There may be circumstances when you may wish to access the Web enrollment site from an external network client. This is most common when the external client needs to obtain an IPSec certificate from a standalone CA on your internal network. Machines don't typically need to access an enterprise CA because certificates are more easily obtained via certificate autoenrollment or the Certificates MMC snap-in.

Publishing the Certificate Web enrollment works like any other type of Web publishing. The specific procedures required to publish a Certificate Server Web enrollment site include:

- Install Internet Information Server and the Standalone Certification Authority
- Identify the Location of the CRL and configure the CRL publishing site and the AIA for the CTL (Certificate Trust List)
- Create a DNS entry in the public DNS
- Install ISA Server 2000 and configure the Incoming Web Requests listener
- Create the Destination Set and HOSTS file entry to support the Web Publishing Rule
- Create the Web Publishing Rule

We will cover each of these procedures in this ISA Server 2000 VPN Deployment Kit document.

Install Internet Information Server (IIS) and the Standalone Certification Authority

The Web enrollment site requires the Internet Information Service World Wide Web service (W3SVC). You must install IIS before installing Microsoft Certificate Services. IIS is installed by default on Windows 2000, but it is not installed by default in Windows Server 2003.

Perform the following steps to install IIS 6.0 on the Windows Server 2003 member server or domain controller computer that act as a standalone CA:

- 1. Click Start, point to Control Panel and click Add or Remove Programs.
- 2. Click the **Add/Remove Windows Components** button in the **Add or Remove Programs** window (figure 1).

| 🐻 Add or Rem | nove Programs | | <u> </u> |
|---|--|-------------------------------------|-------------------------|
| 5 | Currently installed programs: | Sort by: Name | × |
| Change or Remove Programs | ⊕ VMware Tools | Size Used | <u>1.06MB</u> rarely |
| Add <u>N</u> ew Programs | To change this program or remove it from your computer, click Change | Last Used On 5 e/Remove. Change/ | 5/28/2003 /Remove |
| Add/Remove <u>W</u> indows Components | | | |
| | | | |
| | | | |
| | | | |
| 🏄 Start 🛛 🞯 | Add or Remove Programs | * |) 11:45 AM |

3. On the **Windows Components** window, click on the **Application Server** entry and click the **Details** button (figure 2).

| 🐻 Add or Remo | ove Programs | - UX |
|--|--|-------------|
| | Windows Components Wizard | × |
| | Windows Components | |
| C <u>h</u> ange or Remove Programs | You can add or remove components of Windows. | |
| Add <u>N</u> ew Programs | To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: | 2003 pve |
| | Accessories and Utilities 4.5 MB | |
| | 🗹 📑 Application Server 24.6 MB 🗖 | |
| Add/Remove | Ecrificate Services 1.4 MB | |
| <u>W</u> indows Components | E-mail Services 1.1 MB | |
| | I Cale Fax Services 22.0 MB | |
| | Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console. | |
| | Total disk space required: 3.6 MB Details | |
| | Space available on disk: 1943.5 MB | |
| | | |
| | < <u>Back Next></u> Cancel Help | |
| 🏄 Start 🛛 🕑 | and the second s |) 5:18 PM |

4. On the **Application Server** page (figure 3), click on the **Internet Information Services (IIS)** entry and click the **Details** button.

| 🐻 Add or Remo | ove Programs Windows Components Winord | ~미지 |
|---------------------------------|--|--------------------------------|
| \$ | Application Server | |
| Change or Remove Programs | To add or remove a component, click the check box. A shaded box means that only pa of the component will be installed. To see what's included in a component, click Details Subcomponents of Application Server: | rt <u>6MB</u> arely 2003 |
| - - | Application Server Console 0.0 MB | - bvel |
| Add New | 🗆 🎭 ASP.NET 0.0 MB | |
| Programs | 🗹 🙆 Enable network COM+ access 0.0 MB | |
| | D.0 MB O.0 MB | |
| | 🔲 💱 Internet Information Services (IIS) 🗤 🗤 🗤 🖓 👘 👘 👘 💷 18.1 MB. | |
| Add/Remove <u>W</u> indows | 🗌 🚅 Message Queuing 6.5 MB | |
| | Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP). | |
| | Total disk space required: 3.6 MB Details | |
| | Space available on disk: 1943.5 MB | |
| | OK Cancel | |
| | < <u>B</u> ack <u>N</u> ext > Cancel | Help |
| 🏦 Start 🛛 🚱 | a Add or Remove Programs | 🍓 👜 5:18 PM |

5. In the **Internet Information Service (IIS)** dialog box (figure 4), put a checkmark in the **World Wide Web Service** checkbox and click **OK**.

| 🐻 Add or Remo | ove Proorams | -lov |
|------------------|--|--------------------------------|
| | Windows Components Wizard | <u>×</u> |
| | Application Server | |
| Change or | Internet Information Services (IIS) | 🗵 💿 <u>Emb</u> |
| Programs | To add or remove a component, click the check box. A shaded box means that only p of the component will be installed. To see what's included in a component, click Deta | part <u>arely</u> ils. 2003 |
| | Subcomponents of Internet Information Services (IIS): | pve |
| Add <u>N</u> ew | LI 💱 FrontPage 2002 Server Extensions 5.1 MB | |
| riograms | 🗹 🗹 🃸 Internet Information Services Manager 1.3 MB | |
| 1 | 🗌 🌐 🎯 Internet Printing 0.0 MB | |
| <u></u> | 🗌 🔤 🚳 NNTP Service 1.2 MB | |
| Add/Remove | SMTP Service 1.3 MB | |
| <u>_W</u> indows | 🗹 🏈 World Wide Web Service 8.0 MB | |
| Components | | |
| | Description: A core component of IIS that uses HTTP to exchange information with Web clients on a TCP/IP network. | |
| | Total disk space required: 14.1 MB Details | |
| | Space available on disk: 1943.5 MB | |
| | OK Cancel | |
| | | IP. |
| | · · · · · · · · · · · · · · · · · · · | |
| | | 87 |
| | | |
| Start 3 | Mindows Component | 1 🥸 👜 - 5:20 PM |

6. Click **OK** on the **Application Server** dialog box (figure 5).

| 🐻 Add or Remo | ve Programs | -loo |
|---------------------------------|---|--------------------------------|
| | Windows Components Wizard | × |
| | Application Server | |
| Change or Remove Programs | To add or remove a component, click the check box. A shaded box means that only pa of the component will be installed. To see what's included in a component, click Details Subacconstant of Application Course | rt <u>6MB</u> arely 2003 |
| 25 | Sub <u>c</u> omponents of Application Server. | |
| ن الا ال ال | | |
| Programs | Top Ash INCT OOMB OOMB | |
| Contract Processing | Company access | 1 |
| F | Internet Information Services (IIS) 181 MB | |
| Add /Pomouo | Message Queuing 65 MB | |
| Windows | | 2 |
| Components | | |
| | Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP). | |
| | Total disk space required: 14.1 MB | |
| | Space available on disk: 1943.5 MB | |
| | | |
| | | |
| | | |
| | < <u>B</u> ack <u>N</u> ext> Cancel | Help |
| - | | |
| | | |
| 🎒 Start 🛛 🚱 💡 | 🥑 🛛 🚮 Add or Remove Programs 🛛 🚮 Windows Component | 🌯 😥 5:21 PM |

7. Click Next on the Windows Components dialog box (figure 6).

| 🐻 Add or Remo | ye Programs | |
|---|--|----------------------|
| | Windows Components Wizard | |
| Change or Remove | Windows Components You can add or remove components of Windows. | <u>►</u> |
| Programs Add <u>N</u> ew Programs | To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: | arely 2003 ove |
| <i>—</i> | ✓ Image Accessories and Utilities | |
| | 🗹 🗃 Application Server 24.6 MB 💻 | |
| Add/Remove | Eertificate Services 1.4 MB | |
| <u>w</u> indows Components | E-mail Services 1.1 MB 22 0 MB | |
| | Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console. | |
| | Total disk space required: 14.1 MB | |
| T | K <u>B</u> ack <u>N</u> ext > Cancel Help | |
| 赶 Start 🛛 🕑 🧋 | 🥑 🔰 🔂 Add or Remove Programs 🛛 🔂 Windows Component 🥸 👰 5: | 22 PM |

8. Click Finish on the Completing the Windows Components Wizard page (figure 7).

| 🐻 Add or Rem | ove Programs | -lov |
|--|---|-----------------------------|
| Change or Remove Programs Add <u>N</u> ew Programs Add/Remove <u>Windows</u> Components | Windows Components Wizard Image: Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard. You have successfully completed the Windows Components Wizard. To close this wizard, click Finish. | EMB arely 2003 ove |
| | KBack Finish Help | |
| 🏄 Start 🛛 🚱 | 🥑 🔰 Add or Remove Programs 🛛 🔂 Windows Component | 5:26 PM |

Installing Microsoft Certificate Services

Perform the following steps to install and configure a stand-alone CA on a Windows Server 2003 computer:

Mote:

We recommend that you install the stand-alone CA on a member server or domain controller on your internal network. This allows the standalone Certificate Authority's CA certificate to be automatically placed in the Trusted Root Certification Authorities certificate store for all users and computers in the domain.

