Knowledge Base

HOW TO: Enable SSL for All Customers Who Interact with Your Web Site in Internet Information Services

PSS ID Number: 298805

Article Last Modified on 4/24/2003

The information in this article applies to:

- Microsoft Internet Information Server 5.0
- Microsoft Internet Information Services version 6.0

This article was previously published under Q298805

IN THIS TASK

SUMMARY

This article describes the following:

- How to set up and enable server certificates so that your customers can be certain that your Web site is valid, and that any information that they send to you stays private and confidential.
- How to use third-party certificates to enable Secure Sockets Layer (SSL), as well as a general overview of the process that is used to generate a Certificate Signing Request (CSR), which is used to obtain a third-party certificate.
- How to enable SSL connectivity for your Web site.
- How to enforce SSL for all connections, and set the required encryption length between your clients and your Web site.

You can use your Web server's SSL security features for two types of authentication. You can use a *server certificate* to allow users to authenticate your Web site before they transmit personal information, such as a credit card number. Also, you can use *client certificates* to authenticate users that request information on your Web site.

This article assumes that you will use a third-party certificate authority (CA) to provide authentication for your Web server.

To enable SSL server certificate verification, and to provide the level of security that your customers desire, you should obtain a certificate from a third-party CA. Certificates that are issued to your organization by a third-party CA are typically tied to the Web server, and more specifically to the Web site to which you to bind SSL. You can create your own certificate with the Internet Information Services (IIS) server, but if you do so, your clients must implicitly trust you as the certificate authority.

This article assumes the following:

- You have installed IIS.
- You have created and published the Web site that you wish to secure with SSL.

back to the top

Obtain a Certificate

To begin the process to obtain the certificate, you must generate a CSR. You do this through the IIS management console; therefore, IIS must be installed before you can generate a CSR. A CSR is basically a certificate that you generate on your server that validates the computer-specific information about your server when you request a certificate from a third-party CA. The CSR is simply an encrypted text message that is encrypted with a public/private key pair.

Typically, the following information about your computer is included in the CSR that you generate:

- Organization
- Organizational unit
- Country
- State
- Locality
- Common name**NOTE**: The common name is usually comprised of your host computer name and the domain to which it belongs, such as xyz.com. In this case, the computer is part of the .com domain, and is named XYZ. This may be the root server for your corporate domain, or simply a Web site.

back to the top

Generate the CSR

1. Access the IIS Microsoft Management Console (MMC). To do this, right-click **My Computer** and click **Manage**. This opens the Computer Management Console. Expand the **Services and Application** section. Locate **Internet Information Services** and expand the IIS console.
2. Select the specific Web site on which you want to install a server certificate. Right-click the site and click **Properties**.
3. Click the **Directory Security** tab. In the **Secure Communications** section, click **Server Certificate**. This starts the Web Server Certificate Wizard. Click **Next**.
4. Select **Create a New Certificate** and click **Next**.
5. Select **Prepare the request now, but send it later** and click **Next**.
6. In the **Name** field, enter a name that you can remember. It will default to the name of the Web site for which you are generating the CSR.**NOTE**: When you generate the CSR, you need to specify a bit length. The bit length of the encryption key determines the

strength of the encrypted certificate which you send to the third-party CA. The higher the bit length, the stronger the encryption. Most third-party CAs prefer a minimum of 1024 bits.

