$Digital Certificates for ISA Server 2004

Microsoft Internet Security and Acceleration (ISA) Server 2004

Introduction

Digital certificates are the industry standard means of authentication and of providing encryption of sensitive data. A typical example of digital certificate use is in communication between a computer on the Internet and a Web server, in which credit card or bank account and password information may be transmitted. To prevent the reading of this information as it passes through the routers that connect the Internet, the HTTPS protocol, requiring digital certificates, is used.

Microsoft® Internet Security and Acceleration (ISA) Server 2004 enables the use of digital certificates for Web publishing rules, server publishing rules, and site-to-site virtual private network (VPN) connections. This document describes scenarios in which digital certificates, also called Secure Sockets Layer (SSL) certificates, are required on an ISA Server computer or on published servers behind the ISA Server computer. Procedures for obtaining and installing digital certificates are provided.

Certification Authorities

Digital certificates are issued by a certification authority (CA). A CA can be a commercial firm that provides certificates for a fee, or it can be a computer running Windows Server™ 2003 or Windows® 2000 Server in your organization on which you have installed Certificate Services.

Digital certificates require trust. Certificate trust is based on the presence of a root certificate from the CA that issued the certificate.

Consider the scenario where a computer on the Internet will connect to an ISA Server 2004 computer called Server1. When the client requests a secure connection over HTTPS, Server1 presents its certificate. For the client to trust the certificate, it must have locally installed the root certificate from Server1.

When you install a certificate from a commercial CA, there is no need for root certificate distribution because the root certificates are installed with Windows. When you install Certificate Services on one of your organization's servers running Windows and issue your own certificates, you must make arrangements to transfer the root certificate for your CA to any computer that you will allow connections secured with digital certificates. If there no direct connectivity to the Certificate Services computer, information exchange can be done by using a disk or CD, or by

$ Digital Certificates for ISA Server 2004 e-mail. (Be sure that your e-mail system is secure before doing so.) A CA can also be published using Internet Information Services (IIS) and Active Server Pages.

Notes

In Microsoft Windows Server™ 2003, computers within the same domain as the CA will automatically trust certificates from the CA, as they are published to the Active Directory® directory service.

You can also deploy a root CA certificate through group policy in Active Directory.

Because there is a cost associated with commercial digital certificates, in a scenario where the secure connections are expected to come from internal corporate clients, we recommend that you set up a local CA and issue your own certificates. The procedures for doing so are provided in Appendix B: Certificates from a Local Certification Authority in this document.

In a scenario where you anticipate the need for secure connections from public clients, as in the case where you are publishing a website to the Internet, we recommend that you obtain a certificate from a commercial CA. You thus avoid the issue of root certificate distribution, and will also have a certificate from a CA that is known and trusted by public users.

For more information about digital certificates, see the following articles:

- Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure (http://www.microsoft.com).
- An Introduction to the Windows 2000 Public-Key Infrastructure (http://www.microsoft.com).

Scenarios

Digital certificates are used in a wide variety of scenarios. Using Internet Security and Acceleration (ISA) Server 2004, there are two common publishing scenarios which may require digital certificate installation.

Publishing Using Server Publishing Rules

In this scenario, you are publishing an HTTPS server using server publishing rules. The solution for this scenario is provided in Publishing Using Server Publishing Rules Walk-through Procedure 1: Install an SSL Certificate in a Server Publishing Scenario in this document.

Publishing Using Web Publishing Rules

This scenario includes publishing Web servers and publishing Microsoft Outlook® Web Access servers, and can have several solutions. Specific Web publishing solutions depend on the following considerations:

- Are you going to use HTTPS to HTTPS bridging (recommended), which requires certificates on both the ISA Server computer and the Web server computer, or HTTPS to HTTP bridging, which requires a certificate only on the ISA Server computer?

Important

We recommend that for Web publishing, you install digital certificates on both the Web server and the ISA Server computer, and pass HTTPS requests as HTTPS. This is a more secure configuration.

- Do you already have a digital certificate installed on your Web server, and are now placing that Web server behind an ISA Server computer, or are you installing new certificates?

Based on these considerations, the Web publishing scenarios can be subdivided into more specific scenarios.

Web Server Already Has a Certificate Installed Scenario

For the scenario in which you have a Web server that already has a certificate installed on it:

- You are installing ISA Server in front of a Web server that already has a digital certificate, and then publishing the Web server through the ISA Server computer, using HTTPS to HTTPS SSL bridging. HTTPS to HTTPS bridging means that the communication from the client on the Internet to the ISA Server computer, and the communication between the ISA Server computer and the Web server, are both secured with certificates and use the HTTPS protocol. SSL bridging is described in Appendix C: SSL Bridging in this document. This scenario begins with one certificate already installed on the Web server. The solution for this scenario is provided in Publishing Using Web Publishing Rules Walk-through Procedure 2: Use HTTPS to HTTPS Bridging With Certificates Installed in this document.
- You are installing ISA Server in front of a Web server that already has a digital certificate, and then publishing the Web server through the ISA Server computer, using HTTPS to HTTP bridging. HTTPS to HTTP bridging means that the communication from the client on the Internet to the ISA Server computer is secured with a certificate, but the communication between the ISA Server computer and the Web server does not have to be secured, and is therefore over HTTP. This scenario begins with one certificate already installed on the Web server. The solution for this scenario is provided in Publishing Using Web Publishing Rules Walk-through Procedure 3: Use HTTPS to HTTP Bridging With Certificates Installed in this document.