- 1. At a member server or domain controller in your internal network, log on as a domain administrator. Click **Start**, point to **Control Panel** and click **Add/Remove Programs**.
- 2. In the Add or Remove Programs window (figure 8), click the Add/Remove Windows Components button.

| 🐻 Add or Rem | ove Programs | | - U × |
|---|--|--|-------------------------|
| 5 | Currently installed programs: | Sort by: Name | T |
| Change or Remove Programs | ⊕ ∀Mware Tools | Size . Used | <u>1.06MB</u> rarely |
| Add <u>N</u> ew Programs | To change this program or remove it from your comput | Last Used On 5/2 er, click Change/Remove. Change/Re | 8/2003 emove |
| Add/Remove <u>W</u> indows Components | | | |
| Components | | | |
| | | | |
| | | | |
| | | | |
| 🐮 Start 🛛 🚱 | 🥭 🔢 🔂 Add or Remove Programs | 🍓 🔁 | 11:00 AM |

3. In the **Windows Components** dialog box (figure 9), click on the **Certificate Services** entry and click the **Details** button.

| 🐻 Add or Ren | nove Programs | |
|---------------------------------|--|---------------------------------|
| · 🛋 💆 | /indows Components Wizard | × |
| Change or Remove Programs | Windows Components You can add or remove components of Windows. | I.06MB rarely |
| Add <u>N</u> ew Programs | To add or remove a component, click the checkbox. A shaded box mea part of the component will be installed. To see what's included in a comp Details. <u>C</u> omponents: | 28/2003 ponent, click Remove |
| 1 | Accessories and Utilities | 4.5 MB |
| <u> </u> | Application Server | 24.6 МВ |
| Add/Removi | Certificate Services | 1.4 MB |
| Components | 🗆 🛄 E-mail Services | 1.1 MB |
| | I Gild Fax Services | 22.0 MR 🔟 |
| | Description: Installs a certification authority (CA) to issue certificates for public key security programs. | use with |
| | Total disk space required: 2.9 MB | Details |
| | Space available on disk: 1942.7 MB – | |
| | | |
| | < <u>B</u> ack <u>N</u> ext > Cancel | Help |
| | | |
| 🎒 Start 🛛 🚱 | Add or Remove Programs S Windows Component. | |

4. In the **Certificate Services** dialog box, put a checkmark in the **Certificate Services CA** checkbox (figure 10). A **Microsoft Certificate Services** dialog box appears and informs you that you can not change the machine name or the domain membership of the machine while it acts as a certificate server. Read the information in the dialog box and click **Yes**.

| 🐻 Add or Remove Programs | |
|--|------------------|
| Add or Remove Programs Windows Components Wizard Change or Remove Programs Vorded or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subgomponents of Certificate Services: Image: Certificate Services CA Image: Certificate Services Image: Certificate Services CA Image: Certificate Services CA Image: Certificate Services CA Image: Certificate Services CA Image: Certificate Services Image: | MB rely ve |
| 🛃 Start 🛛 😰 🧔 🔹 🕺 🔂 Add or Remove Programs 🛛 🔂 Windows Component 🥸 👜 11:0 | 03 AM |

5. Both the **Certificate Services CA** and **Certificate Services Web Enrollment Support** checkboxes are checked (figure 11). Click **OK** in the **Certificate Services** dialog box.

| Add or Remove Programs | |
|--|-------|
| Windows Components Wizard | _ |
| | • |
| Change or Certificate Services | MB |
| Programs To add or remove a component, click the check box. A shaded box means that only part ra | rely |
| of the component will be installed. To see what's included in a component, click Details. 28/2 | 003 |
| Subcomponents of Certificate Services: | ve |
| Add New Certificate Services CA 0.2 MB | |
| Programs Certificate Services Web Enrollment Support 1.2 MB | |
| E 1 | |
| | |
| Add/Removi | |
| | |
| | |
| Description: Allows you to publish web pages on your server to submit requests and retrieve certificates from a CA. | |
| | |
| I otal disk space required: 4.6 MB Details | |
| Space available on disk: 1942.7 MB | |
| Cancel | |
| | |
| | |
| | |
| Start 2 Add or Bemove Programs Windows Component | 05 AM |
| | |

6. Click Next in the Windows Components dialog box (figure 12).

| 🐻 Add or Rei | move Programs | |
|---------------------------------|--|--------------------|
| - V | Windows Components Wizard | × |
| Change or Remove Programs | Windows Components You can add or remove components of Windows. | |
| Add <u>N</u> ew Programs | To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. <u>C</u> omponents: | '28/2003 Remove |
| 1 | 🗹 📻 Accessories and Utilities 🛛 4.5 MB 🔺 | |
| | 🗹 🗃 Application Server 24.6 MB 💻 | |
| Add/Removi | Ertificate Services | |
| Components | 🗆 🛄 E-mail Services 1.1 MB 🔤 | |
| | I @4Eax Services 22.0 MB | |
| | Description: Installs a certification authority (CA) to issue certificates for use with public key security programs. | |
| | Total disk space required: 4.6 MB Details | |
| | Space available on disk: 1942.7 MB | |
| | | |
| | Z Back Newt Cancel Hold | |
| | | |
| | | |
| 🏄 Start 🛛 🕑 | 🕽 🥑 🚽 🔂 Add or Remove Programs 🛛 🔂 Windows Component | 👜 11:07 AM |

7. Select the **Stand-alone root CA** option on the **CA Type** page (figure 13). Click **Next**.

| 🔂 Add or R | emove Programs | |
|---|---|----------------------|
| | Windows Components Wizard | |
| Change or Remove Programs | CA Type Select the type of CA you want to set up. | <u>1.06MB</u> rarely |
| Add <u>N</u> ew Programs Add/Remov <u>W</u> indows Components | Enterprise root CA Enterprise subordinate CA Stand-alone root CA Stand-alone subordinate CA Description of CA type The most trusted CA in a CA hierarchy. | '28/2003 Remove |
| | Use custom settings to generate the key pair and CA certificate < Back Next> Cancel Help | |
| 🦺 Start 🛛 🚺 | 🗿 🥭 🔢 📆 Add or Remove Programs 🛛 📆 Windows Component 🦓 🚳 | 11:08 AM |

8. On the CA Identifying Information page, type in a Common name for this CA. The common name of the CA is typically the DNS host name or NetBIOS name (computer name) of the machine running Certificate Services. In this example, the name of the machine is WIN2003DC, so we will enter WIN2003DC in the Common name for this CA text box. The default Validity Period of the CA's self-signed certificate is 5 years. Accept this default value unless you have a reason to change it. Click Next.

| 🐻 Add or Re | move Programs | |
|---------------------------------|--|-------------------------|
| V | Vindows Components Wizard | |
| Change or Remove Programs | CA Identifying Information Enter information to identify this CA. | <u>1.06MB</u> rarely |
| <u></u> | Common name for this CA: | 28/2003 |
| | WIN2003DC | Remove |
| Add <u>N</u> ew Programs | Distinguished name suffix: | |
| <u>ب</u> | DC=internal,DC=net | |
| | | |
| Add/Hemov <u>W</u> indows | Preview of distinguished name: | |
| Components | CN=WIN2003DC;DC=internal;DC=net | |
| | | |
| | Validity period: Expiration date: | |
| | 5 Years V | |
| | | |
| | | - |
| | < <u>B</u> ack <u>Next></u> Cancel Help | |
| - | | |
| | | |
| 🛃 Start 🛛 🕑 | 👌 🥑 🔂 Add or Remove Programs 🛛 🔂 Windows Component 🥸 | 11:10 AM |

9. On the **Certificate Database Settings** page (figure 15), use the default locations for the **Certificate Database** and **Certificate Database Log**. You do not need to specify a shared folder to store configuration information because this information will be stored in the Active Directory. Click **Next**.

| 🐻 Add or Rem | iove Programs | |
|---|---|------------|
| - W | indows Components Wizard | × |
| Change or Remove Programs | Certificate Database Settings Enter locations for the certificate database, database log, and configuration information. | |
| 2 | Certificate database: | 28/2003 |
| Add New | C:\WINDOWS\system32\CertLog Brgwse | Remove |
| Programs | Certificate database log: | |
| | C:\WINDOWS\system32\CertLog Browse | |
| Add/Removi <u>W</u> indows Components | Store configuration information in a shared folder Shared folder: Browse Browse Preserve existing certificate database | |
| - | < <u>B</u> ack <u>N</u> ext> Cancel <u>Help</u> | |
| 🦺 Start 🛛 🚱 | 🥵 🔢 🚮 Add or Remove Pr 🔀 Windows Comp 🥑 Help and Support 🦓 | 💼 11:15 AM |

10. Click **Yes** on the **Microsoft Certificate Services** dialog box (figure 16) informing you that Internet Information Services must be stopped temporarily.