7. In the **Organization Information** section, enter your organization and organizational unit information. This must be accurate, because you are presenting these credentials to a third-party CA and you must comply with their licensing of the certificate. Click **Next** to access the **Your Site's Common Name** section.
8. The **Your Site's Common Name** section is responsible for binding the certificate to your Web site. For SSL certificates, enter the host computer name with the domain name. For Intranet servers, you may use the NetBIOS name of the computer that is hosting the site. Click **Next** to access geographical information.
9. Enter your country, state or province, and country or region information. Completely spell out your state or province and country or region; do not use abbreviations. Click **Next**.
10. Save the file as a .txt file. When you actually send the request to the CA, you must paste the contents of this file into the request. This file will be encrypted and contain a header and footer for the contents. You must include both the header and footer when you request the certificate. A CSR should resemble the following:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDATCCAmoCAQAwbDEOMAwGA1UEAxMFcGxhbjgxDDAKBgNVBAsTA1BTUzESMBAG
A1UEChMJTWljcm9zb2Z0MRIwEAYDVQQHEwlDaGFybG90dGUxFzAVBgNVBAgTDk5v
cnRoIENhcm9saW5hMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAtW1koGfdt+EoJbKdxUZ+5vE7TF1ZuT+xaK9jEWHESfw11zoRKrHzHN0f
IASnwg3vZ0ACteQy5SiWmFaJeJ4k7YaKUb6chZXG3GqL4YiSKFaLpJX+YRiKMtmI
JzFzict5GVVGHsa1lY0BDYDO2XOAlstGlHCtENHOKpzdYdANRg0CAwEAAaCCAVMw
GgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUGCisGAQQBgjcCAQ4xJzAlMA4G
A1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYBBAGCNw0C
AjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAaABh
AG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBp
AGQAZQByA4GJAGKa0jzBn8fkxScrWsdnU2eUJOMUK5Ms87Q+fjP1/pWN3PJnH7x8
MBc5isFCjww6YnIjD8c3OfYfjkmWc048ZuGoH7ZoD6YNfv/SfAvQmr90eGmKOFFi
TD+hl1hM08gu2oxFU7mCvfTQ/2IbXP7KYFGEqaJ6wn0Z5yLOByPqblQZAAAAAAAA
AAAwDQYJKoZIhvcNAQEFBQADgYEAhpzNy+aMNHAmGUXQT6PKxWpaxDSjf4nBmo7o
MhfC7CIvR0McCQ+CBwuLzD+UJxl+kjgb+qwcOUkGX2PCZ7tOWzcXWNmn/4YHQl0M
GEXu0w67sVc2R9DlsHDNzeXLIOmjUl935qy1uoIR4V5C48YNsF4ejlgjeCFsbCoj
Jb9/2RM=
-----END NEW CERTIFICATE REQUEST-----
```

11. Confirm your request details. Click **Next** to finish, and exit the Web Server Certificate Wizard.

back to the top

Request the Certificate

There are different methods of submitting your request. Contact the certificate provider of your choice to request and receive your certificate and to determine the best certificate level for your needs.

back to the top

Install the Certificate

Once the third-party CA has completed your request for a server certificate, you will receive it by e-mail or download site. The certificate must be installed on the Web site on which you want to provide secure communications.

To install the certificate, follow these steps:

1. The key can only be decrypted with the private key that you generated earlier. Copy the text of the certificate key (it should appear to be very similar to the key you generated earlier) and paste it into a .txt document. Be sure to include the header and footers of the certificate. Save the file as Cert.txt.
2. Open the IIS MMC as described in the "Generating the CSR" section.
3. Access the **Properties** dialog box for the Web site on which you are installing the certificate.
4. Click the **Directory Security** tab and click **Server Certificate**. This starts the Web Server Certificate Wizard. Click **Next**.
5. Select **Process the Pending Request and install the certificate** and click **Next**.
6. Browse to the text file that you saved in step 1. Click **Next** twice, then click **Finish**.

back to the top

Enforce SSL Connections

Now that the server certificate is installed, you can enforce SSL secure channel communications with clients of the Web server. First, you need to enable port 443 for secure communications with the Web site. To do this, follow these steps:

1. From the Computer Management console, right-click the Web site on which you want to enforce SSL and click **Properties**.
2. Click the **Web Site** tab. In the **Web Site Identification** section, verify that the **SSL Port** field is populated with the numeric value **443**.
3. Click **Advanced**. You should see two fields. The IP address and port of the Web site should already be listed in the **Multiple identities for this web site** field. Under the **Multiple SSL Identities for this web site** field, click **Add** if port 443 is not already listed. Select the server's IP address, and type the numeric value **443** in the **SSL Port** field. Click **OK**.

Now that port 443 is enabled, you can enforce SSL connections. To do this, follow these steps:

1. Click the **Directory Security** tab. In the **Secure Communications** section, note that **Edit** is now available. Click **Edit**.
2. Select **Require Secure Channel (SSL)**.**NOTE**: If you specify 128-bit encryption, clients who use 40-bit or 56-bit strength browser will not be able to communicate with your site unless they upgrade their encryption strength.
3. Open your browser and try to connect to your Web server by using the standard http:// protocol. If SSL is being enforced, you receive the following error message:
   The page must be viewed over a secure channel
   The page you are trying to view requires the use of "https" in the address.

   Please try the following: Try again by typing https:// at the beginning of the address you are attempting to reach. HTTP 403.4 - Forbidden: SSL required Internet Information Services
   Technical Information (for support personnel) Background: This error indicates that the page you are trying to access is secured

with Secure Sockets Layer (SSL).
You can now connect to your Web site only by using the https:// protocol.

back to the top

Additional query words: iis 5 iis5 iis 6 iis 6.0 iis6

Keywords: kbHOWTOmaster KB298805
Technology: kbiis500 kbiis600 kbiisSearch