Web Server With No Installed Certificate Scenario

For the scenario in which you do not have any certificates installed:

- You are publishing a Web server through an ISA Server computer, and want to use HTTPS to HTTPS bridging, but do not have any certificates installed. The solution for this scenario is provided in Publishing Using Web Publishing Rules Walk-through Procedure 4: Use HTTPS to HTTPS Bridging With No Certificate Installed in this document. This solution is also appropriate for the publishing of an Outlook Web Access server with HTTPS to HTTPS bridging.

- You are publishing a Web server through an ISA Server computer, and want to use HTTPS to HTTP bridging, but do not have any certificates installed. The solution for this scenario is provided in Publishing Using Web Publishing Rules Walk-through Procedure 5: Use HTTPS to HTTP Bridging With No Certificate Installed in this document.

Web Server With No Commercial CA Certificate Required Scenario

For the scenario in which you do not need a certificate from a commercial CA:

- You are publishing a Web server for corporate use only. The solution for this scenario is provided in Publishing Using Web Publishing Rules Walk-through Procedure 6: Use HTTPS to HTTPS Bridging With No Commercial CA Certificate Required in this document.

In addition to these publishing scenarios, you can configure a site-to-site VPN connection using IPSec tunneling or L2TP/IPSec with certificate-based authentication. The solution for this scenario is provided in the document Site-to-Site VPN in ISA Server 2004 (http://go.microsoft.com/fwlink?linkid=20746).

Solutions

The following sections provide the solutions to all of the previously listed scenarios.

Publishing Using Server Publishing Rules — Walk-through

When you publish a server using server publishing rules, install a digital certificate on the published server, and not on the ISA Server computer. Select HTTPS server as the mapped protocol in your server publishing rule.

Publishing Using Server Publishing Rules Walk-through Procedure 1: Install an SSL Certificate in a Server Publishing Scenario

The following are the general steps to install an SSL certificate in a server publishing scenario. Detailed instructions for each step are provided in the appendices, as noted in the steps.

1. Install a trusted root certificate on computers that will be SSL clients of the server certificate. If you are using a certificate from a commercial certification authority (CA) that is included in the Internet Explorer database of CAs, you do not have to perform this step.
2. Request and install a certificate. The name on the certificate must be the fully qualified host name or URL for the server that you are publishing, or clients will receive an error message when they send HTTPS requests to the server. To install a

certificate from a commercial CA, follow the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document. To install a certificate from a local CA, follow the procedures in Appendix B: Certificates from a Local Certification Authority in this document.

Publishing Using Web Publishing Rules — Walk-through

When using Web publishing rules to publish a server, if SSL communication from external clients is required, at a minimum, a server certificate must be installed on the ISA Server computer. In addition, you may install (or have previously installed) a certificate on the Web server. You must configure SSL bridging on the Web publishing rule accordingly. For more information, see Appendix C: SSL Bridging in this document.

Publishing Using Web Publishing Rules Walk-through Procedure 1: Install an SSL Certificate in a Web Publishing Scenario

The following are the general steps to install SSL certificates in a Web publishing scenario. The detailed procedure for each of these steps is provided later in this document.

1. Install a trusted root certificate on computers that will be SSL clients of the server certificate. If you are using a certificate from a commercial certification authority (CA) that is included in the Internet Explorer database of CAs, you do not have to perform this step. This procedure is described in Certificates from a Local Certification Authority Procedure 3: Install a Root Certificate in this document.

3. Request and install a certificate on the ISA Server computer. The name on the certificate must be the fully qualified domain name (FQDN) that client computers will use to access the website, such as www.adatum.com. If the name on the certificate is not the FQDN that client computers will use to access the website, clients will receive an error message from the ISA Server computer when they send HTTPS requests.

   - If you are obtaining a certificate from a local CA, it can be requested from and installed directly to the ISA Server computer. However, for most Web publishing purposes, you will use a certificate from a commercial CA, as most personal computers have those root certificates.

   - If you are obtaining a certificate from a commercial CA, you must prepare a certificate request file. This requires Internet Information Services (IIS), which we do not recommend installing on the ISA Server computer. For this reason, we recommend that you prepare the request and install the certificate on the Web server computer, and then export it to the ISA Server computer. Remember that this certificate must bear the FQDN that client computers will use to access the website. To submit a request, you will require access to the CA's website. We recommend that you transfer the request file from the Web server to a computer that does have access to the Internet. Alternatively, you could allow connectivity from your Web server to the commercial CA by creating an ISA Server access rule on the protocols used by the CA.

Note

The preceding steps explain the general steps to install a certificate on the ISA Server computer. The following step explains how to install an additional certificate on the Web server computer. A certificate is not required on the Web server computer to publish a secure website through ISA Server. The certificate on the ISA Server computer is sufficient, and your Web publishing rule would use HTTPS to HTTP bridging, forwarding unencrypted information internally to the Web server. However, we recommend that you use HTTPS to HTTPS bridging, which would require the installation of a certificate on the Web server as well as on the ISA Server computer.

