Active Directory Certificate Services

Certificate Authorities (CAs) are as important to your organization's network infrastructure as domain controllers, DNS, and Dynamic Host Configuration Protocol (DHCP) servers. In this lesson, you learn how certificate templates affect the issuance of digital certificates, how to configure certificates to be assigned to users automatically, and how to configure supporting technologies such as Online Responders and credential roaming. A familiarity with these technologies helps you integrate the use of certificates in your organization's Windows Server 2008 or Windows Server 2008 R2 environment.

After this lesson, you will be able to:

- Install and manage AD CS.
- Configure autoenrollment for certificates.
- Configure credential roaming.
- Configure an Online Responder for Certificate Services.

Estimated lesson time: 45 minutes

Types of Certificate Authority

When planning the deployment of Certificate Services in your network environment, you must decide which type of CA best meets your organizational requirements. There are four types of CA:

- Enterprise Root
- Enterprise Subordinate
- Standalone Root
- Standalone Subordinate

The type of CA that you deploy depends on how certificates will be used in your environment and the state of the existing environment. You have to choose between an Enterprise or a Standalone CA during the installation of the Certificate Services role, as shown in Figure 3-9. You cannot switch between any of the CA types after the CA has been deployed.

Enterprise CAs require access to Active Directory. This type of CA uses Group Policy to propagate the certificate trust lists to users and computers throughout the domain and publish certificate revocation lists (CRLs) to Active Directory. Enterprise CAs issue certificates from certificate templates, which allow the following functionalities:

- Enterprise CAs enforce credential checks on users during the certificate enrollment process. Each certificate template has a set of security permissions that determines whether a particular user is authorized to receive certificates generated from that template.

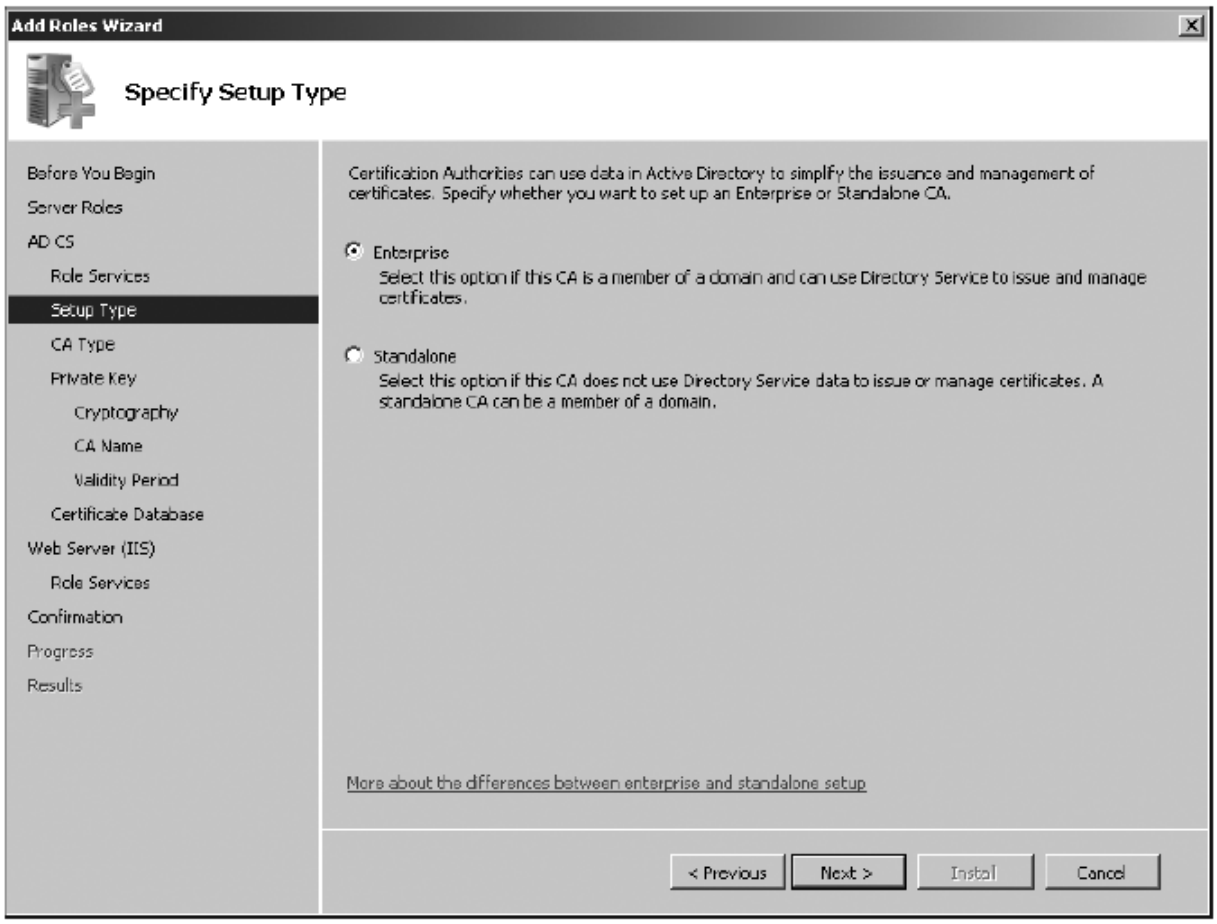

FIGURE 3-9 Selecting an Enterprise or Standalone CA

- Certificate names are generated automatically from information stored within Active Directory. The method by which this is done is determined by certificate template configuration.
- Autoenrollment can be used to issue certificates from Enterprise CAs, vastly simplifying the certificate distribution process. Autoenrollment is configured through applying certificate template permissions.