| 🐻 Add or Remove P | rograms | |
|-------------------------------------|---|------------------|
| Window | s Components Wizard | |
| Certi | ificate Database Settings | |
| Change or Remove | Enter locations for the certificate database, database log, and configuration | 1.06MB rarely |
| | Certificate database: | 28/2003 |
| Add New | C:\WINDOWS\system32\CertLog Browse | Hemove |
| Programs (| Certificate database log: | |
| | C. Microsoft Certificate Services | |
| Add/Remove Windows Components | Yes No Preserve existing certificate database | |
| | < <u>B</u> ack <u>N</u> ext > Cancel Help | |
| | | |
| 🏄 Start 🛛 🚱 🥭 | 🔣 Add or Remove Pr 🔀 Windows Comp 🥑 Help and Support 🛛 🍓 | 11:17 AM |

11. Click **Yes** on the **Microsoft Certificate Services** dialog box (figure 17) informing you that Active Server Pages must be enabled on IIS if you wish to use the Certificate Services Web enrollment site.

| 🐻 Add or Remove I | Programs | |
|---|---|----------------------|
| Window | ws Components Wizard | |
| Con Change or Remove Programs | nfiguring Components Setup is making the configuration changes you requested. | <u>1.06MB</u> rarely |
| Add <u>N</u> ew | Please wait while Setup configures the components. This may take several minutes, depending on the components selected. | 28/2003 Remove |
| Programs | Microsoft Certificate Services | |
| Add/Removi <u>W</u> indows Components | Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is a potential security risk and must be carefully evaluated. You can enable ASPs later if you choose not to do it now. IIS must be manually reconfigured later to enable this functionality. Do you want to enable Active Server Pages now? Yes No | |
| | Kext > Help | |
| 赶 Start 🛛 🚱 🥭 | 🛛 🔂 Add or Remove Pr 🔀 Windows Comp 🥑 Help and Support 🛛 🥸 🗄 | 11:27 AM |

12. Click Finish on the Completing the Windows Components Wizard page (figure 18).

| 🐔 Add or Remove Programs | | - U × |
|--|--|---------------------------------------|
| Windows Components Wizar | d and a second | |
| Change or Remove Programs Add New Programs | Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard. | ▼ <u>rarely</u> 8/2003 emove |
| Add/Removi Windows Components | To close this wizard, click Finish. | |
| | < <u>B</u> ack. [Finish] Help | |
| 🏄 Start 🛛 🞯 🥭 👘 🔂 Add or Remov | re Pr 🔀 Windows Comp 🕐 Help and Support 🛛 🌯 🗐 | 11:30 AM |

13. Close the Add or Remove Programs window.

Approving Certificate Requests to a Standalone Certificate Authority

The stand-alone CA does not automatically issue a certificate when a certificate request is made. The reason is the standalone CA is not able to confirm the validity of the request. It does not check the information provided by the requestor against a directory, such as the enterprise CA does when validating credentials against the Active Directory.

You should keep this default behavior for your published standalone CA in order to prevent users on the Internet from obtaining certificates without your review. Perform the following steps to approve a certificate request:

1. Click **Start** and point to **Administrative Tools**. Click on the **Certification Authority** link (figure 19).

| <u>^</u> | | Active Directory Domains and Trusts |
|-----------------------------|----------------------|--|
| Administrator | | Active Directory Sites and Services |
| Manage Your Server | 😏 My Computer | Active Directory Users and Computers Certification Authority Cluster Administrator |
| Windows Explorer | Control Panel | Component Services |
| Command Promot | Administrative Tools | Computer Management |
| | Printers and Faxes | 🚭 Data Sources (ODBC) 🍌 Distributed File System |
| | () Help and Support | 🚊 DNS |
| Certification Authority | | Domain Security Policy |
| | 707 <u>R</u> un | Event viewer Internet Information Services (IIS) Manager |
| | | 🍘 Licensing 🥥 Manage Your Server |
| | | Microsoft .NET Framework 1.1 Configuration Microsoft .NET Framework 1.1 Wizards |
| All <u>P</u> rograms 🕨 | - | Network Load Balancing Manager |
| | Log Off 🚺 Shut D | Town Performance |
| Start 🕑 🥭 🛛 🔤 Co | mmand Prompt | 🕼 Remote Desktops |

2. In the Certification Authority console (figure 20), expand the server name and then click on the Pending Certificates node. You see a list of pending certificate requests in the right pane of the console. You can see who requested the certificate by scrolling to the right and looking under the Requester Name column (not shown). Right click on the certificate request in the right pane of the console, point to All Tasks and click Issue. The certificate request is removed from the Pending Requests node.

| 📴 Certification Authority | | | | |
|---|---------------------------|---------------------------------------|---|---|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | |
| ⇔ → 🗈 🖬 🕃 🛱 🔮 | | | | |
| Certification Authority (Local) Cert Revoked Certificates Issued Certificates Pending Requests Failed Requests | Request ID 2 3 4 | Binary RequestBEGIN NEBEGIN NE AI R H | Request Status Code The operation comple The operation comple The operation comple Tasks View Attribute ITasks View Attribute efresh Issue elp Deny | Request Disposition Me Taken Under Submissic Taken Under Submissic Taken Under Submissic ites/Extensions ry Data |
| Contains operations that can be performed | on the object | | | <u>•</u> |
| 🐉 Start 🗍 🚱 🥔 🔰 🔤 Comma | nd Prompt | Certifica | ition Authority | 🍓 🗐 3:19 PM |

3. Click on the **Issued Certificates** node in the left pane of the **Certification Authority** console. The certificate request you approved appears in the right pane of the console. This indicates the certificate request was approved. It does not indicate the machine issuing the request has returned to the Web enrollment site to retrieve the certificate (figure 21).

| 📴 Certification Authority | | | | |
|--|------------|-------------------------|--------------------|-----------------|
| <u>File A</u> ction ⊻iew <u>H</u> elp | | | | |
| ⇔ → 🗈 🖬 🕃 🛱 🔮 | | | | |
| Certification Authority (Local) | Request ID | Requester Name | Binary Certificate | Certificate Ter |
| Cert Revoked Certificates Issued Certificates Pending Requests Failed Requests | 4 | INTERNAL\IUSR_WIN2003DC | BEGIN CERTI | |
| | | | | × |
| 🥂 Start 🛛 🚱 🧾 🔤 Comma | ind Prompt | Certification Authority | p 🐴 | 3:21 PM |

Identify the Location of the CA CRL and Configure the URLs for the Certificate Revocation List and Certificate Trust List

A certificate revocation list (CRL) is a list of certificates deemed invalid by Certificate Authority administrator. Clients and servers can use the CRL to check the validity of the certificate of the computer presenting a certificate. If the certificate is on the CRL, then the connection request can be denied. Making the CRL accessible to all hosts using certificates from the CA is critical in certificate authentication process.

The location of the CRL is included in all certificates issued by the CA. When the VPN client connects to the VPN server, the VPN server can check the CRL to confirm that the VPN client's certificate has not been revoked. The VPN client can also check the CRL to confirm the certificate issued to the VPN server has not been revoked.

You should also publish your Certificate Trust List (CTL). The CTL is a list of trusted Certificate Authorities. All participants in the certificate exchange process must trust the CA's that issued the certificate of the opposite party. If one or both participants fail to trust the other's certificate, then the certificate authentication process fails. Publishing the CTL makes it easy to import a list of trusted CAs into a client's certificate store.

Perform the following steps identify the location of the CA CRL and configure URLs for the CRL and CTL:

1. Click Start, point to Administrative Tools and click Certification Authority (figure 22).

| Real Charles Construction | | 🔤 🕫 Active Directory Domains and Trusts 🛛 🤘 |
|---------------------------|---|--|
| Administrator | | Active Directory Sites and Services |
| Manage Your Server | Image: My Computer Image: Control Panel Image: Control Panel Image: Administrative Tools Image: Administrative Tools Image: Printers and Faxes Image: Printers and Support Image: Printers and Support Image: Search Image: Plane | Active Directory Users and Computers Certification Authority Cluster Administrator Component Services Computer Management Configure Your Server Wizard Data Sources (DDBC) Distributed File System DNS Domain Controller Security Policy Domain Security Policy Event Viewer Internet Information Services (IIS) Manager Licensing Manage Your Server Microsoft .NET Framework 1.1 Configuration Motivesk Load Palancing Manager |
| All <u>P</u> rograms | | Retwork Monitor |
| 🥂 Start 🛛 🚱 🛁 👘 Ce | Log Off 💽 Shut Do | own 🗑 Performance |

2. In the **Certification Authority** console, right click on the server name in the left pane of the console and click on **Properties** (figure 23).

| 📴 Certification Authority | | | | | |
|---|--|--|--|--|--|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | | |
| | 2 🕨 🗖 | | | | |
| Certification Authority (Local) | Name Revoked Certificates Issued Certificates Pending Requests Failed Requests | | | | |
| 🔧 Start 🔯 🦷 🕅 Cartification Authority | | | | | |
| | could read only | Contraction of the second seco | | | |

3. In the server **Properties** dialog box (figure 24), click on the **General** tab. On the **General** tab, click on the **View Certificate** button.