4. Request and install a certificate for the Web server computer. The name on the certificate must match the name that ISA Server uses to refer to the Web server, which is the name on the **To** tab of the Web publishing rule. If the names do not match, ISA Server will receive an error message from the Web server computer when ISA Server sends an HTTPS request.

Note

When you create a Web publishing rule using the New Web Publishing Rule Wizard, the name you provide in **Computer name or IP Address** on the **Define website to Publish** page, is the name on the **To** tab of the Web publishing rule.

Publishing Using Web Publishing Rules Walk-through Procedure 2: Use HTTPS to HTTPS Bridging With a Certificate Installed

When installing ISA Server in front of an existing Web server currently published to the Internet, and then publishing the Web server through the ISA Server computer using HTTPS to HTTPS bridging, you will require a certificate on the ISA Server computer and a certificate on the Web server. Note that this procedure assumes that you already have a digital certificate from a commercial CA on the Web server.

The following steps provide general instructions. Detailed instructions for each step are provided in the appendices, as noted.

1. Export the existing certificate from the Web server to the ISA Server computer, as described in Certificates from a Commercial Certification Authority Procedure 4: Export a Certificate from the Web Server Computer to the ISA Server Computer in this document. The name that you use to publish the website in the Web publishing rule must match the name on the certificate.

Note

If you do not want to use the name on the existing digital certificate to publish the website, you must purchase a new commercial certificate following the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document.

2. Because you are publishing using HTTPS to HTTPS bridging, you can choose one of the following options for the certificate on the Web server:

   - Leave a copy of the existing certificate on the Web server. For this to work, the name on the **To** tab of the Web publishing rule must match the name on the certificate. That is, the published name and the name on the **To** tab must be the same. If the names do not match, ISA Server will receive an error message from the Web server computer when ISA Server sends an HTTPS request.

   - Request and install a new commercial certificate for the Web server following the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document. The name on the certificate must match the name that ISA Server uses to refer to the Web server, which is the name on the **To** tab of the Web publishing rule. If the names do not match, ISA Server will receive an error message from the Web server computer when ISA Server sends an HTTPS request.

   - Use a certificate from a local CA for the ISA Server computer to Web server connection. This would save you the cost of a second commercial certificate, and the root certificate from the local CA can be easily stored on the ISA Server computer. To do this, follow the procedures in Appendix B: Certificates from a Local Certification Authority in this document.

   Note

   Alternatively, you can leave the existing commercial certificate on the Web server, and request and install a new commercial certificate for the ISA Server computer following the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document.

Publishing Using Web Publishing Rules Walk-through Procedure 3: Use HTTPS to HTTP Bridging With a Certificate Installed

When installing ISA Server in front of an existing Web server currently published to the Internet, and then publishing the Web server through the ISA Server computer using HTTPS to HTTP bridging, you need a certificate on the ISA Server computer, but not on the Web server, because you are using HTTPS to HTTP bridging. Note that this procedure assumes that you already have a digital certificate from a commercial CA on the Web server.

The following step provides general instructions. Detailed instructions for this step are provided in the appendices.

- Export the existing certificate from the Web server to the ISA Server computer, as described in Certificates from a Commercial Certification Authority Procedure 4: Export a Certificate from the Web Server Computer to the ISA Server Computer in this document. The name that you use to publish the website must match the name you use to publish the Web server in the Web publishing rule.

  Note

If you do not want to use the name on the existing digital certificate, you must purchase a new commercial certificate following the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document.

- Remove the certificate from the Web server computer, as described in Certificates from a Commercial Certification Authority Procedure 6: Remove a Certificate from the Web Server Computer.

Publishing Using Web Publishing Rules Walk-through Procedure 4: Use HTTPS to HTTPS Bridging With No Certificate Installed

You are publishing a Web server through an ISA Server computer, and want to use HTTPS to HTTPS bridging, but do not have any certificates installed. You need a certificate on the ISA Server computer and on the Web server.

The following steps provide general instructions. Detailed instructions for each step are provided in the appendices.

3. Install a commercial certificate on the ISA Server computer. You must prepare a certificate request using the Internet Information Services (IIS) Web Server Certificate Wizard. Because IIS is typically not installed on the ISA Server computer, you will request the certificate from the Web server computer, and export it to the ISA Server computer. The name that you use to publish the website in the Web publishing rule must match the name on the certificate. To install the certificate, follow the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document.

4. Because you are publishing using HTTPS to HTTPS bridging, you can choose one of the following options for the certificate on the Web server:

   - Leave a copy of the certificate that you requested for the ISA Server computer on the Web server, so that both the ISA Server computer and the Web server have the same certificate. For this to work, the name on the **To** tab of the Web publishing rule must match the name on the certificate. That is, the published name and the name on the **To** tab must be the same. If the names do not match, ISA Server will receive an error message from the Web server computer when ISA Server sends an HTTPS request.

   - Request and install a new commercial certificate for the Web server following the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document. The name on the certificate must match the name that ISA Server uses to refer to the Web server, which is the name on the **To** tab of the Web publishing rule. If the names do not match, ISA Server will receive an error message from the Web server computer when ISA Server sends an HTTPS request.

