once the CSR file is created, you will need to send it to your certificate provider. The steps will vary, but most vendors have a simple online form that allows you to either upload the CSR file or paste the text of the file into a Web form. Include the "-----BEGIN RSA PRIVATE KEY-----" and the "-----END RSA PRIVATE KEY-----" statements unless the provider specifies otherwise.

SSL certificate providers will send a certificate file to an email address in the domain. Some might require you have access to an administrator or root email at a domain, such as admin@mycompanyname.com. Just make sure you can receive emails in an email account approved by the SSL certificate provider.

Completing Certificate Request

Once you have received your certificate from your provider, you can proceed with the next step, which is also done within the IIS Manager. When you select Server Certificates in the IIS Manager, the right panel contains a list of Actions. This is where you earlier selected the option to Create Certificate Request. Now it is time to select the Complete Certificate Request option.

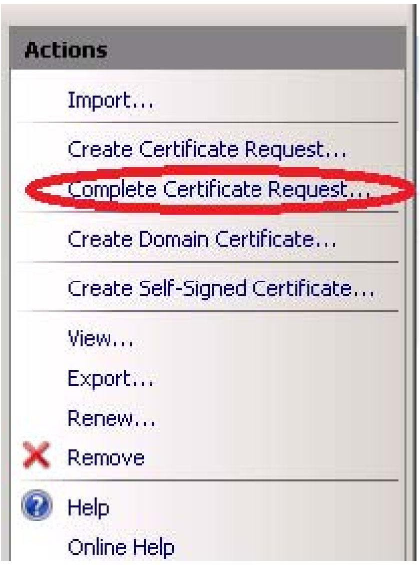
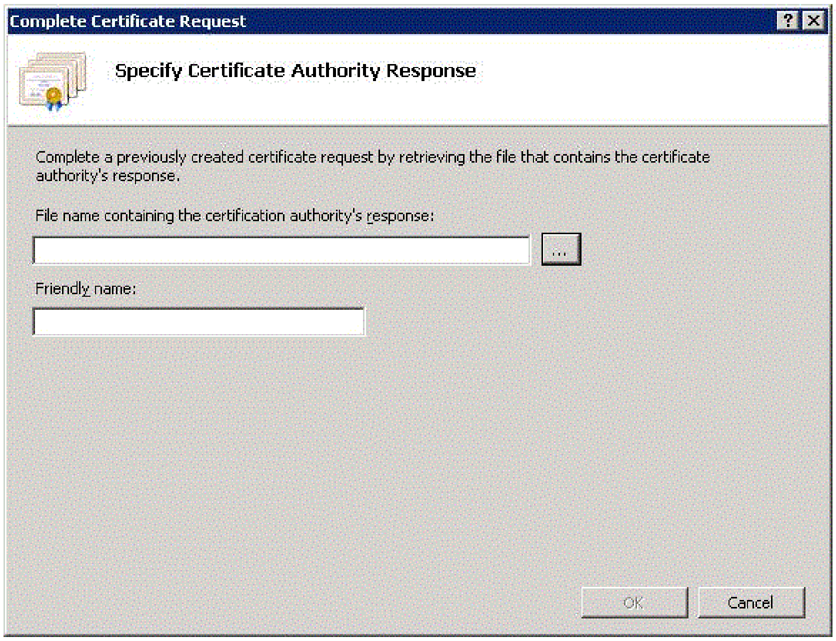

Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help

Figure 3.10: Once the SSL certificate file is received from the SSL provider, choose the Complete Certificate Request option in the Action menu.

This selection starts another series of dialog boxes that allows you to specify the certificate file. Figure 3.11 shows the first dialog box, which lets you select the file and associate a descriptive name with the certificate.


Complete Certificate Request
Specify Certificate Authority Response
...
OK
Cancel

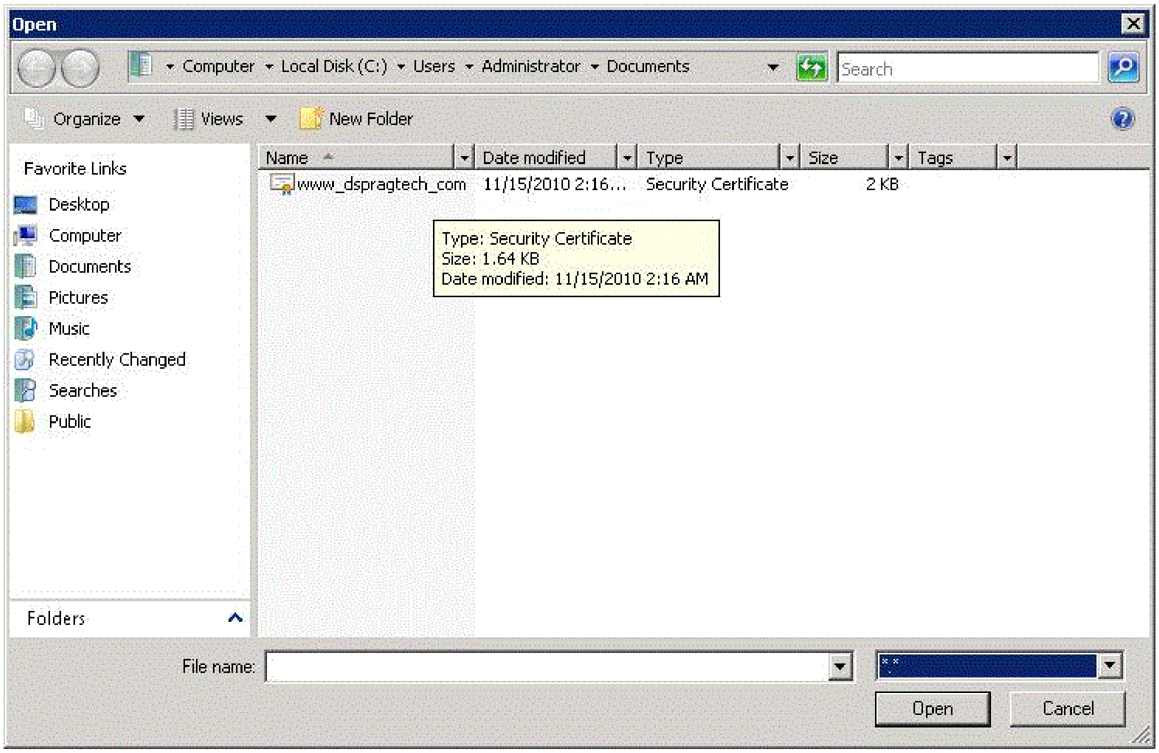
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

Friendly name:

Figure 3.11: Select the SSL certificate file sent to you by your certificate provider.