Enterprise CAs are fully integrated into a Windows Server 2008 or Windows Server 2008 R2 environment. This type of CA makes the issuing and management of certificates for Active Directory clients as simple as possible.

Standalone CAs do not require Active Directory. When certificate requests are submitted to Standalone CAs, the requestor must provide all relevant identifying information and manually specify the type of certificate needed. This process occurs automatically with an Enterprise CA. By default, Standalone CA requests require administrator approval. Administrator intervention is necessary because there is no automated method of verifying a requestor's credentials. Standalone CAs do not use certificate templates, which limits the ability for administrators to customize certificates for specific organizational needs.

You can deploy Standalone CAs on computers that are members of the domain. When installed by a user that is a member of the Domain Admins group, or one who has been delegated similar rights, the Standalone CA's information will be added to the Trusted Root

Certificate Authorities certificate store for all users and computers in the domain. The CA will also be able to publish its CRL to Active Directory.

Whether you install a Root or Subordinate CA depends on whether there is an existing certificate infrastructure. Root CAs are the most trusted type of CA in an organization's public key infrastructure (PKI) hierarchy. Root CAs sit at the top of the hierarchy as the ultimate point of trust and therefore must be as secure as possible. In many environments, a Root CA is used only to issue signing certificates to Subordinate CAs. When not used for this purpose, Root CAs are kept offline in secure environments to reduce the chance that they might be compromised.

If a Root CA is compromised, all certificates within an organization's PKI infrastructure should be considered compromised. Digital certificates are ultimately statements of trust. If you cannot trust the ultimate authority from which that trust is derived, it follows that you should not trust any of the certificates downstream from that authority.

Subordinate CAs are the network infrastructure servers that you deploy to issue the everyday certificates needed by computers, users, and services. An organization can have many Subordinate CAs, each of which is issued a signing certificate by the Root CA. In the event that one Subordinate CA is compromised, trust of that CA can be revoked from the Root CA. Only the certificates that were issued by that CA will be considered untrustworthy. You can replace the compromised Subordinate CA without having to replace the entire organization's certificate infrastructure. Subordinate CAs can be replaced, but a compromised Enterprise Root CA usually means you have to redeploy the Active Directory forest from scratch. If a Standalone Root CA is compromised, it also necessitates the replacement of an organization's PKI infrastructure.

Certificate Services Role-Based Administration

Because of the integral nature of Certificate Services to an organization's security infrastructure, many organizations use different staff members to manage different aspects of Certificate Services. One team is responsible for managing the CA itself, and a different team is responsible for managing the certificates that are issued by the CA. This separation is implemented through the assignment of Certificate Services roles.

The two critical roles are the CA Administrator and the Certificate Manager. Roles are designated by assigning permissions using the Security tab of the Properties dialog box of the certificate server (the server performing the CA role). You assign the CA Administrator role by granting the Manage CA permission to a user or group. You assign the Certificate Manager role by granting the Issue And Manage Certificates permission to a user or group. By default, the Domain Admins, Enterprise Admins, and local Administrators groups can assign these

roles. Figure 3-10 shows that the Alpha global security group holds the Certificate Manager roles because the group is assigned the Issue And Manage Certificates permission.

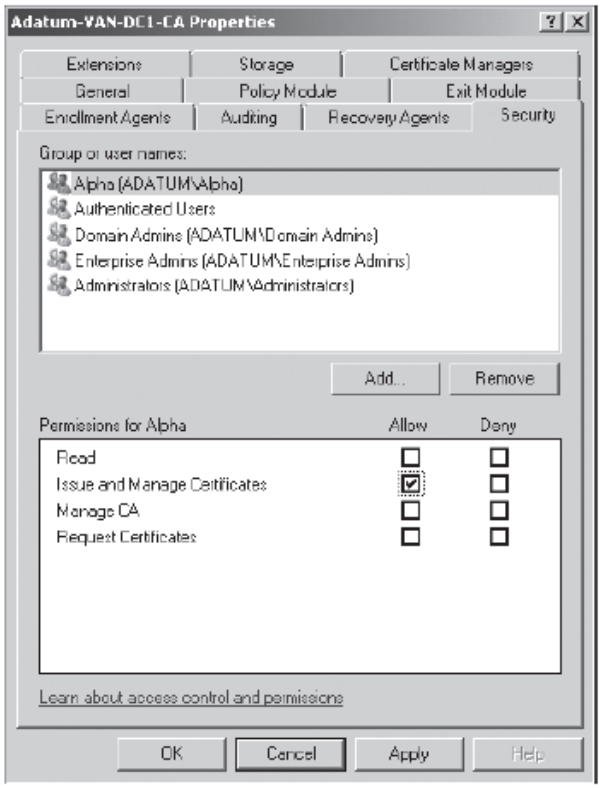

FIGURE 3-10 The Alpha group is assigned the Certificates Manager role

These roles have the following properties:

- **CA Administrator** This role should be assigned to staff who need to configure and maintain the CA itself. Users assigned this role can start and stop the certificate server, configure extensions, assign roles, renew CA keys, define key recovery agents, and configure certificate manager restrictions.
- **Certificate Manager** This role should be assigned to staff who are responsible for approving certificate enrollment and revocation requests. You can restrict certificate managers to specific groups or specific templates. Hence, you can configure one group with the permission to approve certificates issued from one template and configure another group with separate permission to approve certificates issued from a different template. You configure these restrictions on the Certificate Managers tab, shown in Figure 3-11.