   - Use a certificate from a local CA for the ISA Server computer to Web server connection. This would save you the cost of a second commercial certificate, and the root certificate from the local CA can be easily stored on the ISA Server computer. To do this, follow the procedures in Appendix B: Certificates from a Local Certification Authority in this document.

Publishing Using Web Publishing Rules Walk-through Procedure 5: Use HTTPS to HTTP Bridging With No Certificate Installed

You are publishing a Web server through an ISA Server computer, and want to use HTTPS to HTTP bridging, but do not have any certificates installed. You need a certificate on the ISA Server computer, but not on the Web server.

The following step provides general instructions. Detailed instructions for this step are provided in the appendices.

- Install a commercial certificate on the ISA Server computer. You must prepare a certificate request using the Internet Information Services (IIS) Web Server Certificate Wizard. Because IIS is typically not installed on the ISA Server computer, you will request the certificate from the Web server computer, and export it to the ISA Server computer. The name that you use to publish the website in the Web publishing rule must match the name on the certificate. To install the certificate, follow the procedures in Appendix A: Certificates from a Commercial Certification Authority in this document. Then, remove the certificate from the Web server computer, as described in Certificates from a Commercial Certification Authority Procedure 6: Remove a Certificate from the Web Server Computer.

Publishing Using Web Publishing Rules Walk-through Procedure 6: Use HTTPS to HTTPS Bridging With No Commercial CA Certificate Required

You are publishing a Web server for corporate use only, over several corporate networks, using HTTPS to HTTPS bridging. In this scenario, you need two digital certificates, one on the Web server and one on the ISA Server computer. Because the Web server will only be published internally, you can use certificates from a local CA. This assumes that you have access to the client computers that will connect to the ISA Server computer, so that you can install the root certificate for the local computer on each client computer.

The following steps provide general instructions. Detailed instructions for each step are provided in the appendices.

5. Install a certificate from a local CA on the ISA Server computer. To do this, follow the appropriate procedures in Appendix B: Certificates from a Local Certification Authority in this document.

6. Use a certificate from a local CA for the ISA Server computer to Web server connection. To do this, follow the appropriate procedures in Appendix B: Certificates from a Local Certification Authority in this document.

Appendix A: Certificates from a Commercial Certification Authority

Obtaining and installing a certificate from a commercial certification authority (CA) requires:

- Allowing connectivity to the CA.
- Generating a certificate request.
- Sending the request to the CA.
- Receiving the certificate from the CA and installing it.

If the certificate is intended for an ISA Server computer, you must also:

- Export the certificate to the ISA Server computer.
- Install the certificate on the ISA Server computer.
- Remove the certificate from the Web server computer (unless you are using the same certificate on both the ISA Server computer and the Web server computer).

The following procedure details how to generate a certificate request file. Perform this procedure on a computer that has Internet Information Services (IIS) installed. Because IIS is generally not installed on the ISA Server computer, this procedure usually is performed on the published server.

Notes

The certificate request fails if it contains nonalphanumeric characters.

Between creating the request file (that is, completing the following steps) and installing the certificate, do not perform any of the following actions:

- Change the computer name or website bindings.
- Apply service packs or security patches.
- Change encryption levels (that is, apply the high encryption pack).
- Delete the pending certificate request.
- Change any of the website's secure communications properties.

Certificates from a Commercial Certification Authority Procedure 1: Generate a Certificate Request

Perform the following procedure to generate a new certificate request to be sent to a CA for processing.

Note

Procedures vary slightly in different versions of IIS. The procedures in this document are based on IIS 6.0.

7. Open the Internet Services Manager as follows. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Internet Information Services (IIS) Manager** (or open your custom MMC containing the IIS snap-in).
8. Expand the local computer node and the **Web Sites** node. Right-click the website and select **Properties**.
9. Click the **Directory Security** tab.
10. In **Secure Communications**, click **Server Certificate**. This starts the New Web Site Certificate Wizard.
11. On the **Welcome** page, click **Next**.
12. On the **Server Certificate** page, select **Create a New Certificate**, and then click **Next**.
13. On the **Delayed or Immediate Request** page, select **Prepare the Request now, but Send it later** and click **Next**.
14. On the **Name and Security Settings** page, choose a friendly name for the site. This name is not critical to the functioning of the certificate, so pick a name that is easy to refer to and to remember.
15. Select the bit length of the key you want to use and whether you want to use cryptographic service provider (CSP), and then click **Next**.

    Note **For more information about bit length and CSP, see IIS Help.**

16. On the **Organization Information** page, provide your Organization and your Organizational Unit. For example, if your company is called Fabrikam, Inc. and you are setting up a Web server for the Sales department, you would enter **Fabrikam** for the Organization and **Sales** for your Organizational Unit. Click **Next**.
17. On the **Your Site's Common Name** page, provide the common name (CN) for your site. Before continuing this procedure, for information about the certificate name, see the following important information. After the naming considerations have been resolved, click **Next**.

    Important

    In Web publishing, if this certificate will be exported to the ISA Server computer, the name on the certificate must match the name you use to publish the website in the Web publishing rule. If this certificate will remain on the Web server, the name on the certificate must match the name that ISA Server uses to refer to the Web server, which is the name on the **To** tab of the Web publishing rule.