Navigate to the file, which should have an extension such as .cer or .crt.

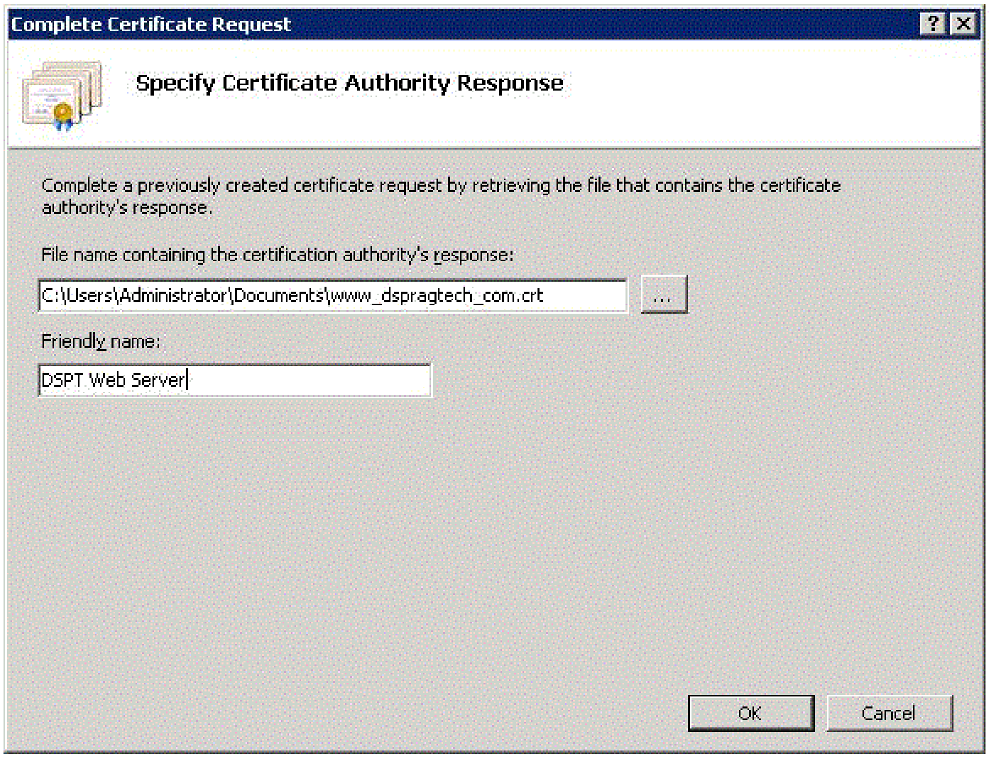


Name	Date modified	Type	Size	Tags
www_dspragtech_com	11/15/2010 2:16...	Security Certificate	2 KB	

Type: Security Certificate
Size: 1.64 KB
Date modified: 11/15/2010 2:16 AM

Figure 3.12: Navigate to the SSL certificate file sent to you by your provider.

After selecting the file, fill in the full descriptive name in the dialog box labeled Specify Certificate Authority Response.



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

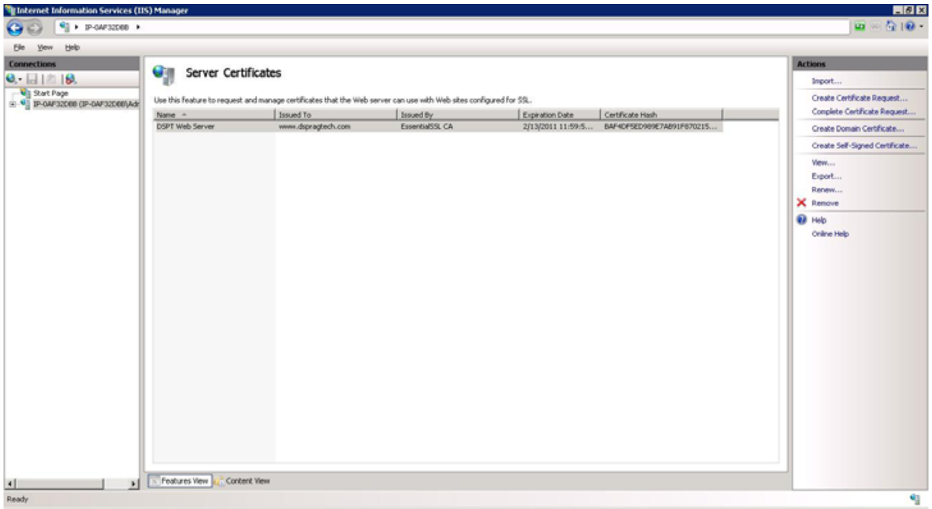
C:\Users\Administrator\Documents\www_dspragtech_com.crt

Friendly name:

DSPT Web Server

Figure 3.13: Specify the file and add a full descriptive name when adding a certificate.

The SSL certificate will then be displayed in the middle window pane of SSL certificates.