| 📴 Certification Autl 🛛 | ert Properties | |
|--|--|--------------|
| <u>File</u> <u>A</u> ction ⊻iew | Certificate Managers Restrictions Auditing Security | |
| ⇔ ⇒ 🗈 💽 | General Policy Module Exit Module Extensions Storage | |
| Certification Authori Cert Revoked C Issued Cert Pending Re Failed Requ | Certification authority (CA) Name: cert CA certificates: Certificate #0 View Certificate | |
| | | |
| | Cryptographic settings | |
| | USP: Microsoft Strong Uryptographic Provider | |
| | Hash algorithm: SHA-1 | |
| | | |
| | | |
| 🏄 Start 🛛 🚱 🥭 | Certification Authority | 🍓 👜 10:20 АМ |

4. Click the **Details** tab in the **Certificate** dialog box (figure 25). Scroll through the list of fields and find the **CRL Distribution Points** field. In the bottom pane of the **Certificate** dialog box you'll see the HTTP address of the CRL. In this example, the HTTP address is <u>http://win2003dc.internal.net/CertEnroll/cert.crl</u>. Write down the HTTP path. Click **OK**.

| 📴 Certification Autl ce | nt Certificate | ?× | |
|--|---|---------------------------|------------|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew | General Details Certification Path | | |
| | C Show: <all></all> | | |
| Certification Authori | | | |
| Revoked C | Field Value | | |
| Issued Cert | Public key RSA (2048 Bits) | | |
| Eailed Beg | TagKey Usage Digital Signature, Certificate Si | | |
| | Subject Key Identifier 7f 97 56 10 7e 5c 54 1d 58 37 | | |
| | CRL Distribution Points [1]CRL Distribution Point: Distr | | |
| | Basic Constraints Subject Type=CA. Path Lengt | | |
| | Thumbprint algorithm sha1 | - | |
| | [1]CRL Distribution Point Distribution Point Name: Full Name: URL=Idap:///CN=cert,CN=WIN2003DC,CN=CDP,CN=Public 20Key% 20Services,CN=Services,CN=Configuration,DC=internal,DC=net? certificateRevocationList?base?objectClass=cRLDistributionPoint URL=http://win2003dc.internal.net/CertEnroll/cert.crl | % | |
| Btatt | Cartification Authority | siz 3 5 | ■ 10-20 AM |
| June 1 🖉 😂 | | | 10.20 AM |

5. Click the Extensions tab in the server Properties dialog box. Click the down arrow in the Select extension drop down list box and select CRL Distribution Point (CDP). Find the HTTP path for the CDP in the list of location and click on it. Find the entry in the list that begins with HTTP. Select that entry and click the Remove button (figure 26).

| 🗃 Certification Autl C | ert Properties | ? × | _D× |
|-------------------------|---|--|--------------|
| <u>File Action ⊻iew</u> | Certificate Managers Restrictions Auditing General Policy Module Exit Module Extensions | Security Storage | |
| Certification Authori | Select e <u>x</u> tension: | | |
| E-C cert | CRL Distribution Point (CDP) | | |
| Issued Cert | Specify locations from which users can obtain a certificate revoc- (CRL). | ation list | |
| I 🛅 Failed Reqr | C:\WINDDWS\system32\CertSrv\CertEnroll\ <caname><crln Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<serv http://<serverdnsname>/CertEnroll/<caname><crlnamesu file://\\<serverdnsname>\CertEnroll\<caname><crlnames< td=""><td><mark>lameSuffix:</mark> /erShortNai iffix><delta uffix><delt< td=""><td></td></delt<></delta </td></crlnames<></caname></serverdnsname></crlnamesu </caname></serverdnsname></serv </crlnamesuffix></catruncatedname></crln </caname> | <mark>lameSuffix:</mark> /erShortNai iffix> <delta uffix><delt< td=""><td></td></delt<></delta | |
| | | • | |
| | Add E | <u>}</u> emove | |
| | Publish CRLs to this location | | |
| | Include in all CRLs. Specifies where to publish in the Active D when publishing manually. | Directory | |
| | \square Include in CRLs. Clients use this to find Delta CRL locations. | | |
| | Include in the CDP extension of issued certificates | | |
| | Publish Delta CRLs to this location | | |
| | | | |
| 🏄 Start 🛛 🕑 🥭 | Ertification Authority | | 🌯 🔂 10:22 AM |

6. Click the Yes button in the Confirm removal dialog box (figure 27).

| 📴 Certification Autl C | ert Properties | <u> </u> |
|-------------------------|--|---|
| <u>Eile Action ⊻iew</u> | Certificate Managers Restrictions Auditing General Policy Module Exit Module Extensions | Security Storage |
| Certification Authori | Select extension: | |
| E Concert Revoked C | CRL Distribution Point (CDP) | • |
| Issued Cert | Specify locations from which users can obtain a certificate revoca (CRL). | ation list |
| Falled Requ | C:\WINDOWS\system32\CertSrv\CertEnroll\ <caname><crln Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<servi http://cServerONSName>/CertEnroll/CEaName><cblnamesu< td=""><td>ameSuffix: erShortNai ffix:<dette< td=""></dette<></td></cblnamesu<></servi </crlnamesuffix></catruncatedname></crln </caname> | ameSuffix: erShortNai ffix: <dette< td=""></dette<> |
| Confirm remov | file://// <serverdnsname>/CertEnroll/<daname><crlnamesu< td=""><td>uffix><delt< td=""></delt<></td></crlnamesu<></daname></serverdnsname> | uffix> <delt< td=""></delt<> |
| | rou want to remove the selected location? |) |
| | | emove |
| | Inglude in all CHLs. Specifies where to publish in the Active D when publishing manually. | rirectory |
| | ☑ Include in CRLs. Clients use this to find Delta CRL locations. | |
| | Include in the CDP extension of issued certificates | |
| | Publish Delta CRLs to this location | |
| | · · · · · · · · · · · · · · · · · · · | |
| 赶 Start 🛛 📴 🥭 | Certification Authority | 🌯 👜 10:24 AM |

7. Click the **Add** button on the **Extensions** tab (figure 28).

| 🛅 Certification Autl | cert Properties | ?× | _D× |
|---|---|---------------------------------------|--------------|
| <u>F</u> ile <u>A</u> ction ⊻iew | Certificate Managers Restrictions Auditing | Security | |
| ⇔ ⇒ 🗈 🖬 | General Policy Module Exit Module Extensions | Storage | |
| Certification Authori | Select extension: | | |
| E Cert | CRL Distribution Point (CDP) | • | |
| Issued Cert Pending R∉ | Specify locations from which users can obtain a certificate revoca (CRL). | ation list | |
| a second s | C:\WINDOWS\system32\CertSrv\CertEnroll\ <caname><crln Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<serv< p=""></serv<></crlnamesuffix></catruncatedname></crln </caname> | ameSuffix: erShortNat | |
| | file://\\ <serverdnsname>\CertEnroll\<caname><crlnames< td=""><td>uffix><delt< td=""><td></td></delt<></td></crlnames<></caname></serverdnsname> | uffix> <delt< td=""><td></td></delt<> | |
| | | | |
| | | | |
| | | <u>{emove</u> | |
| | I Publish CRLs to this location | | |
| | Include in all CRLs. Specifies where to publish in the Active D when publishing manually. | Directory | |
| | ☑ Include in CRLs. Clients use this to find Delta CRL locations. | | |
| | Include in the CDP extension of issued certificates | | |
| | Publish Delta CRLs to this location | | |
| | | | |
| <u></u> | | īL | 1 |
| 🏄 Start 🛛 🕑 🥭 | Certification Authority | | 🌯 🔂 10:27 AM |

8. In the **Location** text box, type in the HTTP to the CRL. This is the path we wrote down in step 4 (figure 29). Click **OK**.

| 📴 Certification Aut | cert Properties | ?× × |
|--|--|--------------|
| <u>File Action ⊻iew</u> | Add Location | ? × |
| ← → È II Certification Authori Cert Revoked C Issued Cert Pending Re Failed Requ | A location can be any valid URL or path. Enter an HTTP, LDAP, file addre or enter a UNC or local path. To insert a variable into the URL or path, sele the variable below and click Insert. Location: http://win2003dc.internal.net/CertEnroll/cert.crl Variable: kcanade Variable: kcanade Description of selected variable: Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crl< td=""><td>Na</td></crl<></caname></serverdnsname> | Na |
| | Implicate in the Contextension on issued certificates Implicate in the Contextension on issued certificates Implication | |
| 🛃 Start 🛛 🕑 🍠 | Ertification Authority | 🍪 😥 10:28 AM |

9. Put a checkmark in the Include in CRLs. Clients use this to find Delta CRL locations and Include in the CDP extension of issued certificates checkboxes (figure 30). Click Apply.

