Knowledge Base

HOW TO: Implement SSL on a Windows 2000 IIS 5.0 Computer

PSS ID Number: 299875

Article Last Modified on 5/20/2003

The information in this article applies to:

- Microsoft Internet Information Services 5.0, when used with:
  - the operating system: Microsoft Windows 2000

This article was previously published under Q299875

IN THIS TASK

- SUMMARY
- Requirements
  - Create a Certificate RequestSubmit a Certificate RequestIssue and Download a CertificateInstall the Certificate and Set Up an SSL Web SiteConfigure and Test the Certificate
- Troubleshooting
- REFERENCES

SUMMARY

The Internet has opened up new ways for organizations to communicate, both internally and externally. Better communication between employees, vendors, and customers enables an organization to cut costs, bring products to market faster, and build stronger customer relationships. This improved communication requires--at times--transmitting sensitive information over the Internet and intranets. It thus becomes imperative to be able to conduct private, tamper-proof communication with known parties. To bring this about, organizations can build a secure infrastructure based on public-key cryptography by using digital certificates with technologies such as Secure Sockets Layer (SSL). This step-by-step guide discusses how to set up SSL on an Information Services (IIS) version 5.0 computer.

back to the top

Requirements

The following items describe the recommended hardware, software, network infrastructure, skills and knowledge, and service packs that you will need:

- Windows 2000 Server, Advanced Server, or Professional, with Internet Information Services (IIS) version 5.0 and Microsoft Certificate Server version 2.0 installed and configured.

If the computer that is hosting Certificate Server is not the same computer that has IIS, you need a valid network or Internet connection to the server that is hosting Certificate Server.

back to the top

Create a Certificate Request

First, the Web server must make a certificate request. To do this, follow these steps:

1. Start the Internet Service Manager (ISM), which loads the Internet Information Server snap-in for the Microsoft Management Console (MMC). To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Service Manager**.
2. Double-click the server name so that you see all of the Web sites.
3. Right-click the Web site on which you want to install the certificate, and then click **Properties**.
4. Click the **Directory Security** tab, and then click **Server Certificate** under **Secure Communications** to start the Web Server Certificate Wizard.
5. Select **Create a new certificate** and click **Next**.
6. Select **Prepare the request now, but send it later** and click **Next**.
7. Click **Next**, and give your certificate a name. You may want to match it with the name of the Web site. Now, select a bit length; the higher the bit length, the stronger the certificate encryption. Select **Server Gated Cryptography** if your users may be coming from countries with encryption restrictions.
8. Type your organization name and the organizational unit (for example, MyWeb and Development Dept). Click **Next**.
9. Type either the fully qualified domain name (FQDN) or the server name as the common name. If you are creating a certificate that will be used over the Internet, it is preferable to use a FQDN (for example, www.MyWeb.com). Click **Next**.
10. Enter your location information, and then click **Next**.
11. Type the path and file name to save the certificate information to, and click **Next** to continue.

    NOTE: If you type anything other than the default location and file name, be sure to note the name and location you choose, because you will have to access this file in later steps.
12. Verify the information that you have typed, and then click **Next** to complete the process and create the certificate request.

back to the top

Submit a Certificate Request

The certificate request that you just created needs to be submitted to a Certificate Authority (CA). This may be your own server with Certificate Server 2.0 installed on it or an online CA such as VeriSign. Contact the certificate provider of your choice and determine the best level of certificate for your needs. There are different methods of submitting your request. Contact the Certificate Authority of your choice to request and receive your certificate. You can create your own certificate with Certificate Server 2.0, but your clients must implicitly trust you as the Certificate Authority. The steps below assume that you are using Certificate Server 2.0 as the certificate provider.

1. Open a browser and browse to http://*YourWebServerName*/CertSrv/.
2. Select **Request a Certificate** and click **Next**.
3. Select **Advanced Request** and click **Next**.
4. Select **Submit a Certificate Request using a Base64** and click **Next**.
5. In Microsoft Notepad, open the request document that you created in the "Create a Certificate Request" section.
6. Copy the contents of the document. The contents should resemble the following:

   ```
   -----BEGIN NEW CERTIFICATE REQUEST-----
   MIICcjCCAhwCAQAwYjETMBEGA1UEAxMKcm9ic3NlcnZlcjELMAkGA1UECxMCTVMx
   CzAJBgNVBAoTAk1TMREwDwYDVQQHEwhCZWxsZXZ1ZTERMA8GA1UECBMIV2FzaGl0
   b24xCzAJBgNVBAYTAlVTMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALYK4sYDNQ7h
   LmSfL0qpIvUfY7Ddw7fNCvDp3rM7z4QqoLhA2c8TkyamqWTBsV0WRHIidf/J6mU4
   wN4wrUzJTLUCAwEAAaCCAVMwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUG
   CisGAQQBgjcCAQ4xJzAlMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEF
   BQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0
   ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBw
   AGgAaQBjACAAUAByAG8AdgBpAGQAZQByA4GJAGKa0jzBn8fkxScrWsdnU2eUJOMU
   K5Ms87Q+fjP1/pWN3PJnH7x8MBc5isFCjww6YnIjD8c3OfYfjkmWc048ZuGoH7Zo
   D6YNfv/SfAvQmr90eGmKOFFiTD+hl1hM08gu2oxFU7mCvfTQ/2IbXP7KYFGEqaJ6
   wn0Z5yLOByPqblQZAAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADQQCgRCWkaXlY2nVa
   tbn6p5miPwWfrbViYo0B62wkuH0f7J0nSGcxMnn/6Q/iLEIsgHqFhox5PWCzIV0J
   tXKPWrBL
   -----END NEW CERTIFICATE REQUEST-------
   ```

   NOTE: If you save the document with the default name and location, it is located at C:\Certreq.txt.