Internet Information Services (IIS) Manager

Server Certificates

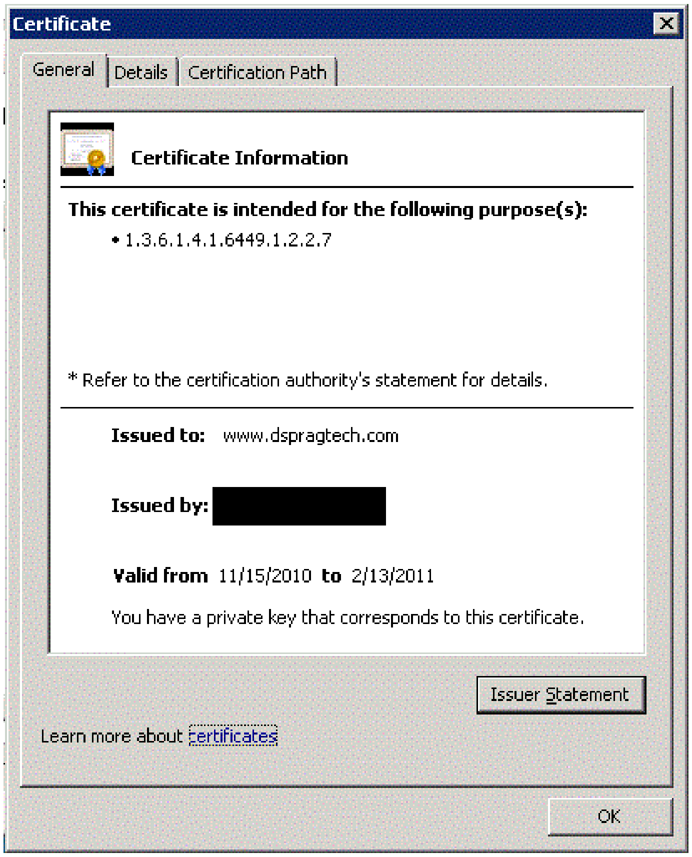
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
DSPT Web Server	www.dspragtech.com	EssentialSSL CA	2/13/2011 11:59:5...	BAF4DF5ED989E7AB91F870215...

IP-0AF32D8B
File
View
Help
Connections
Start Page
IP-0AF32D8B (IP-0AF32D8B\Adr
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help
Features View
Content View
Ready

Figure 3.14: The SSL certificate has been successfully added.

It s a good idea to verify that the certificate you wanted to just install is actually the one you did install. Double-click the certificate in the list to show its details.



Certificate Information

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

- 1.3.6.1.4.1.6449.1.2.2.7

* Refer to the certification authority's statement for details.

Issued to: www.dspragtech.com

Issued by: [redacted]

Valid from 11/15/2010 **to** 2/13/2011

You have a private key that corresponds to this certificate.

Learn more about certificates

Figure 3.15: Verify the information in the certificate by double-clicking the certificate entry in the SSL Certificates center pane.

The certificate request process is done. The next step is to add the SSL certificate to a site.

Adding Site Binding

In the Connections panel on the left side of the IIS Manager, navigate to the site you want to associate with your certificate. Click the site, then, in the right panel labeled Actions, click Bindings.

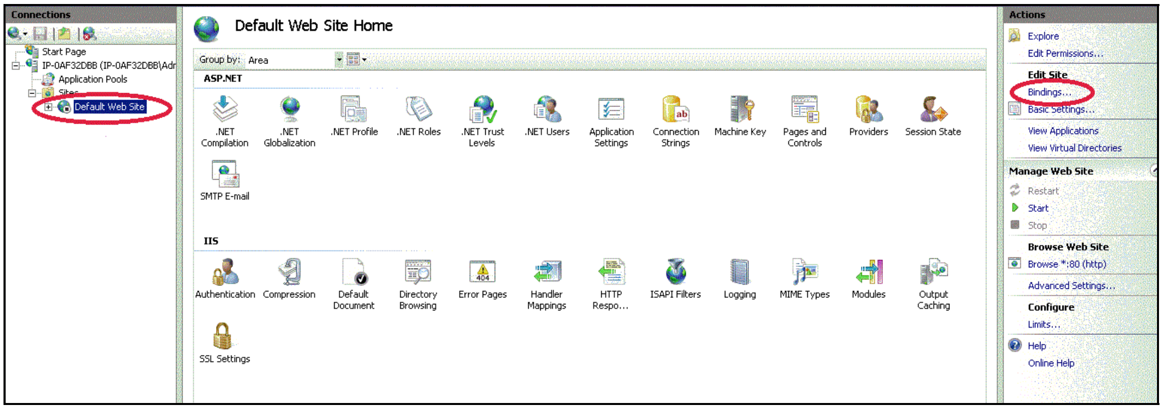
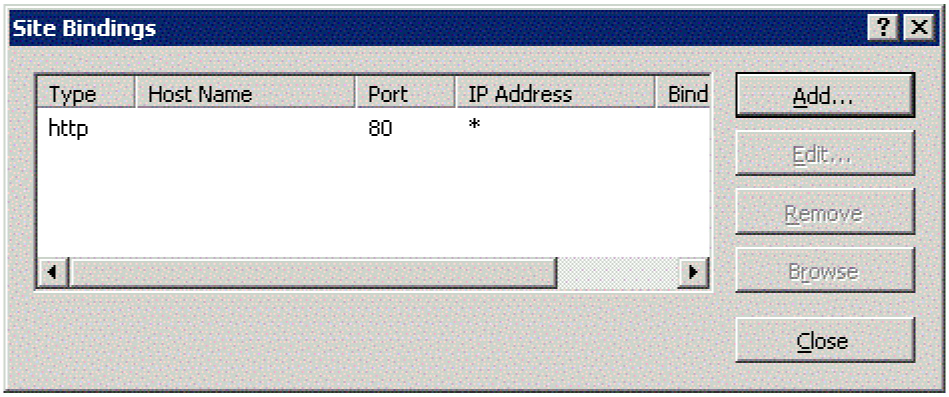


Figure 3.16: After selecting the Web site, click Bindings on the right to associate an SSL certificate with the Web site.