| 📴 Certification Autl | cert Properties | <u>?×</u> × |
|--|---|--|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew | Certificate Managers Restrictions Auditing Sec | unity |
| ⇐ ⇒ 🔁 🖬 | General Policy Module Exit Module Extensions S | torage |
| Certification Authori | Select e <u>x</u> tension: | |
| Bevoked C | CRL Distribution Point (CDP) | |
| Issued Cert | Specify locations from which users can obtain a certificate revocation (CRL). | ı list |
| I 🔁 Failed Req | C:\WINDOWS\system32\CertSrv\CertEnroll\ <caname><crlname Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<serversh file://\\<serverdnsname>\CertEnroll\<caname><crlnamesuffix http://wip2003dc.interpal.net/CertEproll/cert.crl</crlnamesuffix </caname></serverdnsname></serversh </crlnamesuffix></catruncatedname></crlname </caname> | sSuffix: nortNai ≻ <delt< td=""></delt<> |
| | | |
| | Add <u>R</u> emo | ove |
| | Eublish CRLs to this location | |
| | Include in all CRLs. Specifies where to publish in the Active Direc when publishing manually. | tory |
| | ✓ Include in CRLs. Clients use this to find Delta CRL locations. | |
| | Include in the CDP extension of issued certificates | |
| | Publish Delta CRLs to this location | |
| | | |
| 🏄 Start 🛛 🚱 🥭 | Certification Authority | 🌯 🗐 10:29 AM |

10. Click Yes in the Certification Authority dialog box (figure 31).

| Entification Aut | cert Properties | |
|----------------------|---|---|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| | Select automican | |
| Certification Author | CPL Distribution Boist (CDD) | |
| E C cert | | |
| | Specify locations from which users can obtain a certificate revocation list (CRL). | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix: Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<servershortnar< td=""><td></td></servershortnar<></crlnamesuffix></catruncatedname></crlnamesuffix: </caname> | |
| | Certification Authority | |
| | | |
| | You must restart Certificate Services for the changes to take effect. Do you want to restart the service now? | |
| | | |
| | <u>Yes</u> <u>N</u> o | |
| | I MOUDE M AIL UNLY ODEGILES WHELE TO DUDING IN THE POLYCE DIRECTOR | |
| | when publishing manually. | |
| | Include in CRLs. Clients use this to find Delta CRL locations. | |
| | Include in the CDP extension of issued certificates | |
| | Publish Delta CRLs to this location | |
| | | |
| l | | - · · · · · · · · · · · · · · · · · · · |
| | OK Cancel Apply | |
| 💋 Start 🛛 🕑 🍠 | Ertification Authority | 🍓 🛃 10:30 AM |

11. The Certificate Server service restarts (figure 32).

| Ertification Aut | eit Properties | |
|----------------------|--|--------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| | Select extension: | |
| Certification Author | CRL Distribution Point (CDP) | |
| Revoked (| Specify locations from which users can obtain a certificate revocation list (CRL). | |
| Failed Rec | C:\WINDDWS\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix: Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<servershortnar file://\\<serverdnsname>\CertEnroll\<caname><crlnamesuffix><delt< td=""><td></td></delt<></crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname></crlnamesuffix: </caname> | |
| | | |
| | Starting Certificate Services | |
| | | |
| | Include in all CHLs. Specifies where to publish in the Active Directory when publishing manually. | |
| | ☑ Include in CRLs. Clients use this to find Delta CRL locations. | |
| | ✓ Include in the CDP extension of issued certificates | |
| | Publish Delta CRLs to this location | |
| | | |
| | | |
| 🏄 Start 🛛 🔂 🥭 | Entification Authority | 🍓 👜 10:31 АМ |

12. Click the down arrow in the **Select extension** drop down list box and select the **Authority Information Access (AIA)** option. Select the location that begins with **http://** from the list of locations and click the **Remove** button (figure 33).

| Entification Aut | ceit Properties | |
|----------------------|--|--------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| Certification Author | Select extension: | |
| E Cert | Authority Information Access (AIA) | |
| Revoked (| Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>_CN=AIA_CN=Public Key Services_CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce< td=""><td></td></ce<></caname></serverdnsname></serverdnsname></catruncatedname></canar </serverdnsname> | |
| | file://\\ <serverdnsname>\CertEnroll\<serverdnsname>_<caname><c< td=""><td></td></c<></caname></serverdnsname></serverdnsname> | |
| | | |
| | A <u>d</u> d <u>R</u> emove | |
| | ✓ Include in the AIA extension of issued certificates ✓ Include in the online certificate status protocol (OCSP) extension | |
| | | |
| | OK Cancel Acriv | |
| 🏄 Start 🛛 🕑 🥭 | Certification Authority | 🌯 👜 10:32 AM |

13. Click Yes in the Confirm removal dialog box (figure 34).

| E Certification Aut | cerc Properties | _ × |
|-------------------------|--|------------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| Certification Author | Select extension: | |
| E Centineation Addition | Authority Information Access (AIA) | |
| Revoked (| Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN=S</catruncatedname></canar </serverdnsname> | |
| | file://\\ Confirm removal | |
| | | |
| | Are you sure you want to remove the selected location? | |
| | Yes <u>N</u> o | |
| | | |
| | | |
| | | |
| | Include in the AIA extension of issued certificates | |
| | Include in the online certificate status protocol (OCSP) extension | |
| | | |
| | OK Cancel Apply | |
| 🏄 Start 🛛 🕑 🥭 | Certification Authority | 🌯 👜 10:33 AM |

14. Click the Add button on the Extensions tab (figure 35).

| Certification Aut | en Properties 📰 🔼 | |
|-------------------------------------|--|--------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| Certification Author | Select extension: | |
| E Cochinedatori idane | Authority Information Access (AIA) | |
| Revoked (Ssued Cer Pending R | Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar< td=""><td></td></canar<></serverdnsname> | |
| | file://\\ <serverdnsname>\CertEnroll\<serverdnsname>_<caname><c< td=""><td></td></c<></caname></serverdnsname></serverdnsname> | |
| | | |
| | | |
| | A <u>d</u> d | |
| | | |
| | | |
| | ✓ Include in the AIA extension of issued certificates | |
| | Include in the online certificate status protocol (OCSP) extension | |
| | | |
| | | |
| 🏄 Start 🛛 🚱 🥭 | UK Cancel Apply | 🍓 👜 10:33 AM |

 In the Add Location dialog box, type the path to the Certificate Trust List in the Location text box. In this example, the path to the CTL is <u>http://win2003dc.tacteam.net/</u> <u>WIN2003DC.internal.net_cert.crt</u>. Click OK (figure 36).

| Entitication Aut | cert Properties | |
|---|---|--------------|
| Certification Aut | Add Location 🔗 🗙 | |
| File Action ⊻iew ← → È II Certification Author ← Certification Author ← C | A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert. Location: http://win2003DC.internal.net/WIN2003DC.internal.net_cert.ort Variable: CaName> Insert Description of selected variable: Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""><td></td></crlna<></caname></serverdnsname> | |
| | | |
| | | |
| | Cancel | |
| | | 1 |
| | Include in the online certificate status protocol (UUSP) extension | |
| ļ | | |
| | OK Cancel Apply | |
| 🛃 Start 🛛 🚱 🥭 | Certification Authority | 🌯 📵 10:57 AM |

16. Place checkmarks in the Include in the AIA extension of issued certificates and Include in the online certificate status protocol (OCSP) extension checkboxes. Click Apply (figure 37).

| Certification Au | cert Properties | |
|------------------------|--|--------------|
| Eile Action ⊻iew | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| Castific stices Avalue | Select extension: | |
| E-Co cert | Authority Information Access (AIA) | |
| Revoked | Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>_CN=AIA,CN=Public Key Services,CN=S</catruncatedname></canar </serverdnsname> | |
| | file://\\ <serverdnsname>\CertEnroll\<serverdnsname>_<caname><c http://win2003DC.internal.net/WIN2003DC.internal.net_cert.crt</c </caname></serverdnsname></serverdnsname> | |
| | x x | |
| | A <u>d</u> d <u>R</u> emove | |
| | 🗖 laskada in the AIA extension of issued antification | |
| | | |
| | Implement of the online certificate status protocol (ULSP) extension | |
| - | | |
| 赶 Start 🛛 🕑 🥭 | Certification Authority | 🌯 👜 10:58 AM |

17. Click Yes in the Certification Authority dialog box (figure 38).

| Certification Aut | cerc Properties | |
|-------------------|--|--------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| | Select extension: | |
| | Authority Information Access (AIA) | |
| Revoked (| Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>_CN=AIA,CN=Public Key Services,CN=S</catruncatedname></canar </serverdnsname> | 4% |
| | Certification Authority | |
| | You must restart Certificate Services for the changes to take effect | |
| | Do you want to restart the service now? | |
| | <u>Y</u> es <u>N</u> o | |
| | | |
| | | |
| | Include in the AIA outensien of issued partitiontee | |
| | Include in the antine partitieste status protocol (OCSP) eutonoion | |
| | I Molude in the gnine certificate status protocol (oCSP) extension | |
| l | | |
| | OK Cancel Apply | |
| 💋 Start 🛛 🚱 🍠 | Certification Authority | 🅙 😥 10:59 AM |

18. Click **OK** on the server **Properties** dialog box (figure 39).

| Ertification Aut | ett Properties | |
|---------------------|--|--------------|
| File Action View | Certificate Managers Restrictions Auditing Security | |
| | General Policy Module Exit Module Extensions Storage | |
| | Select extension: | |
| Ertification Author | Authority Information Access (AIA) | |
| Revoked (| Specify locations from which users can obtain the certificate for this CA. | |
| Failed Rec | C:\WINDOWS\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN=S file://\\<serverdnsname>\CertEnroll\<serverdnsname> <caname><c< td=""><td></td></c<></caname></serverdnsname></serverdnsname></catruncatedname></canar </serverdnsname> | |
| | http://win2003DC.internal.net/WIN2003DC.internal.net_cert.crt | |
| | | |
| | A <u>d</u> d <u>R</u> emove | |
| | | |
| | | |
| | Include in the AIA extension of issued certificates | |
| | Include in the online certificate status protocol (OCSP) extension | |
| | | |
| | OK Cancel Apply | |
| 🛃 Start 🛛 🚱 🥭 | Certification Authority | 🌯 👜 11:00 AM |

Create a DNS Entry in the Public DNS for the Published CA

There must be a public DNS entry for the Fully Qualified Domain Name listed in the CRL. The external network client must be able to resolve the FQDN found in the CRL to the IP address on external interface address on the ISA firewall/VPN server that is being used for the Incoming Web Requests listener.