    In the case of server publishing, the certificate should have the name that users will use to connect to the server.

18. On the **Geographical Information** page, enter your information in **Country/Region**, **State/province**, and **City/locality**. It is important that you do not abbreviate the names of the state/province or city/locality. Click **Next**.
19. On the **Certificate Request File Name** page, provide a name for the certificate request file that you are about to create. This file will contain all the information that you included in this procedure, as well as the public key for your site. This

creates a .txt file when the procedure steps are completed. The default name for the file is Certreq.txt. Click **Next**.

20. On the summary page, verify that all of the information is correct, and then click **Next**.
21. On the **Completing the Web Server Certificate** page, click **Finish**.
22. Click **OK** to close the **Web Site Properties** dialog box.

Certificates from a Commercial Certification Authority Procedure 2: Submit a Certificate Request File

For the certificate to be used on the Internet, submit the request file to a CA (online authority). The CA will generate a certificate response file, which contains your public key and which is digitally signed by the commercial CA. Follow the instructions provided by the commercial CA to submit the request file. The CA will respond with a certificate response, which you will use to install the certificate.

Important

To submit a request, you will require access to the CA's website. We recommend that you copy the request file from the Web server to a computer that has access to the Internet, and then submit it to the CA according to the CA's instructions.

Alternatively, you can allow connectivity from your Web server to the commercial CA by creating an ISA Server access rule on the protocols used by the CA. The access rule should be as specific as possible. For example, if you require access on the HTTP protocol, create an allow rule from a computer set containing only the Web server, to a URL set containing only the CA's Web site, and allowing only HTTP traffic. For more information about access rules, see the ISA Server product documentation.

Certificates from a Commercial Certification Authority Procedure 3: Install a Certificate

After you receive your response file from the CA, install it on the Web server. A certificate that will be exported to the ISA Server computer must first be installed on the Web server for which the certificate was requested.

23. Open Internet Services Manager.
24. Expand Internet Information Services, and expand Web Sites. Select the website that has a pending certificate request.
25. Right-click the website and then click **Properties**.
26. Click the **Directory Security** tab.
27. In **Secure Communications**, click **Server Certificate**.
28. On the Web Site Certificate Wizard, click **Next**.
29. Select **Process the Pending Request and Install the Certificate** and click **Next**.

30. Type the location of the certificate response file (you may also browse to the file), and then click **Next**.

31. On the **SSL Port** page, select the SSL port that the Web site will use. By default, this is port 443.

32. On the **Certificate Summary** page, review the information to ensure that you are processing the correct certificate, and then click **Next**.

33. On the **Completing the Web Server Certificate Wizard** page, click **Finish**.

34. Verify that the server certificate was properly installed. From the **Start** menu, click **Run**. Type **MMC**, and then click **OK**.

35. In MMC, click **File**, and then click **Add/Remove Snap-in**.

36. In **Add/Remove Snap-in**, click **Add** to open the **Add Standalone Snap-in** dialog box. From the list of snap-ins, select **Certificates**, and then click **Add**.

37. In **Certificates snap-in**, select **Computer account**, and then click **Next**. In **Select Computer**, verify that **Local computer** (the default) is selected, and then click **Finish**. Click **Close**, and then click **OK**.

38. In MMC, expand **Certificates (local computer)**, expand the **Personal** node, click **Certificates**, and double-click the new server certificate. On the **General** tab, there should be a note that says **You have a private key that corresponds to this certificate**. On the **Certification Path** tab, you should see a hierarchical relationship between your certificate and the CA, and a note that says **This certificate is OK**.

39. Close MMC. Save the console settings with a descriptive name, such as **LocalComputerCertificates.msc**.

Certificates from a Commercial Certification Authority Procedure 4: Export a Certificate from the Web Server Computer to the ISA Server Computer

Use the following procedure to export a certificate from the Web server computer to the ISA Server computer.

40. **Add/Remove Snap-in**, and in the **Add/Remove Snap-in** dialog box, click **Add** to open the **Add Standalone Snap-in** dialog box.

41. Select **Certificates**, click **Add**, select **Computer account**, and then click **Next**.

42. In **Select Computer**, verify that **Local computer** (the default) is selected, and then click **Finish**. In the **Add Standalone Snap-in** dialog box click **Close,** and in the **Add/Remove Snap-in** dialog box, click **OK**.

43. Expand the **Certificates** node, expand **Personal**, and then click **Certificates**. A certificate with the name of your website appears in the **Issued To** column in the right pane.

44. Right-click your certificate, click **All Tasks**, and then click **Export**. This opens the Certificate Export Wizard.

45. In the welcome page, click **Next**.

46. On the **Export Private Key** page, select **Yes, export the private key**, and then click **Next**.

    Note

    If you do not have the option to click **Yes** in the **Export Private Key** page, the private key has already been exported to another computer or the key never existed on this computer. You cannot use this certificate on the ISA Server computer. You must request a new certificate for ISA Server for this website.

47. On the **Export File Format** page, select **Personal Information Exchange**. Maintain the default setting for all three check boxes. Click **Next**.