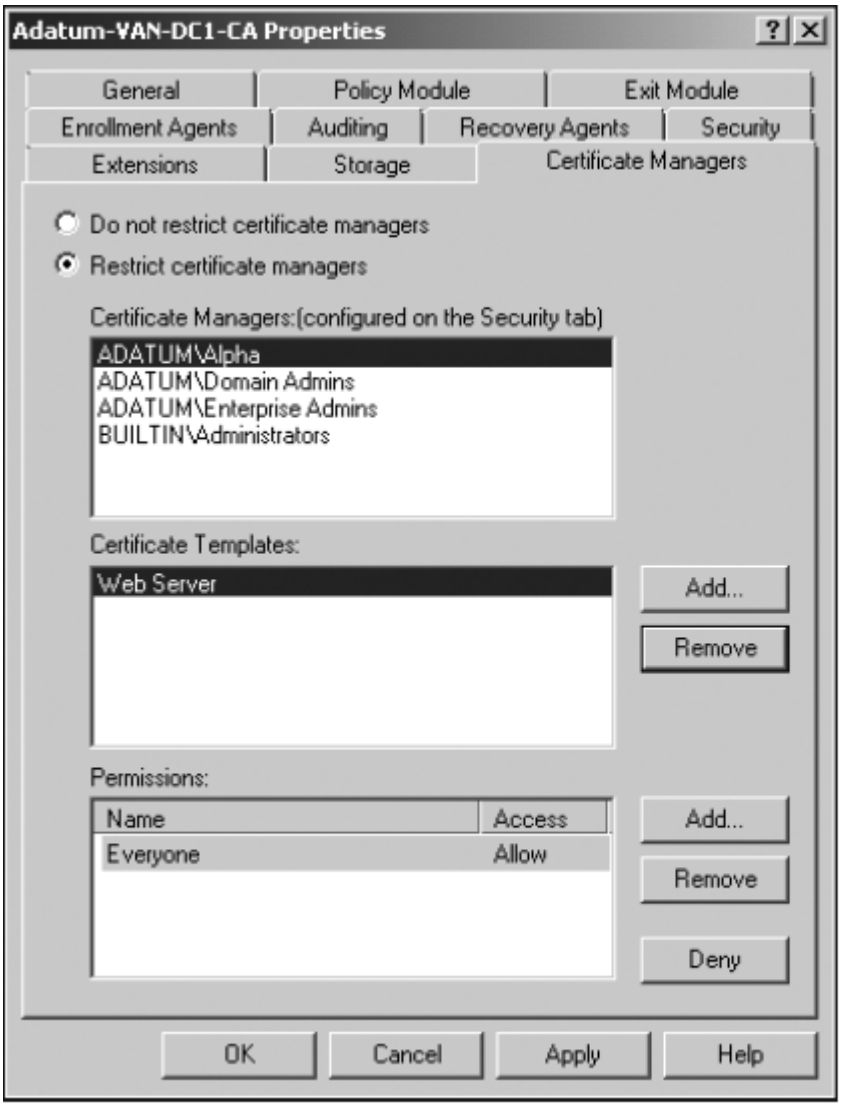

FIGURE 3-11 The Alpha user group can manage Web Server certificates

Installing a Root CA Certificate

Typically, a Root CA certificate is the first AD CS role service that you install in an organization. If your organization has a basic PKI, a Root CA may be the only CA that you need to deploy. The Root CA certificate establishes the basic rules that govern the issuing and use of certificates for your PKI. It defines standards for what is acceptable and unacceptable in the PKI hierarchy and AD CS applies those standards to any other CAs and AD CS role services.

A Root CA can be an Enterprise or Standalone CA. Many organizations minimize the exposure of their Root CA by keeping it offline except when it is needed to process a request for a Subordinate CA certificate.

To install a stand-alone Root CA on a server running Windows Server 2008 or Windows Server 2008 R2, you need (at a minimum) to be a member of the local Administrators group on that server. To install an Enterprise CA, you need (at a minimum) to be a member of the Domain Admins group for the domain. The high-level procedure to install a Root CA certificate is as follows:

1. Click Add Roles in Server Manager. Select the Active Directory Certificate Services role.
2. On the Select Role Services page, click Certification Authority.
3. On the Specify Setup Type page, select either Standalone or Enterprise as appropriate. Note that if you select Enterprise, you must have a network connection to a domain controller.
4. On the Specify CA Type page, click Root CA.
5. On the Set Up Private Key page, click Create A New Private Key.
6. On the Configure Cryptography page, select a cryptographic service provider, key length, and hash algorithm.
7. On the Configure CA Name page, specify a unique name to identify the CA.
8. On the Set Validity Period page, specify the number of years or months for which the Root CA certificate will remain valid.
9. On the Configure Certificate Database page, you typically accept the default location If you want, you can specify a custom location for the certificate database and the certificate database log.
10. On the Confirm Installation Options page, review all your configuration settings. If these are satisfactory, click Install.

Windows Server 2008 R2 Enhancements

Windows Server 2008 R2 retains all the enhancements to AD CS that were implemented by Windows Server 2008, and it introduces the following AD CS features and services that allow more flexible PKI deployments, reduce administration costs, and provide better support for Network Access Protection (NAP) deployments:

- **Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service** These services enable certificate enrollment over Hypertext Transport Protocol (HTTP).
- **Support for certificate enrollment across forests** This enables CA consolidation in multiple-forest deployments.
- **Improved support for high-volume CAs** This provides reduced CA database sizes for some NAP deployments and other high-volume CAs.

Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service

These new AD CS role services enable policy-based certificate enrollment over HTTP by using methods such as autoenrollment (discussed later in this lesson). The Web services act as a proxy between a client and a CA. This makes direct communication between the client and CA unnecessary and allows certificate enrollment over the Internet and across forests. The certificate enrollment Web services are available in all editions of Windows Server 2008 R2.