   NOTE: Be sure to copy all of the content just as shown.
7. Paste the contents of the document into the Web form's **Base64 Encoded Certificate Request** text box.
8. Under **Certificate Template**, select **Web Server**, and then click **Submit**.
9. If **Certificate Server** is set to **Always Issue the Certificate**, you can access the certificate immediately. To do this, follow these steps:
   a. Click **Download CA Certificate** (do not click **Download CA Certificate path**).
   b. When you are prompted, select **Save this file to disk** and save the certificate to your desktop or another location that you will remember. You may now go directly to the "Install the Certificate and Set Up an SSL Web Site" section.

back to the top

Issue and Download a Certificate

To issue a certificate in Certificate Server, follow these steps:

1. Open the CA MMC snap-in. To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certificate Authority**.
2. Expand **Certificate Authority** and click the **Pending Requests** folder. Your pending certificate requests appear in the right pane.
3. Right-click the pending certificate request that you just submitted, select **All Tasks**, and then click **Issue**.

   NOTE: After you select **Issue**, the certificate is no longer displayed in this window and folder. It now resides in the Issued Certificate folder.
4. After you have issued (and authorized) the certificate, you can return to the Certificate Servers Web interface to select and download the certificate. To do this, follow these steps:
   a. Browse to http://*YourWebServerName*/CertSrv/.
   b. On the default page, select **Check on a pending certificate** and click **Next**.
   c. Select your pending certificate, then click **Next** to go to the download page.
   d. On the download page, click **Download CA Certificate** (do not click **Download CA Certificate path**).
   e. When you are prompted, select **Save this file to disk** and save the certificate to your desktop or another location that you will remember.

back to the top

Install the Certificate and Set Up an SSL Web Site

To install the certificate, follow these steps:

1. Open the Internet Services Manager and expand the server name so that you can view the Web sites.
2. Right-click the Web site for which you created the certificate request and click **Properties**.
3. Click the **Directory Security** tab. Under **Secure Communications**, click **Server Certificate**. This starts the Certificate Installation Wizard. Click **Next** to continue.
4. Select **Process the pending request and install the certificate** and click **Next**.
5. Type the location of the certificate that you downloaded in the "Issue and Download a Certificate" section, then click **Next**. The Wizard displays the Certificate Summary. Verify that the information is correct, then click **Next** to continue.
6. Click **Finish** to complete the process.

back to the top

Configure and Test the Certificate

To configure and test the certificate, follow these steps:

1. On the **Directory Security** tab, under **Secure Communications**, note that there are now three available options. To set the Web site to require secure connections, click **Edit**. The **Secure Communications** dialog box appears.
2. Select **Require Secure Channel (SSL)** and click **OK**.
3. Click **Apply** and then **OK** to close the property sheet.

4. Browse to the site and verify that it works. To do this, follow these steps:
   a. Access the site through HTTP by typing `http://localhost/Postinfo.html` in the browser. You receive an error message that resembles the following:
   HTTP 403.4 - Forbidden: SSL required.
   b. Try to browse to the same Web page using a secured connection (HTTPS) by typing `https://localhost/postinfo.html` in the browser. You may receive a security alert that states that the certificate is not from a trusted root CA. Click **Yes** to continue to the Web page. If the page appears, you have successfully installed your certificate.

back to the top

Troubleshooting

- The use of SSL slows performance between HTTP servers and browsers.For additional information, click the article number below to view the article in the Microsoft Knowledge Base:

  150031 Use of SSL Creates Performance Overhead for Browsers

- When you use Microsoft Visual InterDev version 6.0 to author Web sites with SSL, there are several issues and limitations to consider. For more information, see the following Knowledge Base article:

  238662 INFO: Using Visual InterDev and Secure Sockets Layer

- This article discusses server certificates only. A server certificate enables users to authenticate your server, check the validity of Web content, and establish a secure connection. If you also intend to authenticate users who browse to your Web site, you may consider using client certificates. A typical client certificate contains several items of information: the identity of the user, the identity of the certification authority, a public key that is used for establishing secure communications, and validation information, such as an expiration date and serial number.

back to the top

REFERENCES

For more information, see the following Knowledge Base articles:

228991 HOW TO: Create and Install an SSL Certificate in Internet Information Server 4.0

257591 Description of the Secure Sockets Layer (SSL) Handshake

299525 HOWTO: Set Up SSL by Using Internet Information Services 5.0 and Certificate Server 2.0

298805 HOW TO: Enable SSL for All Customers Who Interact with Your Web Site in Internet Information Services

For more information, see the following Microsoft Web site:

Obtaining a Client Certificate
http://www.microsoft.com/windows2000/en/advanced/iis/default.asp?url=/WINDOWS2000/en/advanced/iis/htm/core/iiclisc.htm

Keywords: kbhowto KB299875
Technology: kbiis500 kbiisSearch kbOSWin2000 kbOSWinSearch

Send feedback to Microsoft