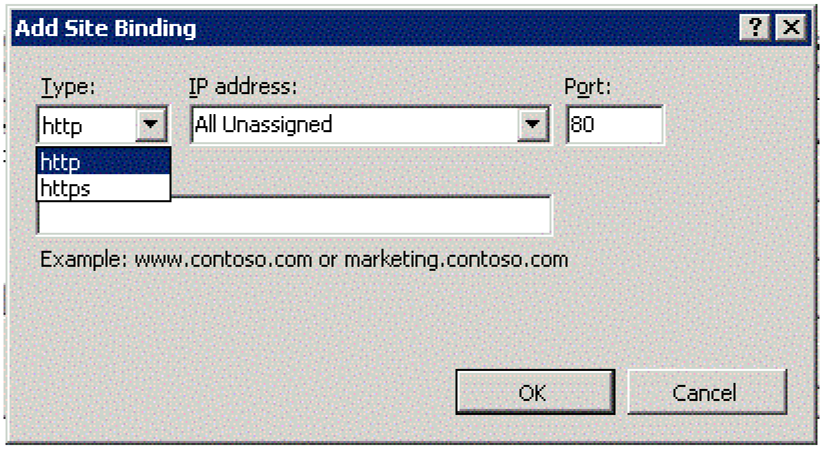
This displays the Site Bindings dialog box.



Type	Host Name	Port	IP Address	Bind
http		80	*	

Figure 3.17: Site Bindings allows you to add an SSL certificate to a site.

Click Add to display the Add Site Binding dialog box, then select https from the Type drop-down menu.



Type: http

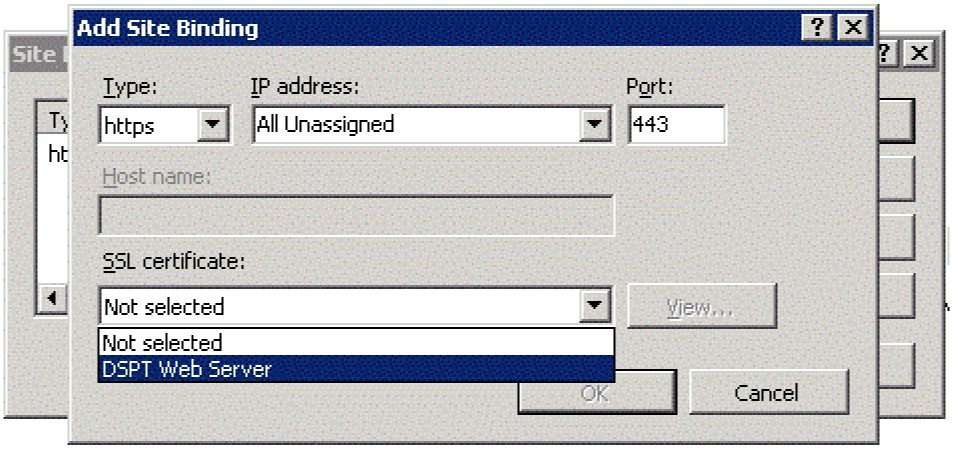
IP address: All Unassigned

Port: 80

Example: www.contoso.com or marketing.contoso.com

Figure 3.18: The Add Site Binding dialog box allows you to specify protocol type (https) and the certificate.

Select the certificate from the drop-down menu of SSL certificates.



Type: https

IP address: All Unassigned

Port: 443

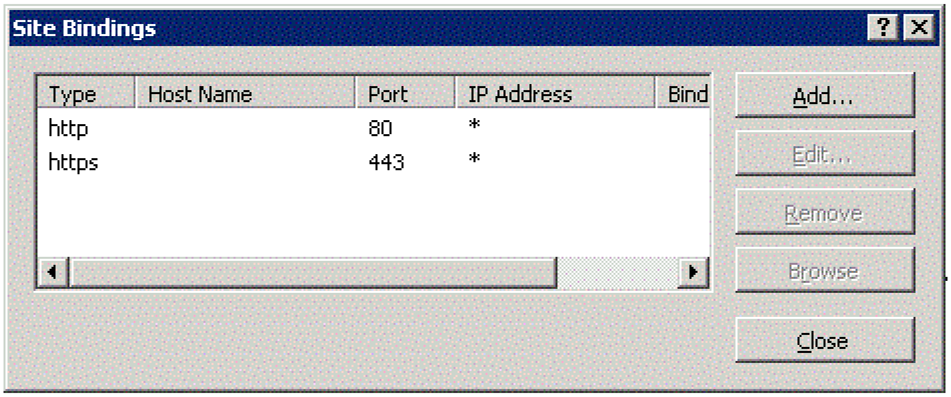
Host name:

SSL certificate: Not selected

Not selected
DSPT Web Server

Figure 3.19: After selecting Type https, select the name of the certificate to bind to this server.

The final dialog box should show a binding with type https and a port of 443, assuming you selected the default port. Your certificate is now bound to the site. You can close the Site Bindings dialog box.



Type	Host Name	Port	IP Address	Bind
http		80	*	
https		443	*	

Figure 3.20: A list of site bindings, including the https binding just added.

Configuring SSL Settings

Now that our SSL certificate binding is in place, we can configure SSL settings if we want to enforce non-default behavior. To start, from the IIS Manger interface with the Web site selected, click the SSL Settings icon.