For example, Northwind Traders is a large multinational organization whose network infrastructure uses multiple forests. The company has an existing PKI, but it can benefit from the expanded accessibility of certificate enrollment provided by the certificate enrollment Web services, which enable its clients running Windows 7 to use HTTP to enroll certificates from CAs in different forests with Windows Server 2008 R2 schemas. To take advantage of this feature, the organization's Enterprise CA needs to be running the Enterprise or Datacenter edition of Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003.

Certificate Enrollment Across Forests That Have Two-Way Trust Relationships

Before the enhancements to AD CS introduced by Windows Sever 2008 R2, CAs could issue certificates only to members of the same forest, and each forest had its own PKI. Now, with added support for LDAP referrals, Windows Server 2008 R2 CAs can issue certificates across

forests that have two-way trust relationships. This facility allows direct enrollment and does not use HTTP.

For instance, in the Northwind Traders example given earlier, if the organization's Enterprise CA is running Windows Server 2008 R2 Enterprise or Windows Server 2008 R2 Datacenter, if each forest had a PKI, and if two-way trust relationships were established between the forests, the CA could issue cross-forest certificates. There are fewer restrictions in this scenario. Provided that the Enterprise CA was running an appropriate edition of Windows Server 2008 R2, the forests would require only a forest functional level of Windows Server 2003 or greater, and clients could be running Window XP, Windows Server 2003, or Windows Vista. Clients do not have to be running Windows 7.

Support for High-Volume CAs

Windows Server organizations whose CAs process a high volume of requests can choose to bypass certain CA database operations to reduce CA database size. For example, a high volume of CA traffic is generated when an organization deploys NAP with Internet Protocol Security (IPsec) enforcement. NAP health certificates typically expire within hours after being issued, and the CA might issue multiple certificates for each computer every day. By default, records for each request and issued certificate are stored in the CA database. A high volume of requests increases the CA database growth rate and administration cost. You can specify that issued certificates are stored elsewhere, not in the CA database on Enterprise CAs

running any edition of Windows Server 2008 R2.

If you specify this option, you need to bear in mind that because issued certificates are not stored in the CA database, certificate revocation is not possible. However, maintenance of a CRL for a high volume of short-lived certificates is often impractical or non-beneficial, and therefore you might choose to use this feature and accept the revocation limitation.

Configuring Credential Roaming

Credential roaming allows for the storage of certificates and private keys within Active Directory. For example, a user's Encrypting File System (EFS) certificate can be stored in Active Directory and provided to the user when she logs on to different computers within the domain. The same EFS certificate will always be used to encrypt files. This means that the user can encrypt files on an NTFS-formatted USB storage device on one computer and then decrypt them on another because the EFS certificate will be transferred to the second computer's certificate store during the logon process. Credential roaming also allows for all of a user's certificates and keys to be removed when she logs off the computer.

Credential roaming is enabled through the Certificate Services Client – Credential Roaming Policy, located through the Group Policy Management feature in Server Manager under User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies, as shown in Figure 3-12.

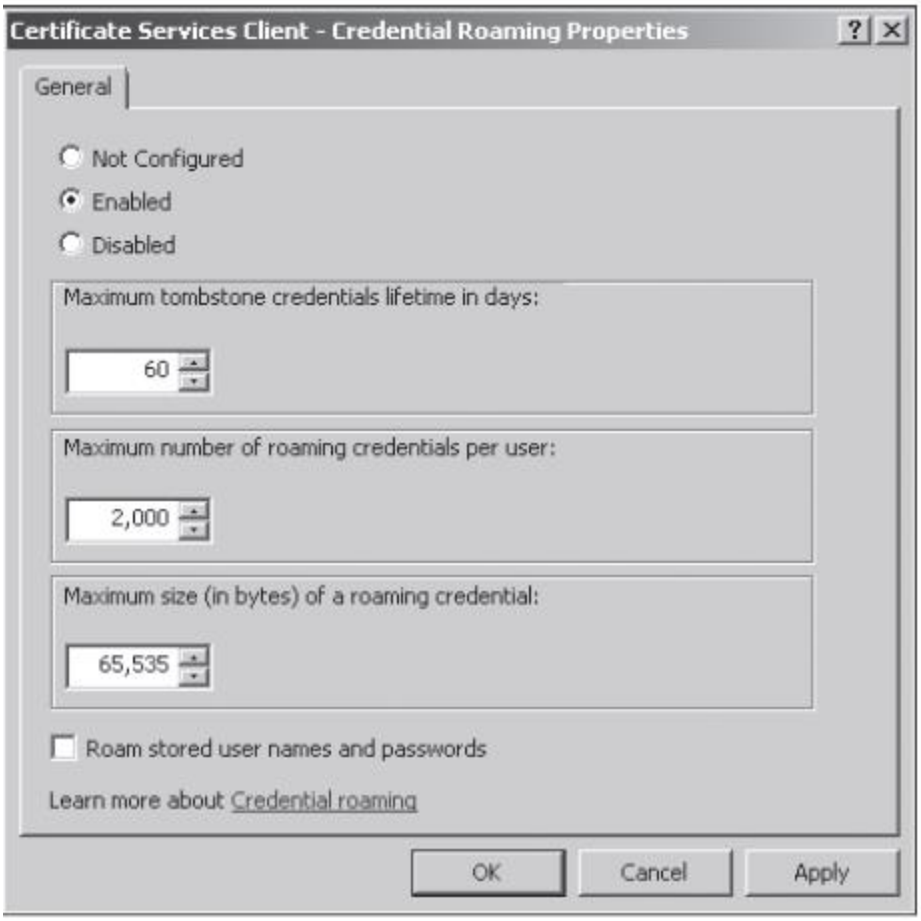

FIGURE 3-12 Credential Roaming Policy

When a user logs on to a client in a domain where the Credential Roaming Policy has been enabled, the certificates in the user's store on the client are compared to certificates stored for the user within Active Directory.