48. On the **Password** page, assign a password to protect the exported file, and then confirm the password. Click **Next**

49. On the **File to Export** page, provide a file name and location for the export file, and then click **Save**. Click **Next**.

50. On the wizard completion page, click **Finish**. Make sure that you safeguard the file that you just created, because your ability to use the SSL protocol depends upon this file.

51. Copy the file that you created to the ISA Server computer.

Certificates from a Commercial Certification Authority Procedure 5: Install a Certificate on the ISA Server Computer

Use the following procedure to install a certificate on the ISA Server computer. This procedure assumes that you successfully exported a certificate as described in Certificates from a Commercial Certification Authority Procedure 4: Export a Certificate from the Web Server Computer to the ISA Server Computer in this document, and that you copied the file to the ISA Server computer.

52. Click **Start**, and then click **Run**. In **Open**, type **MMC**, and then click **OK**.

53. Click **File**, click **Add/Remove Snap-in**, and in the **Add/Remove Snap-in** dialog box, click **Add** to open the **Add Standalone Snap-in** dialog box.

54. Select **Certificates**, click **Add**, select **Computer account**, and then click **Next**.

55. Select **Local Computer**, and then click **Finish**. In the **Add Standalone Snap-in** dialog box, click **Close,** and in the **Add/Remove Snap-in** dialog box, click **OK**.

56. Expand the **Certificates** node, and right-click the **Personal** folder.

57. Select **All Tasks**, and then click **Import**. This starts the Certificate Import Wizard.

58. On the **Welcome** page, click **Next**.

59. On the **File to Import** page, browse to the file that you created previously in Procedure 4, and then click **Next**.

60. On the **Password** page, type the password for this file, and then click **Next**.

    Note

    The **Password** page provides the option **Mark this key as exportable**. If you want to prevent the exporting of the key from the ISA Server computer, do not select this option.

61. On the **Certificate Store** page, verify that the selection **Place all certificates in the following store** and **Certificate Store** are set to **Personal** (the default settings), and then click **Next.**

62. On the wizard completion page, click **Finish**.

63. Verify that the server certificate was properly installed. Open the MMC console that you created in Procedure 4. From the **Start** menu, point to **All Programs**, point to **Administrative Tools**, and select **LocalComputerCertificates.msc** (or the name that you provided when creating the certificates console).

64. Expand **Certificates (local computer)**, expand the **Personal** node, click **Certificates**, and double-click the new server certificate. On the **General** tab, there should be a note that shows **You have a private key that corresponds to this certificate**. On the **Certification Path** tab, you should see a hierarchical relationship between your certificate and the CA, and a note that shows **This certificate is OK**.

Certificates from a Commercial Certification Authority Procedure 6: Remove a Certificate from the Web Server Computer

If you will be using a different certificate on the Web server computer, you must remove the exported certificate from Internet Information Services (IIS). You may also want to delete the certificate from the Web server computer. This will reduce the possibility that the certificate will be used elsewhere.

Use the following procedure to remove a certificate from the Web server computer. There are two parts to this procedure: removing the certificate from IIS, and deleting the certificate from the computer.

To remove the certificate from IIS.

65. On the Web server computer, open Internet Services Manager.

66. Expand the server node and select the **Default Web Site** node. Click **Properties**.

67. Click the **Directory security** tab. In **Secure Communications**, click **Server Certificate**. This starts the New Web Site Certificate Wizard.

68. On the **Welcome** page, click **Next**.

69. On the **Modify the Current Certificate Assignment** page, select **Remove the current certificate** and click **Next**.

70. On the **Remove a Certificate** page, click **Next.**

71. On the wizard completion page**,** click **Finish**.

72. Close Internet Services Manager.

To delete the certificate from the computer.

73. Open the MMC console that you created in Procedure 4. From the **Start** menu, point to **All Programs**, point to **Administrative Tools**, and select **LocalComputerCertificates.msc** (or the name that you provided when creating the certificates console).

74. Expand **Certificates (local computer)**, expand the **Personal** node, click **Certificates**, and right-click the certificate. Click **Delete**, and then click **OK** on the warning dialog box.

Appendix B: Certificates from a Local Certification Authority

You need a certification authority (CA) if you want to issue digital certificates. When the certificates are for internal use, we recommend that you create a local CA, negating the need to purchase a commercial certificate.

Certificates from a Local Certification Authority Procedure 1: Set Up the Certification Authority

This procedure is performed on a computer running Windows Server 2003 or Windows 2000 Server. For a stand-alone root CA, this can be any computer. An enterprise root CA must be installed on a server that is a member of a domain.

This procedure also installs the services that will enable computers to obtain the certificates through a Web page. If you prefer a different approach for obtaining the certificates for computers, you do not have to perform the Internet Information Services (IIS) and Active Server Pages installations described in this procedure.

75. Open the Control Panel.

76. Double-click Add **or Remove Programs**.

77. Click **Add/Remove Windows Components**.

78. Double-click **Application Server**.

79. Double-click **Internet Information Services (IIS)**.

80. Double-click **World Wide Web Service**.

81. Select **Active Server Pages**.

82. Click **OK** to close the **World Wide Web Service** dialog box, click **OK** to close the **Internet Information Services (IIS)** dialog box, and then click **OK** to close the **Application Server** dialog box.