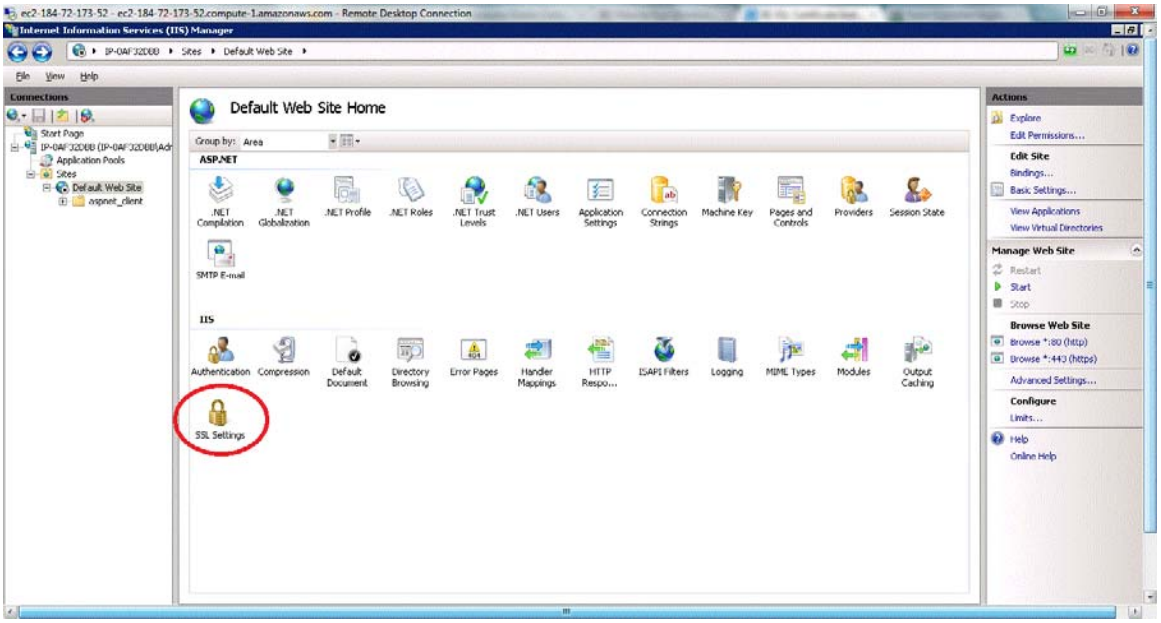
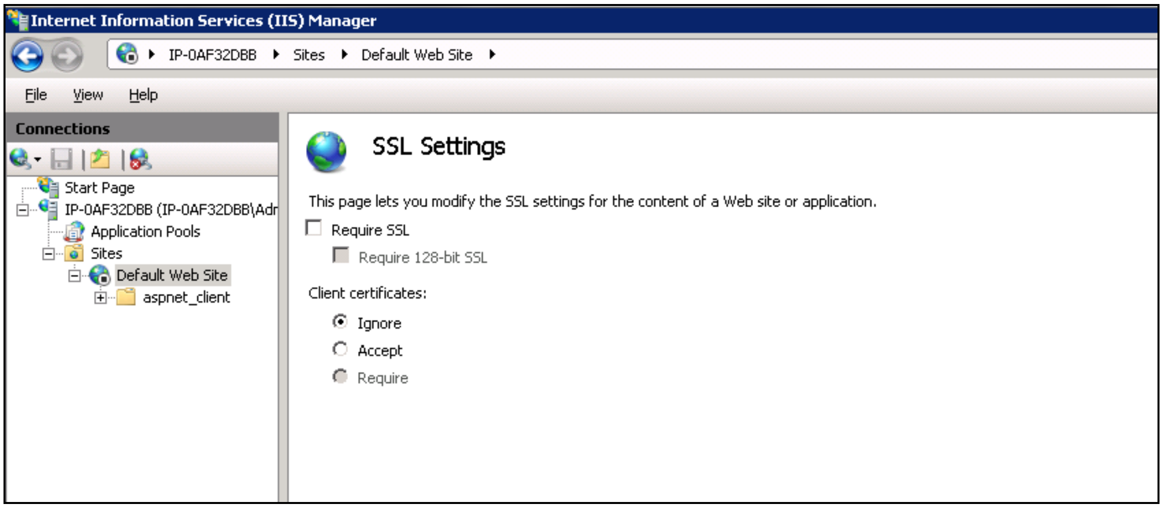


Figure 3.21: From the IIS Manager with the Web site selected, click SSL settings to change SSL configuration.

This displays the settings page from which you can specify whether SSL is required and how to respond to client certificates.

You might want to require SSL for secure communications, for example, if you are receiving or transmitting financial or personal information. If you select the Require SSL check box, then 40-bit encryption will be required. If you want the more-secure 128-bit encryption, also select the Require 128-bit SSL check box.


Internet Information Services (IIS) Manager
IP-0AF32DBB ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
IP-0AF32DBB (IP-0AF32DBB\Adr
Application Pools
Sites
Default Web Site
aspnet_client

SSL Settings

This page lets you modify the SSL settings for the content of a Web site or application.

☐ Require SSL

☐ Require 128-bit SSL

Client certificates:

● Ignore
○ Accept
○ Require

Figure 3.22: The SSL Settings configuration allows you to specify whether SSL is required, the minimal key length, and how to handle client certificates.

The default is to ignore client certificates. We will discuss reasons you might want to accept or require them in a later section.

Verifying Installation

To verify that the installation worked correctly and you users will see expected behavior at your Web site, we need to browse to the site. In the IIS Manger pane on the right, under Actions, click the Browse *:443(https) option.

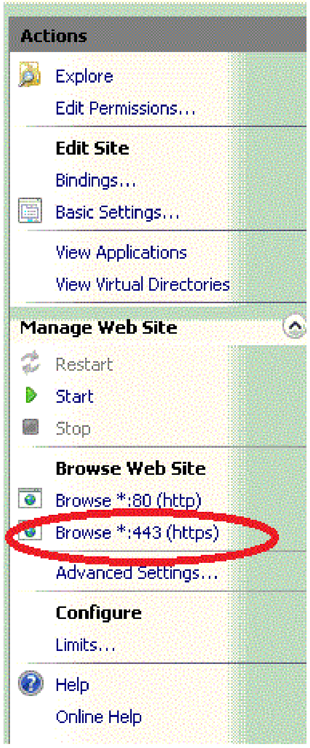


Figure 3.23: It is easy to verify the installation of an SSL certificate by browsing to the site using https.

When you browse to the site, if you receive a message that there is a problem with the Web site's security certificate, there was an error in the installation, which could be caused by:

- A difference in the information in the certificate and the server
- The Web site is not properly configured to receive https requests
- A step was missed in the SSL certificate process.

In the first case, generate a new certificate request to reflect accurate information about the server you are trying to secure. In the second case, see the Windows IIS Manager documentation to help diagnose the problem. In the third case, review the steps outlined in this chapter to ensure something was not missed. It is not unusual to hit a bump here and there when working with servers. For many of us, it's the norm.

Troubleshooting Tips

One of the challenges of developing and supporting Web applications is that users can have different configurations and use different browsers, which can combine to create headaches for systems administrators and developers. Fortunately, working with SSL certificates is pretty well standardized, and when errors do crop up, the root causes can often be fairly quickly identified.