- If the certificates in the user's certificate store are up to date, no further action is taken.
- If more recent certificates for the user are stored in Active Directory, these credentials are copied to the client.
- If more recent certificates are located in the user's store, the certificates stored in Active Directory are updated.

Credential roaming synchronizes and resolves any conflicts between certificates and private keys from any number of clients that a user logs on to, as well as certificates and private keys stored within Active Directory. Credential roaming is triggered whenever a private key or certificate in the local certificate store changes, whenever the user locks or unlocks a computer, and whenever Group Policy refreshes. Credential roaming is supported on Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 SP1, Windows 7, Windows Vista, and Windows XP SP2.

Configuring Autoenrollment

Autoenrollment allows certificates to be distributed to clients without direct client intervention. It also enables the automatic enrollment of subjects for specific certificates and allows for the retrieval of issued certificates and the automatic renewal of expiring certificates without the need for subject or administrator intervention. In most cases, autoenrollment occurs without the user being aware of it, although you can configure certificate templates in such a way that they do interact with the subjects.

Configuring a Template for Autoenrollment

Before a certificate can be enrolled automatically, it is necessary to configure several aspects of the certificate template. Certificate templates are modified using the Certificate Templates snap-in, which you will need to add to a custom MMC. Only users with the Certificate Manager role's permissions are able to create and modify certificate templates.

When using the Certificate Templates console, note that you cannot configure the autoenrollment permission for a Level 1 certificate template. Level 1 certificates have Windows 2000 as their minimum supported CA. Level 2 certificate templates have Windows Server 2003 as a minimum supported CA. Level 2 certificate templates are also the minimum level of certificate template that supports autoenrollment. Level 3 certificate templates are supported only by clients running Windows Server 2008, Windows Server 2008 R2,

Windows Vista, or Windows 7. Level 3 certificate templates allow administrators to configure advanced Suite B cryptographic settings. These settings are not required to allow certificate autoenrollment, and most administrators find Level 2 certificate templates are adequate for their organizational needs.

If you do create a new certificate template based on an existing one, you should configure the template you copied as a superseded template. This allows certificates that are configured using previous settings to be updated to the new settings. You will also need to configure the CA to publish this new template through the Certification Authority console. To configure automatic certificate enrollment for a specific template, perform these steps:

1. Open the Certificate Templates snap-in.
2. Right-click the certificate template that you want to modify, and then click Properties.
3. Configure the General, Request Handling, and Issuance Requirements as necessary for the purposes of the certificate. (Note that not every certificate template has all three tabs in its Properties dialog box. For example, the Basic EFS certificate template does not have an Issuance Requirements tab. In addition, note that this step is not necessary for autoenrollment, but you should review these settings because they allow you to tune the automatic issuing of certificates better.)
4. On the Certificate Template's Security tab, select the group that you will allow to enroll certificates automatically and the select the Allow box next to the Autoenroll

permission. Figure 3-13 shows autoenrollment configured for the Authenticated Users group for Kerberos authentication, which is a Level 2 certificate template.

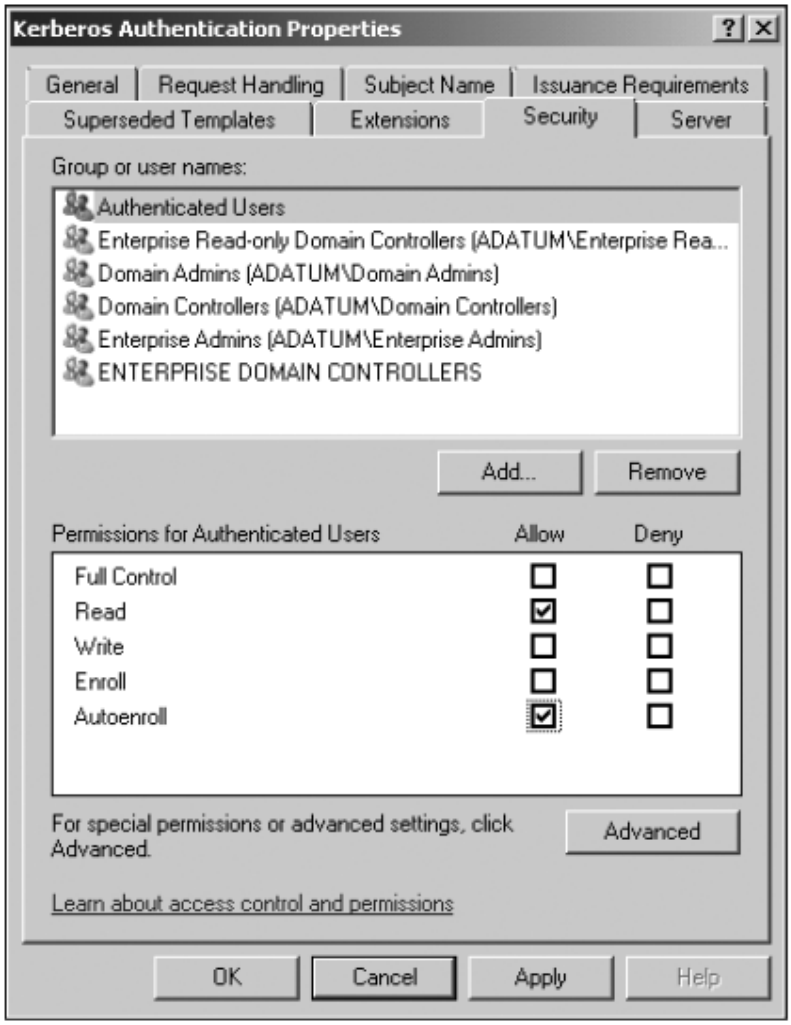

FIGURE 3-13 Enabling the autoenroll permission to allow automatic enrollment

Configuring Group Policy for Autoenrollment

After you have set up the permissions on certificate templates, your next step in deploying autoenrollment of certificates throughout your organization is to configure the default domain policy to support autoenrollment. To configure Group Policy for autoenrollment, perform the following steps:

1. Edit the Default Domain Policy GPO using the Group Policy Management Console feature located in Server Manager under Features.
2. Under User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies, double-click Certificate Services Client – Auto-Enrollment. This will open the Certificate Services Client – Auto-Enrollment Properties policy dialog box.
3. Choose Enabled from the Configuration Model drop-down list and then configure the expiration and update settings as shown in Figure 3-14.

After you enable the Certificate Services autoenrollment policy, those certificates that have templates configured for autoenrollment will be deployed automatically. You can also enable the following policy options as a part of the autoenrollment policy:

- **Renew Expired Certificates, Update Pending Certificates, And Remove Revoked Certificates** This policy primarily relates to certificate management. If you have enabled autoenrollment, you will probably want to ensure that expired certificates are renewed automatically, revoked certificates are removed, and pending certificates are

updated. Enabling this option vastly reduces the workload of certificate administrators.

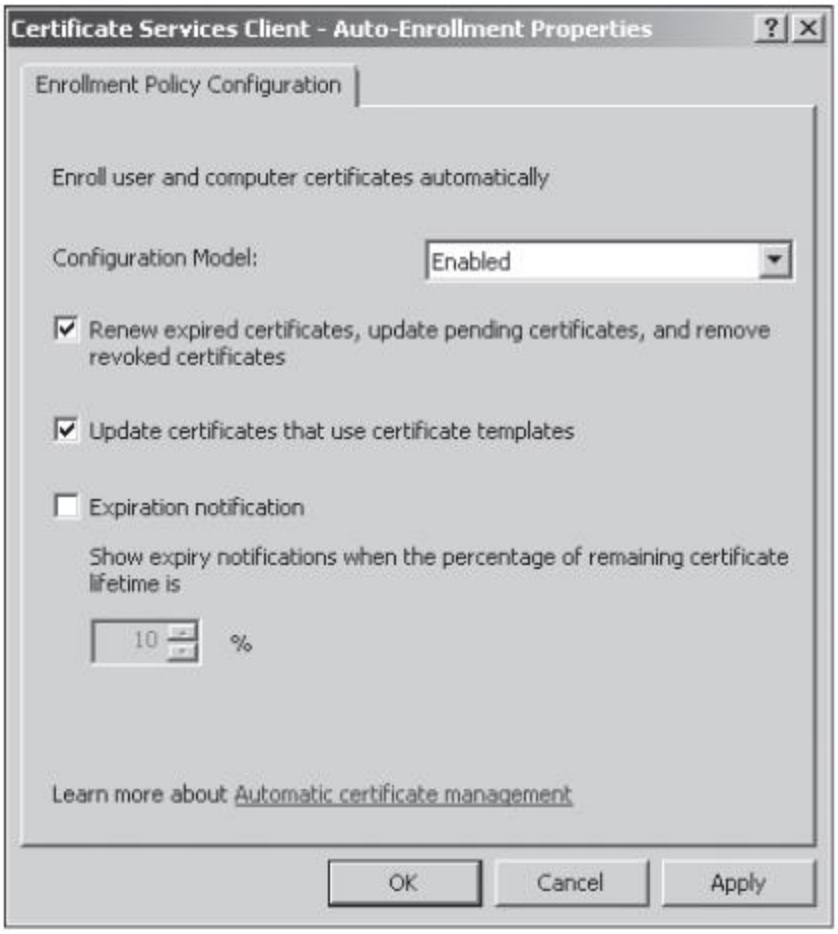

FIGURE 3-14 Configuring autoenrollment policies

- **Update Certificates That Use Certificate Templates** When this policy is enabled and the template that the certificate was issued from is revised or replaced, the issued certificate will be updated.
- **Expiration Notification** This policy is less necessary when you configure expired certificates to renew automatically, but it can be useful when certificate templates are configured so that automatic renewal (rather than automatic enrollment) does not occur.

Configuring Web Enrollment Support

Web enrollment allows users of Windows Internet Explorer version 6 and later to submit certificate requests to a CA directly through a Web application. You can use Web enrollment to do any of the following:

- Request certificates and review existing certificate requests
- Access CRLs
- Perform smart card enrollment

Web enrollment is deployed primarily to provide an enrollment mechanism for organizations that need to issue and renew certificates for users and computers that are not joined to an Active Directory domain or who are using non-Microsoft operating systems. Users of browsers other than Internet Explorer version 6 and later are able to submit enrollment requests using the Web enrollment application, but they must first create a Public-Key Cryptography Standards (PKCS) #10 request before submitting it through the Web enrollment pages. Once the request is made successfully, users can reconnect to the Web enrollment application and are able to download and install their requested certificates.

To configure a server to support Web enrollment, the Certification Authority Web Enrollment role service needs to be added to the server role. When the Certification Authority Web Enrollment role service is installed on a computer that is operating as a CA, no future configuration steps are required. If the Certification Authority Web Enrollment service is installed on a separate computer from the CA, the CA needs to be specified during the Certification Authority Web Enrollment role service installation process.