For example, if the public address used by the Incoming Web Requests listener is **131.107.0.1** and the FQDN in the CRL is **cert.internal.net**, then you must create a Host (A) resource record in the public DNS that resolves **cert.internal.net** to 131.107.0.1.

If your ISP hosts your public DNS records, you can ask your ISP to make the change or if your ISP allows you to manipulate your own DNS records, you can use their administrative interface to make the changes. If you publish your own DNS servers, you can add the record on your own published DNS servers.

Note that you can only provide a single HTTP location that users can use to obtain a certificate. You cannot provide an internal network FQDN location and a separate external network FQDN location. While you can create multiple HTTP locations, only the location at the top of the list will be used if it is available. Alternate locations are queried only when the those higher on the list are not available. You should create a split DNS infrastructure to support internal external network clients name resolution for the CRL locations.

Configure the Incoming Web Requests Listener

The Incoming Web Requests listener accepts requests for the published Web server. The listener accepts the request from the external client and sends the request to the Web Proxy service for evaluation. If the request matches the settings in a Web Publishing Rule, the request is forwarded to the published server. If there is no matching Web Publishing Rule, the request is dropped.

Perform the following steps to configure the Incoming Web Requests listener on the ISA firewall:

1. Open the **ISA Management** console, expand the **Servers and Arrays** node and then expand your server name. Right click on your server name and click the **Properties** command (figure 40).

Figure 40

| ISA Management | | | | | | |
|---|---------------------|-------------|---------------|----------------|--|--|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | | | |
| ⇔ → 🗈 🖪 🖗 😫 | | | | | | |
| Internet Security and Acceleration Server Servers and Arrays Servers and Arrays Monitorin Compute Back Up Back Up Back Up Bestore Promote Promote Promote Properties Monitorin Extensior Help H.323 Gatekeepers | Array WIN2003ISA | Description | Type Stand | Mode Integi | | |
| Opens property sheet for the current selection. | | J | | | | |
| 🛃 Start 🛛 🚱 🥥 👘 ISA Management 🌇 🍓 👜 11:41 AM | | | | | | |

2. In the server **Properties** dialog box, click the **Incoming Web Requests** tab (figure 41). On the **Incoming Requests** tab, select the **Configure listeners individually per IP address** option, then click the **Add** button to configure the listener.

| 👖 ISA Managemen 🗎 | #IN2003ISA Properties | <u>?×</u> |
|---|--|---------------------------|
| <u>File</u> <u>A</u> ction <u>V</u> iew | General Outgoing Web Requests | County |
| Internet Security ar Servers and Ari Servers and Ari WIN2003IS | Identification C Use the same listener configuration for all IP addresses Image: Configure listeners individually per IP addresses | Type Mode Stand Integr |
| Compu ⊕ | Server IP Address Display N Authentic Server (Add <u>Berrove Edit.</u> ICP port: 80 CCL port: 443 | |
| H.323 Gatekee | Connections Connection settings: Ask unauthenticated users for identification OK Cancel | іе] |
| 🏄 Start 🛛 🚱 🥭 | ISA Management | 🌯 🗊 11:42 AM |

 On the Add/Edit Listeners dialog box, use the drop-down list boxes to select the Server you are working on, the IP address on the external interface you want the listener to listen on, and a Display Name that describes the listener. You will not use authentication at the listener when publishing the Web enrollment site, so you do not need to change the authentication settings (figure 42). Click OK.

Figure 42 (fig303)

| ISA Managemen | WIN2003ISA Properties | | ?× | -D× |
|---|--|----------------------------------|-----|---------------------------|
| <u>F</u> ile <u>A</u> ction ⊻iew | Add/Edit Listeners | | ?×) | |
| | Ser <u>v</u> er: | WIN2003ISA | i l | |
| Internet Security and Environment Security and Environment Security and Arr | I <u>P</u> Address: | 172.31.0.2 | | Type Mode Stand Integr |
| E ∰ Monitor | Displ <u>a</u> y Name: | External | | |
| Compu ⊡ ∰ Access | Use a server certificate | e to authenticate to web clients | | |
| ⊡ Bandw ⊡ Bandw ⊡ ∰ Cache | Authentication | in: | | |
| Extensi | | Select domain | n | |
| ⊕ 🛺 Networ | Digest with this dom | ain: | | |
| 🗄 둸 H.323 Gatekee | | Select domain | ñ | |
| | ✓ Integrated ☐ Client certificate (see | ure channel only) | | |
| | | OK Cancel | | |
| 🏄 Start 🛛 🚱 🥭 | ISA Manageme | nt | | 🌯 💼 11:43 AM |

4. Click **Apply** on the server **Properties** dialog box (figure 43)

| ISA Managemen | WIN2003ISA Properties | |
|--|---|---------------------------|
| Eile Action ⊻iew ← → È II Internet Security a ⊖ ∰ Servers and A ⊖ ∰ WIN2003I | General Outgoing Web Requests Incoming Web Requests Auto Discovery Performance Security Identification Identification Identification Identification Image: Use the same listener configuration for all IP addresses Image: Outgoing Web Requests Image: Outgoing Web Requests | Type Mode Stand Integr |
| E S Monte Comp E S Acces E E Publis E Bandy E Acces Policy E Monte E Monte | Server IP Address Display N Authenti Server C WIN2003ISA 172.31.0.2 External Integrated Add Remove Edit | |
| ⊕- 🦃 Extens ⊕- 🛺 Netwo E Client ⊕- 🔂 H.323 Gateke | get port: 443 Enable SSL listeners Connections | |
| 🍂 Start | OK Cancel Apply | ▶ ▲ 🗊 11:44 AM |

5. In the **ISA Server Warning** dialog box, select the **Save the changes and restart the service(s)** option. This will cause the **Web proxy** service to restart and disconnect any users that are currently connected to the Web Proxy service. The users will automatically reconnect when the Web Proxy service restarts (figure 44).



6. Click OK in the server Properties dialog box (figure 45).

| ISA Managemer | WIN2003ISA Properties | |
|--|--|---------------------------|
| Eile Action ⊻iew ← → ▲ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ | General Outgoing Web Requests Incoming Web Requests Auto Discovery Performance Security Identification Identification Identification Identification Issue the same listener configuration for all IP addresses Configure listeners individually per IP address | Type Mode Stand Integi |
| E Sandy Comp E S Acces Publis E Bandy E Sandy E Sa | Server IP Address Display N Authenti Server C WIN2003ISA 172.31.0.2 External Integrated | |
| Erene Erene Extens | ICP port: 80 SSL port: 443 Connections Connection settings: Ask unauthenticated users for identification | |
| 🍂 Start | OK Cancel Apply | ▶ ▲ 🗊 11:45 AM |

Create the Destination Set and HOSTS File Entry to Support the Web Publishing Rule

The Web Publishing Rule uses a Destination Set to match against the Host Header in the incoming request. For example, when the external user sends a request for <u>http://www.internal.net</u>, then the host header will contain the entry for <u>www.internal.net</u>. If the Web Publishing Rule contains a Destination Set that instructs it to listen for incoming connections to <u>www.internal.net</u>, then the Rule will further evaluate the request.