One problem can occur if we decide to require SSL. This is a reasonable choice when we are exchanging private and confidential information through a Web server. For example, if your business uses a Web application to collect and store financial information about customers, you will want to protect that information. Requiring SSL is reasonable and may even be required by regulations. If for some reason a client device is not properly configured to support SSL communications with a server, this can cause problems. Your options, however, are limited. If you want to require SSL communications to improve security or are required to have encrypted communications, the client device will have to be reconfigured. However, if you're providing access to a public Web site and are more concerned with assuring users that your site is a site associated with your business, then requiring SSL encryption may not be necessary.

Most of our discussion up to this point has been about assuring clients that the server is legitimately associated with the business or organization they think it is. What about assuring the server that clients are who they appear to be?

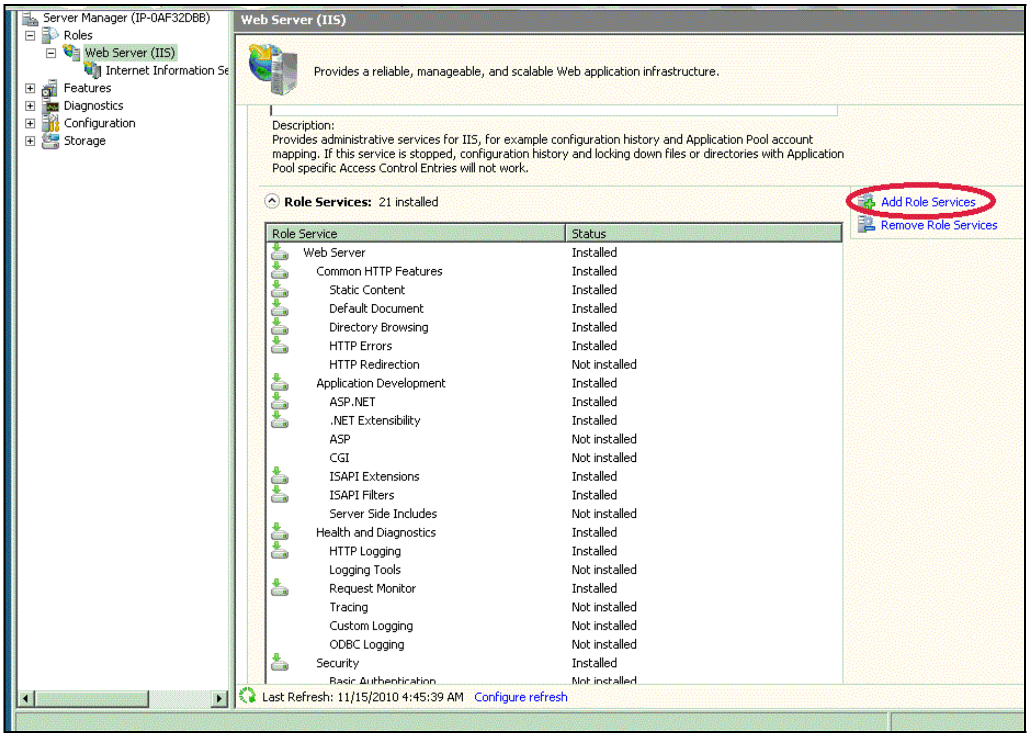
Authenticating Clients with Client Certificate Mapping

Do you need client authentication? The answer depends on your security requirements. If you are hosting a non-public Web site or you are providing an application or service that is limited to employees, business partners, and so on, then you might want to consider requiring client authentication.

> **Caveat Emptor: Some Programming Required**
>
> Setting up client certificate mapping requires some programming—that is, there is not (yet) a GUI client for all the steps. This section describes the GUI-enabled parts. Pointers are provided to documentation on programming details because delving into C## or VB code is beyond the scope of this chapter.

The basic idea behind client authentication is that you can map a user account to an SSL certificate. Let's say, for example, that Alice, an employee in the Finance department, needs remote access to the accounts payable system. Alice travels quite a bit, so she has installed an SSL certificate on her laptop so that she can get her work done while maintaining a road warrior lifestyle.

To configure client certificates with user accounts, use the Server Manager (available from the Start | Administrative Tools menu). From the Server Manger, select Roles then Web Server (IIS), then click Add Role Services on the left side of the window pane.



Server Manager (IP-0AF32DBB)
- Roles
  - Web Server (IIS)
    - Internet Information Se
- Features
- Diagnostics
- Configuration
- Storage

Web Server (IIS)

Provides a reliable, manageable, and scalable Web application infrastructure.

Description:
Provides administrative services for IIS, for example configuration history and Application Pool account mapping. If this service is stopped, configuration history and locking down files or directories with Application Pool specific Access Control Entries will not work.

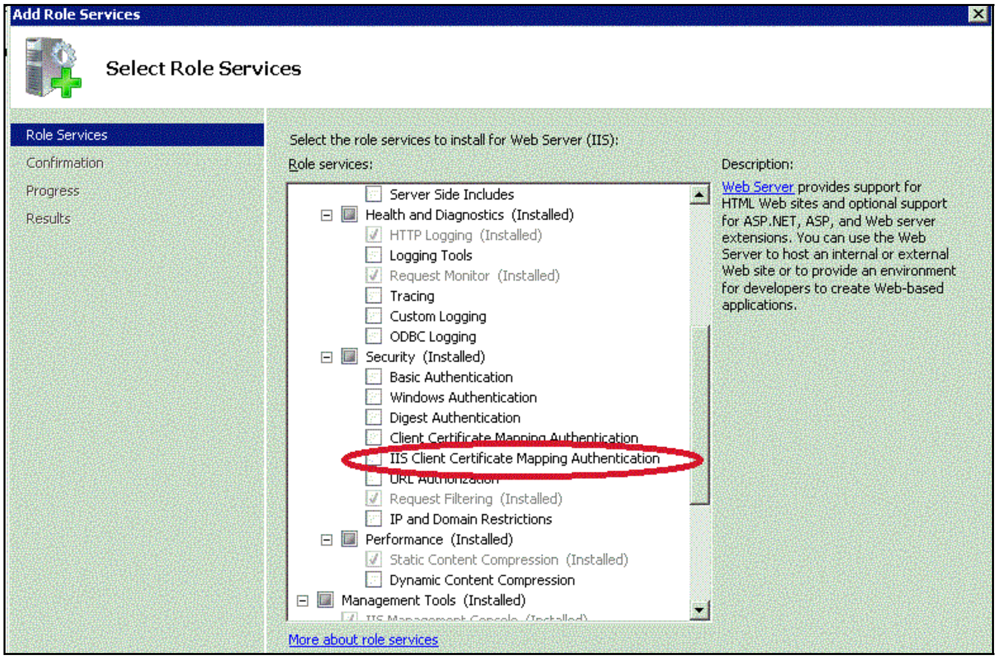
Role Services: 21 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Not installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Not installed
CGI	Not installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Not installed
Health and Diagnostics	Installed
HTTP Logging	Installed
Logging Tools	Not installed
Request Monitor	Installed
Tracing	Not installed
Custom Logging	Not installed
ODBC Logging	Not installed
Security	Installed
Basic Authentication	Not installed