Web enrollment has the following limitations:

- Web enrollment cannot be used with version 3 certificate templates. Only version 1 and 2 certificate templates are supported by Web enrollment.
- Computer certificates cannot be requested using Web enrollment from a Windows Server 2008 or Windows Server 2008 R2 CA.
- If Microsoft Internet Information Services (IIS) is installed on a 64-bit version of Windows Server 2008 or on Windows Server 2008 R2, some 32-bit Web applications cannot be installed because this will force IIS to run in 32-bit mode. The Web enrollment role service will attempt to install as a 64-bit Web application, and the installation will fail. This does not apply to 32-bit versions of Windows Server 2008.

Configuring CRLs

Certificate Services do more than issue certificates. Certificates are tokens of trust, and in certain cases those tokens of trust need to be revoked. This process is called *certificate revocation*. The most common method of publishing information about which certificates issued by a CA are no longer valid is the certificate revocation list (CRL). CRLs are lists of certificate serial numbers for certificates that have either been revoked or are placed on hold. CRLs are issued by the CA that issues the corresponding certificate, rather than an upstream or a downstream CA. When a certificate is to be used, a check against the issuing CA's CRL needs to be made. The location of the CRL is included with the certificate so that the client knows where on the network to look to verify that the certificate that it is about to accept is still actually valid.

Specifying a CRL Distribution Point

The Extensions tab on a Certificate Server's Properties dialog box, shown in Figure 3-15, allows you to add, remove, or modify CRL distribution points. When you make a modification to the list of distribution points, you should be aware that this will apply only to certificates issued from that point on; it does not apply retroactively. Your user account must have been assigned the Certificate Manager role to modify CRL distribution point configuration information. CRL Uniform Resource Locators (URLs) can use HTTP, FTP, LDAP, or FILE addresses.

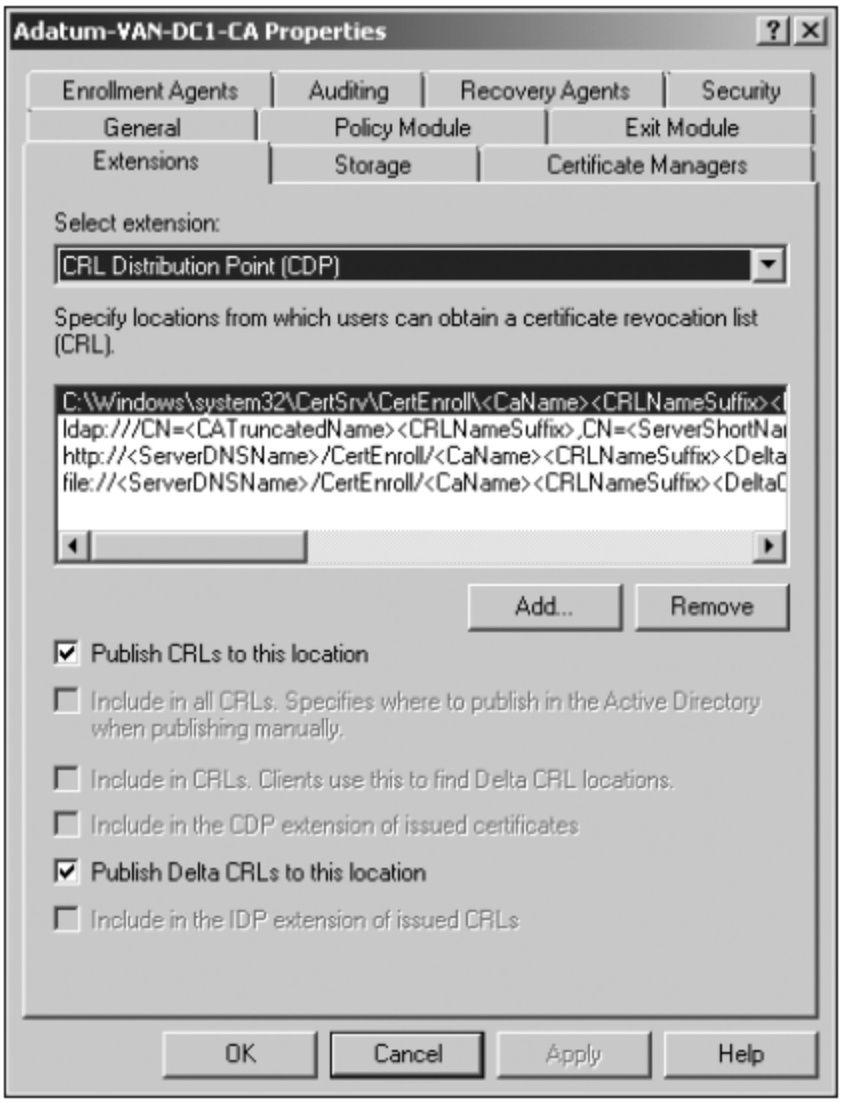

FIGURE 3-15 Configuring a CRL distribution point

Configuring CRL and Delta CRL Publication

Because CRLs can become very large, you can publish a smaller type of CRL called a delta CRL at a more frequent interval. A delta CRL contains only data about certificates that have been revoked since the publication of the last full CRL. This allows clients to retrieve the small delta CRL and add it to a cached copy of the full CRL to build a complete list of revoked certificates. Delta CRLs allow for revocation data to be published more frequently, which makes the deployment of Certificate Services more secure. An outdated CRL cannot be used to inform clients of the most recent revocations because these revocations will not be published until the next time the full CRL is published.