Perform the following steps to create the Destination Set you will use in the Web Publishing Rule:

1. In the **ISA Management** console, expand the **Servers and Arrays** node and then expand the server node. Expand the **Policy Elements** node and right click on **Destination Sets**. Point to **New** and click on **Set** (figure 46).

| ISA Management | | | | |
|--|-------|-------------|---------------|-----------------------|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | |
| | | | | |
| Internet Security and Acceleration Server Servers and Arrays WIN2003ISA Monitoring Computer Computer Access Policy Publishing Bandwidth Rules Policy Elements Schedules Bandwidth Priorities Destination Sets Protocol Definiti Content Groups Dial-up Entries Help Cache Configuration Extensions Network Configuration | Array | Description | Type Stand | <u>Mode</u> Integi |
| Image: Client Configuration Image: Image: Client | | | | × |
| Creates a new object in this container. | | | | |
| 🏄 Start 🛛 🚱 🥭 👘 ISA Managemer | nt | 3 | 2:0 | 8 PM |

In the New Destination Set dialog box, type in a name for the Destination Set. In this example we'll name the Destination Set Certificate Server. You can type in an optional description for the Destination Set. In this example we'll describe the Destination Set as Destination Set for Certificate Server Web Publishing Rule. Click the Add button in the New Destination Set dialog box (figure 47).

| ISA Management | | | |
|---|-----------------------------|--|--------------|
| <u>File</u> <u>A</u> ction <u>V</u> iew | Hain New Destination Set | ? | X |
| | | Castificante Casular | |
| Internet Security and | <u>N</u> ame: | | Type Mode |
| Servers and Array | <u>D</u> escription | Destination Set for Certificate Server | Stand Integr |
| WIN2003ISA | (optional): | Web Publishing Rule | |
| | | 2 | |
| E Access F | Include these destinatio | | |
| 🕀 🔄 Publishin | melade mese desandad | 13. | |
| - 💭 Bandwidt | Name/IP Range | Path | |
| E 🍄 Policy Ele | | | |
| Band | | | |
| | | | |
| - Client | | | |
| Proto | | | |
| Conte | | | |
| Dial-u | | | |
| E Cache Lo | Add | Edit Remove | |
| | | | |
| Hetwork | | OK Cancel | |
| 📃 🔄 🛃 Client Co | | | |
| 🗄 🔂 H.323 Gatekeepe | ns 🔟 🗋 | | |
| | | | |
| 🏄 Start 🛛 📴 🥭 | ISA Manageme | int | 🍓 👜 2:09 PM |

3. In the Add/Edit dialog box, select the Destination option and type in the FQDN that the external user will use to access the certificate server Web enrollment site. In this example the external user will use the name cert.internal.net. Three paths are required: /CertEnroll*, /CertControl* and /CertSrv*. Type /CertEnroll* in the Path text box and click OK (figure 48).

| ISA Management | | | | |
|---|---|---|--------------------------|---------------------------|
| <u>File</u> <u>A</u> ction <u>V</u> iew Hal | n | | | |
| ⇔ → € 💽 🤅 | Add/Edit Destination | | <u>?</u> × | |
| Internet Security and Servers and Array WIN2003ISA Monitorin Computer Computer Computer Computer Bandwidt Policy Ele | Destination: To include all control IP addresses: Erom: To (optional) | cert.internal.net | <u>B</u> rowse | Type Mode Stand Integr |
| Sche Band Desti Clieni Proto Conte Dial-u | To include a specific dir below. To include all the To select a spec <u>P</u> ath: | ectory in the destination set, t files, use this format: /dir/*. ific file, use this format: /dir/fil | type the path lename. | |
| ⊡- 😭 Cache Co ⊡- 📆 Monitorin | /CertEnroll* | | | |
| Extensior ⊕-∭ Network ∰ Client Co | | ОК | Cancel | |
| 😥 💀 H.323 Gatekeepers | MIN | | | • |
| | | | | |
| 🏄 Start 🛛 🚱 进 🗍 | ISA Management | | | 🍓 🗐 2:10 РМ |

4. Click the Add button in the New Destination Set dialog box (figure 49).

| ISA Management | | | <u>-0×</u> |
|--|-----------------------------|--|--------------|
| <u>F</u> ile <u>A</u> ction <u>V</u> iew | Hain Now Destination Cat | | 2 2 |
| ⇐ ⇒ 🗈 🖪 🔮 | New Desunation Set | | |
| Internet Security and | <u>N</u> ame: | Certificate Server | Type Mode |
| 📴 🖏 Servers and Array | Description I | Destination Set for Certificate Server | Stand Integi |
| 🖻 🚮 WIN2003ISA | (optional): | Web Publishing Rule | |
| | | | |
| E S Access F | Include these destination | 18. | |
| 🗄 🔄 Publishin | | | |
| Bandwidt | Name/IP Range | Path | |
| Sche | cert.internal.net | /CertEnroll* | |
| 🛅 Band | | | |
| | | | |
| | | | |
| - Conte | | | |
| Dial-u | | | |
| E Cache Co | Add | Edit Bemove | |
| Extension | <u></u> | | |
| E Metwork | | OK Car | ncel |
| Elient Co | | | |
| H:323 Gatekeepe | ns 🛄 🗋 | | |
| | | j | |
| 📶 Start 🛛 🕑 🥭 | ISA Manageme | nt | 🥙 🛃 2:11 PM |

5. Select the **Destination** option and type in the FQDN used by the external user to access the Web enrollment site. Type /**CertControl*** in the **Path** text box (figure 50). Click **OK**.

| ISA Management | | | | -D× |
|---|--|---|------------------------|---------------------------|
| <u>File Action View Hal</u> | ~ | | | |
| ← → 🗈 🖬 🛃 | Add/Edit Destination | | <u>?×</u> | |
| Internet Security and Servers and Array WIN2003ISA Monitorin Computer Access F Publishiny Bandwidt Policy Ele | Destination: To include all con To include all con IP addresses: Erom: <u>I</u> o (optional) | cert.internal.net | Browse | Type Mode Stand Integr |
| Sche Band Desti Clieni Clieni Proto Conte Dial-u | To include a specific dir below. To include all the To select a spec <u>P</u> ath: | ectory in the destination set, t files, use this format: /dir/*. ific file, use this format: /dir/fil | ype the path ename. | |
| E Bache Co E Bache Co E Bache Co | /CertControl* | | | |
| ⊕ | | OK | Cancel | |
| H.323 Gatekeepers | M | | | × |
| | | | | |
| 🏄 Start 🛛 🚱 🥭 👘 | ISA Management | | | 🍓 🗐 2:12 PM |

6. Click the Add button in the New Destination Set dialog box (figure 51).

| ISA Management | | | _ _ × |
|--|---|---|---------------------------|
| <u>File Action View</u> | Help New Destination Set | ? > | <u> </u> |
| Internet Security and Servers and Array WIN2003ISA WIN2003ISA WIN2003ISA | Name: C Description D (optional): W | ertificate Server estination Set for Certificate Server /eb Publishing Rule | Type Mode Stand Integr |
| E Computer ⊡ S Access F ⊡ S Publishin | Include these destinations: | ** | |
| Bandwidt | Name/IP Range cert.internal.net cert.internal.net | Path /CertControl [*] /CertEnroll [*] | |
| | Add | Edit <u>R</u> emove | |
| | | | |
| 🛃 Start 🛛 🚱 🥭 | ISA Management | t internet in the second se | 🌯 🗐 2:12 PM |

7. Select the **Destination** option and type in the FQDN used by the external user to access the Web enrollment site. Type /**CertSrv*** in the **Path** text box (figure 52). Click **OK**.

| 19 ISA Management | | | | -D× |
|---|---|---|---------------------------|---------------------------|
| | • | | - In | |
| ⇔ → € 💽 🤅 | Add/Edit Destination | | <u>? ×</u> | |
| Internet Security and Servers and Array WIN2003ISA T | Destination: To include all co IP addresses: Erom: To (optional) | cert.internal.net omputers in a domain, type *.d | Browse | Type Mode Stand Integi |
| Policy Ele Sche Band Desti Clieni Proto Conte Dial-u | To include a specific di below. To include all th To select a spec <u>P</u> ath: | I irectory in the destination set, e files, use this format: /dir/*. cific file, use this format: /dir/f | type the path ilename. | |
| ⊡ ∰ Cache Co ⊡ ∰ Monitorin | /CertSrv* | | | |
| Extension ⊡ ∰ Network | | (OK) | Cancel | |
| H.323 Gatekeepers | | | | Þ |
| | | ** | | |
| 🏄 Start 🛛 🕑 🥭 👘 | 🗓 ISA Managemen | t d | | 🍓 🗐 2:13 РМ |

8. Click **OK** in the **New Destination Set** dialog box to save the new Destination Set (figure 53).

| ISA Management | | | -D× |
|---|---|---|--------------|
| <u>F</u> ile <u>A</u> ction ⊻iew | Haln New Destination Set | 2 | |
| ← → È II : | New Destination Set | Certificate Server | Type Mode |
| Servers and Array | Description (optional): | Destination Set for Certificate Server Web Publishing Rule | Stand Integi |
| ⊡ 🛒 Access F ⊕ 🔄 Publishin | Include these destinatio | ns: | |
| - 🦲 Bandwidt | Name/IP Range | Path | |
| E- | cert.internal.net cert.internal.net cert.internal.net | /CertSrv* /CertControl* /CertEnroll* | |
| Dial-u ⊡ ்∰ Cache Co ⊡ ∰ Monitorin ⊡ ∯ Extensior ⊡ ∰ Network ⊡ ∰ Client Co | , <u>[</u> <u>A</u> dd | <u>Edit</u> <u>B</u> emove OK Cancel | |
| 庄 🔂 H.323 Gatekeepe | ns 🔟 🗋 | | |
| 🏄 Start 🛛 🕑 🥭 | ISA Manageme | ent | 🌯 👜 2:13 РМ |