83. Select **Certificate Services**. Review the warning regarding the computer name and domain membership. Click **Yes** in the warning dialog box if you want to continue, and then click **Next** in the **Windows components** dialog box.

84. On the **CA Type** page, choose one of the following, and then click **Next**:

   - **Enterprise-root CA.** An enterprise root CA must be installed on a domain member. The enterprise root CA will automatically issue certificates when requested by authorized users (recognized by the domain controller).

   - **Stand-alone root CA.** A stand-alone root CA requires that the administrator issue each requested certificate.

85. On the **CA Identifying Information** page, provide a common name for the CA, check the distinguished name suffix, select a validity period, and then click **Next**.

86. On the **Certificate Database Settings** page, review the default settings. You may revise the database locations. Click **Next**.

87. On the **Completing the Windows Components Wizard** page, review the summary, and then click **Finish**.

   Note

   To allow access to the CA website, you must publish it. To limit access to the website, you can publish only the specific folders needed from the website to a specific set of users, rather than publishing a complete server to all users. For more information about Web publishing, see the document Publishing Web Servers Using ISA Server 2004 (http://go.microsoft.com/fwlink/?LinkId=20744).

Certificates from a Local Certification Authority Procedure 2: Install a Server Certificate

This procedure is performed on the computer that requires the digital certificate. In the case of Web publishing, this will be the ISA Server computer, at a minimum, and may also include the Web server computer. In the case of server publishing, this will be only the server computer that you are publishing. If you installed a stand-alone root CA rather than an enterprise root CA, there are also actions that take place on the certification authority.

88. Open Internet Explorer.

89. From the menu, select **Tools**, and then select **Internet Options**.

90. Select the **Security** tab, and in **Select a Web content zone to specify its security settings**, click **Trusted Sites**.

91. Click the **Sites** button to open the **Trusted sites** dialog box.

92. In **Add this Web site to the zone**, provide the certificate server website name (http://*IP address of certification authority server*/certsrvname) and click **Add**.

93. Click **Close** to close the **Trusted sites** dialog box, and then click **OK** to close Internet Options.

94. Browse to: http://*IP address of certification authority server*/certsrv.

95. Request a certificate.

96. Select **Advanced Certificate Request**.

97. Select **Create and submit a request to this CA** (Windows Server 2003 CA), or **Submit a certificate request to this CA using a form** (Windows 2000 Server CA).

98. Complete the form and select **Server Authentication Certificate** from the **Type** drop-down list. To avoid the client receiving an error when trying to connect, it is critical that the common name you provide for the certificate matches the published server name, as follows:

    - For server publishing, in common name, type the fully qualified host name or URL for the server you are publishing.

    Note

    For an explanation of the options available on the **Advanced Certificate Request** page, see one of the following articles for Windows Server 2003 or Windows 2000 Server:

    - Using Windows Server 2003 Certificate Services Web pages (http://www.microsoft.com)
    - Using Windows 2000 Certificate Services Web pages (http://www.microsoft.com)

    - For Web publishing, for a certificate on the ISA Server computer, type the fully qualified host name or URL that external clients will type in their Web browser to access the website, for example news.adatum.com.
    - For Web publishing, if you are also installing a server certificate on the Web server in addition to the certificate required on the ISA Server computer, the common name is the name that the ISA Server computer uses to access the Web server through the Web publishing rule. This should be the fully qualified domain name (FQDN) of the Web server, such as webserver1.adatum.com.

99. Select **Store Certificate in the local computer certificate store** (Windows Server 2003 CA) or **Use local machine store** (Windows 2000 Server CA) and submit the request by clicking **Submit**. Review the warning dialog box that appears, and then click **Yes**.

100. If you installed a stand-alone root CA, perform the following steps on the certification authority computer. These steps are automated in an enterprise root CA.

    a. Go to the Microsoft Management Console (MMC) Certification Authority snap-in, (Click **Start**, point to **All Programs**, point to **Administrative tools**, and then select **Certification Authority**.)

    b. Expand the *CAName* certificates node, where *CAName* is the name of your certification authority.

c. Click the **Pending requests** node, right-click your request, select **All Tasks**, and then select **Issue**.

101. On the ISA Server computer, return to the Web page http://*IP address of certification authority server*/certsrv, and then click **View status of a pending request**.

102. Click your request and choose **Install this certificate**.

103. Verify that the server certificate was properly installed. Open MMC, and go to the Certificates snap-in. Open **Certificates (local computer)**, expand the **Personal** node, click **Certificates**, and double-click the new server certificate. On the **General** tab, there should be a note that says **You have a private key that corresponds to this certificate**. On the **Certification Path** tab, you should see a hierarchical relationship between your certificate and the root certificate, and a note that says **This certificate is OK**.

Note

On an ISA Server 2004 computer, and on any virtual private network (VPN) server running Windows Server 2003 or Windows 2000 Server, the server certificate obtained from a CA must be stored in the Personal Certificate store of the ISA Server computer. The root certificate for the VPN server to which the connection will be established must be stored in the Trusted Root Certificate Authorities store of the ISA Server computer.