Last Refresh: 11/15/2010 4:45:39 AM Configure refresh

Figure 3.24: Adding Role Services in Server Manager.

In the Select Role Services window, select the IIS Certificate Client Mapping Authentication check box.



Add Role Services

Select Role Services

Select the role services to install for Web Server (IIS):

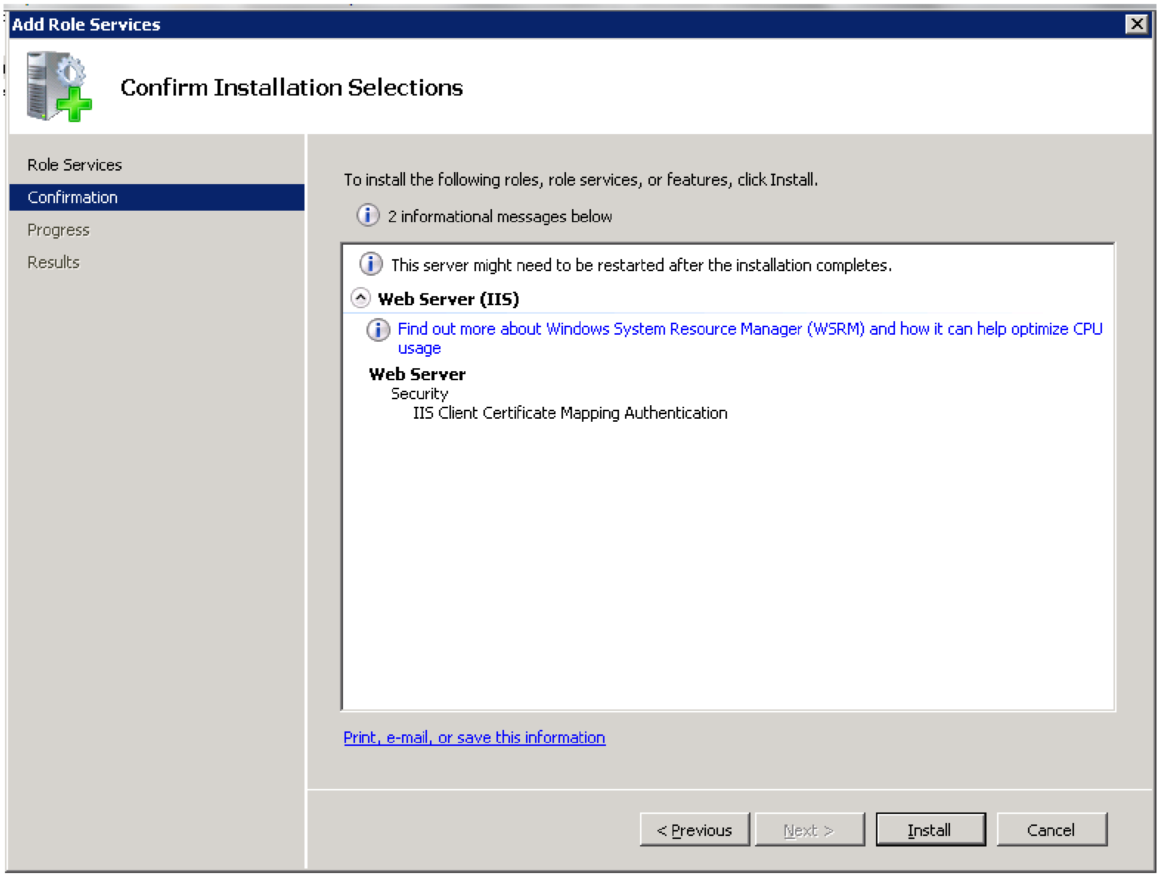
Role services:

- ☐ Server Side Includes
- ▣ Health and Diagnostics (Installed)
  - ☑ HTTP Logging (Installed)
  - ☐ Logging Tools
  - ☑ Request Monitor (Installed)
  - ☐ Tracing
  - ☐ Custom Logging
  - ☐ ODBC Logging
- ▣ Security (Installed)
  - ☐ Basic Authentication
  - ☐ Windows Authentication
  - ☐ Digest Authentication
  - ☐ Client Certificate Mapping Authentication
  - ☐ IIS Client Certificate Mapping Authentication
  - ☐ URL Authorization
  - ☑ Request Filtering (Installed)
  - ☐ IP and Domain Restrictions
- ▣ Performance (Installed)
  - ☑ Static Content Compression (Installed)
  - ☐ Dynamic Content Compression
- ▣ Management Tools (Installed)
  - ☑ IIS Management Console (Installed)

Description:
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

More about role services

Figure 3.25: Enabling IIS Client Certificate Mapping Authentication in Server Manager.



To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
Security
IIS Client Certificate Mapping Authentication

Figure 3.26: After confirming Client Authentication services, a dialog box appears; click Install to complete installation.

And now to repeat the bad news—there is no GUI interface for configuring client authentication.