The next step is to create the HOSTS file entry so that you can use the same fully qualified domain name that the external user uses to access the site in the redirect:

1. Open the **Windows Explorer** and navigate to the **SystemRoot\system32\drivers\etc** folder (figure 54). Right click on the **Hosts** file and click on the **Open** command.

| 🔄 C:\WINDOWS\system32\drivers\ | Vetc | | | | _ 8 × |
|--|---|---|---|------------|-----------|
| <u>File Edit View Favorites T</u> ools | <u>H</u> elp | | | | - |
| 🔇 Back 🔹 🕥 🗟 🏂 🔎 Search 🚺 | 🏷 Folders | » 🗙 🍤 🛽 | H . | | |
| Address 🛅 C:\WINDOWS\system32\dr | ivers\etc | | | | 🔁 Go |
| Folders × | Name 🔻 | Size | Date Modified | Attributes | |
| | services protocol renetworks ren | 7 KB 1 KB 1 KB 4 KB 1 KB 1 KB n I To → I To → I To → I To → I To → | 3/25/2003 7:00 AM 3/25/2003 7:00 AM 3/25/2003 7:00 AM 3/25/2003 7:00 AM 3/25/2003 7:00 AM | | |
| disdn | P <u>r</u> op | erties | | | |
| Open Image: Start Image: S | inagement | C:\WINE |)0\\$\syste | 8 |) 2:16 PM |

2. In the **Open With** dialog box, click on the **Notepad** entry and click **OK** (figure 55).

| 🔄 C: \WINDOWS \sysl | Open With | ? × | _ 8 × |
|-----------------------------|---|-----|-------------|
| Eile Edit View Fa | Choose the program you want to use to open this file: File: hosts | | 🥂 🔁 Go |
| Folders | Internet Explorer Notepad Paint Windows Media Player Windows Picture and Fax Viewer WordPad MordPad Always use the selected program to open this kind of file Browse | | ributes |
| Type: File Date Modified: 3 | OK Cancel | | y Computer |
| 🏄 Start 🛛 🚱 🥭 | ISA Management C:\WINDOWS\syste | | 🌯 🔂 2:17 PM |

Type in an entry for the certificate server on the internal network. Use the same FQDN that the
external users use to access the published server, but use the *internal* IP address of the server
for the name mapping. In this example, the external users type <u>http://cert.internal.net</u> to reach the
published Web enrollment site (figure 56).

| () | :\WINDO | ₩S\system32\ | drivers\etc | _ 8 × |
|------------|--|--|--|---------|
| Eib | 📕 hosts - | Notepad | | - |
| G | <u>F</u> ile <u>E</u> dit | F <u>o</u> rmat ⊻iew | Help | |
| Ad(Fol | <u>N</u> ew Open Save Save <u>A</u> s | Ctrl+N Ctrl+O Ctrl+S | 93-1999 Microsoft Corp. HOSTS file used by Microsoft TCP/IP for Windows ns the mappings of IP addresses to host names. E kept on an individual line. The IP address shoul | Di Go |
| | Page Se <u>P</u> rint | etyp Ctrl+P | e first column followed by the corresponding host Ind the host name should be separated by at least | |
| | E <u>x</u> it # lines # # For e # # | or follow xample: 102.54.94. 38.25.63.1 | omments (such as these) may be inserted on indivi ing the machine name denoted by a '#' symbol. 97 rhino.acme.com # source server 10 x.acme.com # x client host | |
| | 127.0.0 10.0.0. | .1] 2 c | ocalhost ert.internal.net | |
| • | | | | : |
| Туре | : File Date M | lodified: 3/25/200 | 03 7:00 AM Size: 734 bytes 734 bytes 🪽 My Computer | |
| | Start 🛛 🚱 | 🥭 🗍 👖 | ISA Management 🛛 🙆 C:\WINDOWS\sy 🕞 hosts - Notepad 🛛 🍓 🗐 | 2:18 PM |

Create the Web Publishing Rule

All the components are now in place to create the Web Publishing Rule. Perform the following steps to create the Web Publishing Rule to publish the Certificate Server Web enrollment site:

1. In the **ISA Management** console, expand the **Servers and Array** node and then expand the server node. Expand the **Publishing** node and right click on the **Web Publishing Rules** node. Point to **New** and click on **Rule** (figure 57).

| ISA Management | | | | |
|--|----------------------------|----------------------|-------|--------|
| <u>E</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp | | | | |
| | | | | |
| Internet Security and Acceleration Server | Array | Description | Туре | Mode |
| Ervers and Arrays | J WIN2003ISA | | Stand | Integi |
| Monitoring | | | | |
| Computer ⊡Si Access Policy | | | | |
| | | | | |
| Server Publishing Rules | w ▶ <u>R</u> ule | | | |
| Bandwidth Rules Re | resh <u>P</u> ublish Outlo | ok Web Access Server | | |
| Elements Elements Elements Elements Elements Elements Elements Elements Elements | lp | | | |
| Monitoring Configuration | | | | |
| | | | | |
| Client Configuration | | | | |
| H-MY H.323 Galekeepers | | | | |
| | | | | |
| | | | | |
| Creates a new object in this container | | | | |
| | • | | | |
| 🗾 Start 🗍 🕼 🥮 👘 🗍 🎹 ISA Manage | ment | | 122 | I PM |

2. Type a name for the rule in the **Web publishing rule name** text box on the **Welcome to the New Web Publishing Rule Wizard** page (figure 58). Click **Next**.

| ISA Management | | |
|--|---|---------------------|
| Eile Action New Web Publishing Rule Wi | zard | × |
| → € → Serve → ⊕ → ⊕< | Welcome to the New Web Publishing Rule Wizard This wizard helps you create a new Web publishing rule. Web publishing rules map incoming requests to the appropriate Web servers. Note: Be sure to create new policy elements required by the rule before you use this wizard. Web publishing rule name: Certificate Server To continue, click Next. | e Mode nd Integi |
| | <back next=""> Cancel <</back> | |
| 🏄 Start 🛛 🞯 🥭 👘 🕅 🏙 ISA Manager | nent | 🍐 👜 2:22 PM |

3. On the **Destination Sets** page, click the down arrow for the **Apply this rule to** drop down list box (figure 59) and select the **Specified destination set** option. Select the **Certificate Server** Destination Set you created earlier in the **Name** drop down list box. Click **Next**.

| ISA Manag | gement | |
|-----------------------------------|---|---------|
| <u>File</u> <u>Action</u> | New Web Publishing Rule Wizard 🛛 🔀 | |
| ← → E Internet Si → Serve - | Destination Sets Select the destinations to which this rule applies. | e Mode |
| | Apply this rule to: Specified destination set For Web publishing rules, destination sets usually include the external name or IP address of your ISA Server computer and path | n megr |
| | Name: Certificate Server Description: Destination Set for Certificate Server Web Publishing Rule | |
| ⊞∰ H.323 | < <u>Back</u> Cancel | |
| 🏄 Start 🛛 🕼 |) 🥑 🛛 🕅 ISA Management 🛛 🕹 📴 | 2:22 PM |

4. On the **Client Type** page, select the **Any request** option (figure 60). You do not want to force authentication at the Incoming Web Requests listener. Click **Next**.

| ISA Manag | jement | |
|--|--|---------|
| <u>File</u> <u>Action</u> | New Web Publishing Rule Wizard | د ا |
| ← → È Mi Internet Si ⊡ ጫ Serve – | Client Type You can specify client type by user name, group name, or IP address. | e Mode |
| | Apply the rule to requests from: Any request Specific computers (client address sets) Specific users and groups | nu mog |
| | <u>ABack</u> Next> Cancel | |
| 🦺 Start 🛛 🕑 | 🤪 🛛 🏙 ISA Management 🛛 🐴 | 2:23 PM |

5. On the **Rule Action** page, select the **Redirect the request to this internal Web server (name or IP address)** option (figure 61). In the text box below this option, type in the FQDN you entered in the HOSTS file. This redirects the request to the internal IP address for the published server and it will also show that the redirect to this FQDN. This will simplify your Web Proxy logs and make them more meaningful.

| ISA Manage | ement | |
|-----------------------------------|---|---------|
| Eile Action N | ew Web Publishing Rule Wizard 🛛 🔀 | |
| ← → € Internet Si ⊡ ⊕ Serve | Rule Action Specify how you want this rule to respond to requests from clients. | e Mode |
| | Response to client request: Discard the request Redirect the request to this internal Web server (name or IP address): cert.internal.net Brgwse Send the original host header to the publishing server instead of the actual one (specified above). Connect to this port when bridging request as HTTP: 80 Connect to this port when bridging request as SSL: 443 Connect to this port when bridging request as ETP: 21 | |
| | < <u>B</u> ack <u>Next></u> Cancel | F |
| 🏄 Start 🛛 🚱 | 🥑 🛛 🕅 ISA Management | 2:23 PM |

6. Review your settings on the **Completing the New Web Publishing Rule Wizard** page, then click the **Finish** button (figure 62).



The Web Publishing is effective without requiring your to restart the server or any of the ISA Server services.