Certificates from a Local Certification Authority Procedure 3: Install a Root Certificate

For a client computer to trust the server certificates that you have installed from a local CA, it must have installed the root certificate from the CA. Follow this procedure on any client computer that requires the root certificate. Note that you can also transfer the root certificate on a medium such as a disk, and then install in on the client computer.

104. Open Internet Explorer.

105. From the menu, select **Tools**, and then select **Internet Options**.

106. Select the **Security** tab, and click **Custom Level** to open the **Security Setting**s dialog box. Set the value in the **Reset custom settings** drop-down menu to **Medium**, click **OK** to close the **Security Settings** dialog box, and then click **OK** to close the **Internet Options** dialog box.

Note

Certificate installation is not possible when the security setting is set to **High**.

107. Browse to: http://*IP address of certification authority server*/certsrv.

108. Click **Download a CA Certificate, Certificate Chain, or CRL** (the text used by Windows Server 2003) or **Retrieve the CA certificate or certificate revocation list** (the text used by Windows 2000 Server). On the next page, click **Download CA Certificate**. This is the trusted root certificate that must be installed on the ISA Server computer. In the **File Download** dialog box, click **Open**.

109. On the **Certificate** dialog box, click **Install Certificate** to start the Certificate Import Wizard.

110. On the **Welcome** page, click **Next**. On the **Certificate Store** page, select **Place all certificates in the following store** and click **Browse**. In the **Select Certificate Store** dialog box, select **Show Physical Stores**. Expand **Trusted Root Certification Authorities**, select **Local Computer**, and then click **OK**. On the **Certificate Store** page, click **Next**.

111. On the summary page, review the details and click **Finish**.

112. Verify that the root certificate was properly installed. Open MMC, and go to the Certificates snap-in. Open **Certificates (local computer)**, expand the **Trusted Root Certification Authorities** node, click **Certificates**, and verify that the root certificate is in place.

Note

You can also install certificates on a computer from the MMC Certificates (Local Computer) snap-in. This only provides access to CAs on the same domain.

Appendix C: SSL Bridging

If you are publishing a server that requires Secure Sockets Layer (SSL) communication, you must have a digital certificate installed on your ISA Server computer. In addition, you may have a digital certificate installed on the Web server or Outlook Web Access server. In either case, to ensure that SSL requests are sent from the ISA Server computer to the Web server using the appropriate protocol, you must configure SSL bridging accordingly.

SSL bridging is a property for each Web publishing rule. SSL bridging determines whether SSL requests received by the ISA Server computer are passed to the Web server as SSL requests or as Hypertext Transfer Protocol (HTTP) requests, as follows:

- If there is no digital certificate installed on the Web server, SSL and HTTP requests must be passed to the Web server as HTTP requests. The SSL-secured communication is handled by ISA Server, and the request continues internally using the HTTP protocol.
- If there is a digital certificate installed on the Web server, SSL requests are passed to the internal Web server as SSL requests, and HTTP requests are passed as HTTP requests. You can also select to have both SSL and HTTP requests passed as SSL requests. SSL-secured communication is performed on both the ISA Server computer and the Web server levels.

If your Web server has a digital certificate, and you want ISA Server to listen for SSL requests without purchasing an additional certificate, you must export the certificate from the Web server and import it to the ISA Server computer.

Use the following steps to modify the SSL bridging configuration.

113. In the **Properties** dialog box of the Web publishing rule, select the **Bridging** tab.

114. Ensure that **Web server** is selected.

115. Perform one of the following to select redirection to either an HTTP port or SSL port:

- If you are using the ISA Server SSL certificate to handle SSL requests (no SSL certificate is installed on the Web server), select **Redirect requests to HTTP port**, and then click **OK**.
- If you want to continue to use an existing SSL certificate on the Web server (as well as the certificate on the ISA Server computer), select **Redirect requests to SSL port**, ensure that the default port number 443 is appropriate to your network, and then click **OK**. To force the redirection of HTTP requests to the SSL port, clear the **Redirect requests to HTTP port** checkbox.

Note

The option **Use a certificate to authenticate to the SSL Web server** enables you to specify the client certificate that ISA Server will use to authenticate itself to the Web server.

Appendix D: Certificate Troubleshooting

A common issue in Web publishing using SSL bridging is that the server name or IP address provided on the Web publishing rule **To** tab does not match the name on the digital (SSL) certificate. This will result in the Web client receiving a **500 Internal Server Error** page, with the message **principal name is incorrect**.

This problem can be resolved using one of the following approaches:

- Obtain a new certificate that matches the name on the Web server.
- Change the server name on the Web publishing rule **To** tab to match the name on the certificate, and configure the local DNS server to map that name to the internal Web server.
- Change the server name on the Web publishing rule **To** tab to match the name on the certificate. On the ISA Server computer, in the file WINNT\system32\drivers\etc\hosts, add a mapping from the certificate **To** tab name to the IP address of the internal Web server.

A **500 Internal Server Error** page will also be received by a Web client in an HTTPS to HTTPS bridging scenario, if the certificate on the Web server has expired.

To resolve this issue, obtain a new certificate for the published Web server. This error no longer occurs when the published server has a valid certificate.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, places, or events is intended or should be inferred.

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious and no association with any real company, organization, product, person, or event is intended

Do you have comments about this document? Send feedback.