> **Resource**
> For programming details, see the IIS.Net article at http://www.iis.net/ConfigReference/system.webServer/security/authentication/iisClientCertificateMappingAuthentication#006.

The final topic we need to address is setting up development and test environments with self-signed certificates.

Setting Up SSL Development and Test Environments

SSL certificates from a trusted third party are essential for public Web sites that need to assure users they are interacting with a legitimate site. The benefit of using third-party providers is that they vouch for our authenticity. The disadvantage of these third-party providers is that they too have businesses to run and need to charge for their services. When it comes to developers connecting to development and test servers on the company intranet, it is a pretty safe to assume that they will trust developmentserver.mycompany.com. Do we really have to pay to test things like SSL connectivity on development and test servers? No. There is a less expensive way: self-signed certificates.

The basic idea here is that we don't need a trusted third party to assure developers about the authenticity of a server. They already trust the company they work for, so that company might as well sign the certificates used on the servers they use.

In IIS Manager, select SSL Certificates then Create Self-Signed Certificate from the Actions menu on the right side of the interface.

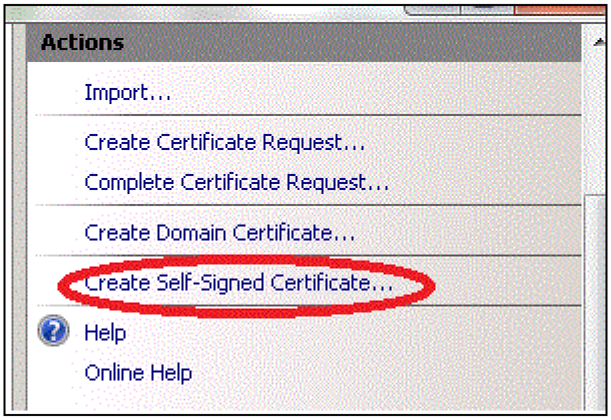
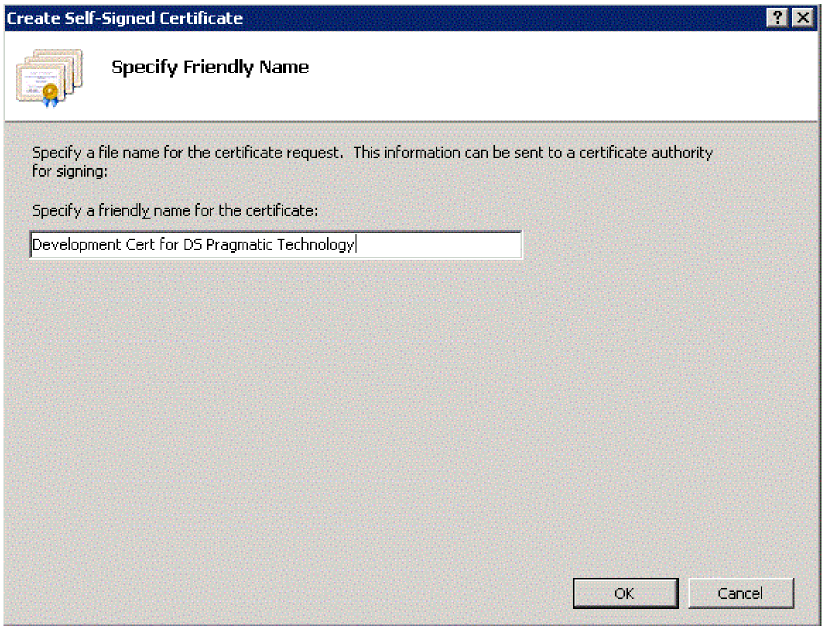

Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Figure 3.27: From the SSL Certificates interface of IIS Manger, we have the option to Create Self-Signed Certificates.

The next step is easy; just enter a descriptive name for the certificate.



Create Self-Signed Certificate

Specify Friendly Name

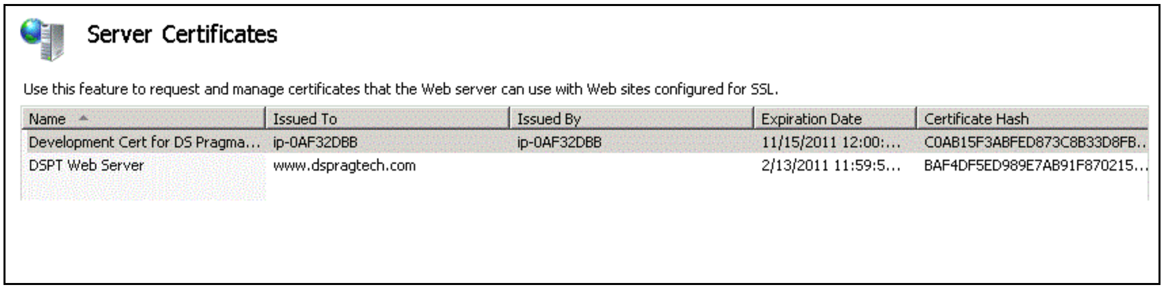
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Development Cert for DS Pragmatic Technology

Figure 3.28: When creating a self-signed SSL certificate, the first step is to specify a descriptive name.

You can then see the self-signed certificated listed alongside those from trusted third-party providers in the Server Certificates window.



Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
Development Cert for DS Pragma...	ip-0AF32DBB	ip-0AF32DBB	11/15/2011 12:00:...	C0AB15F3ABFED873C8B33D8FB..
DSPT Web Server	www.dspragtech.com		2/13/2011 11:59:5...	BAF4DF5ED989E7AB91F870215...

Figure 3.29: Self-signed certificates are listed along with those from trusted third-party providers.

Summary

Users expect to be able to work with authentic instances of business' Web servers. Microsoft IIS is a popular Web server. Logic dictates that we provide our users with the assurances they need about the authenticity of our Web sites running on IIS. Microsoft, along with trusted third-party SSL certificate providers, offers the means to provide assurances to our customers and business partners through the use of SSL certificates. The process of acquiring and installing SSL certificates is straightforward thanks to a (mostly) GUI-enabled process.

Download Additional Books from Realtime Nexus!