The CRL and delta CRL publication intervals are configured by modifying the properties of the Revoked Certificates node on a CA, as shown in Figure 3-16. You can access this dialog box by right-clicking Revoked Certificates under the CA in the Server Manager console and clicking Properties. The default CRL publication interval is once a week, and the default delta CRL publication interval is once a day.

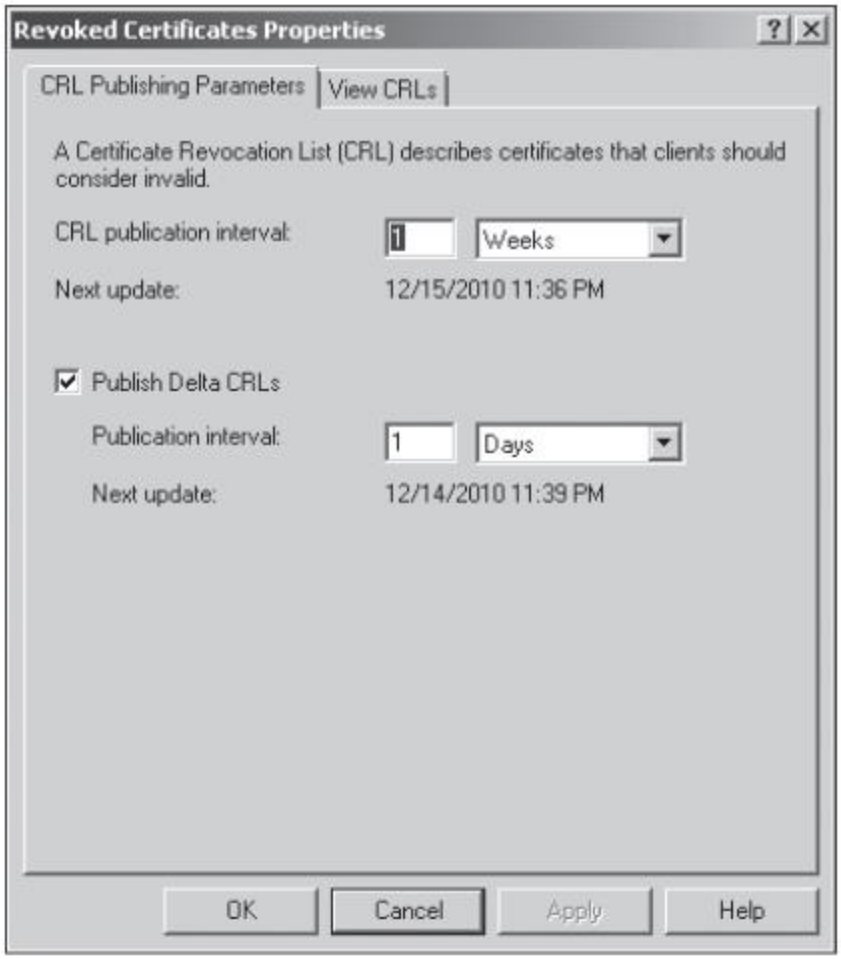

FIGURE 3-16 Configuring CRL publication interval

Configuring an Online Responder for Certificate Services

Significant delays in CRL publication can occur during periods of peak activity, such as when large numbers of users log on using smart cards, encrypt files, or use digital signatures. This is because the entire CRL has to be checked and, as mentioned earlier in the lesson, CRLs can become very large. CRL checks cannot be load-balanced to another CA if the issuing CA is experiencing a traffic spike. Attempts have been made to solve this problem using solutions such as partitioned CRLs, delta CRLs, and indirect CRLs. All these prior solutions ended up increasing the complexity of CA implementation without significantly reducing the problem of traffic spikes. This is where Online Certificate Status Protocol (OCSP) comes in.

An Online Responder receives and responds only to requests about the status of individual certificates. For example, rather than having to download the CA's entire CRL to see whether the signing certificate issued to Don Hall is valid, the client queries the Online Responder to see if Don Hall's signing certificate is valid and receives a response that provides only information about Don Hall's signing certificate. This significantly reduces the load on the issuing CA and also reduces network traffic. CRLs can get very large, and distributing a CRL to each of 100 clients can use a lot of bandwidth. Depending on the size of the CRL, providing revocation information about 100 different specific certificates may use less bandwidth than forwarding the current CRL to a single client.

Windows Server 2008 and Windows Server 2008 R2 OCSP includes the following features:

- **Web proxy caching** The Online Responder Web proxy cache is the interface that clients connect with to access Online Responder data. It is implemented as an Internet Server Application Programming Interface (ISAPI) extension hosted by IIS.
- **Support for nonce and no-nonce requests** You can set nonce and no-nonce request configuration options to prevent replay attacks on Online Responders. Replay attacks work by either repeating or delaying the transmission of legitimate data. A replay attack could be used to indicate that a revoked certificate is still valid.
- **Advanced cryptography support** You can configure OCSP to use elliptic curve and SHA-256 cryptography.
- **Kerberos protocol integration** OCSP requests and responses can be processed with Kerberos password authentication, allowing for the validation of server certificates during the logon process.
- **Single point or responder array** A single computer can function as an Online Responder, or multiple linked computers can host Online Responders, allowing for certificate validity checks to be balanced across multiple hosts.

You can install the Online Responder service on a CA, but Microsoft recommends deploying the Online Responder service on a separate computer. A single computer with the Online Responder service deployed can provide revocation status data for certificates issued by a single or multiple CAs. As mentioned earlier, a single CA's revocation data can be distributed across multiple Online Responders.

The Online Responder service is installed on computers running Windows Server 2008 and Windows Server 2008 R2 and is managed through the Online Responder MMC snap-in, shown in Figure 3-17. Note that you cannot access this console until you deploy an Online Responder, which you do in a practice later in this chapter.

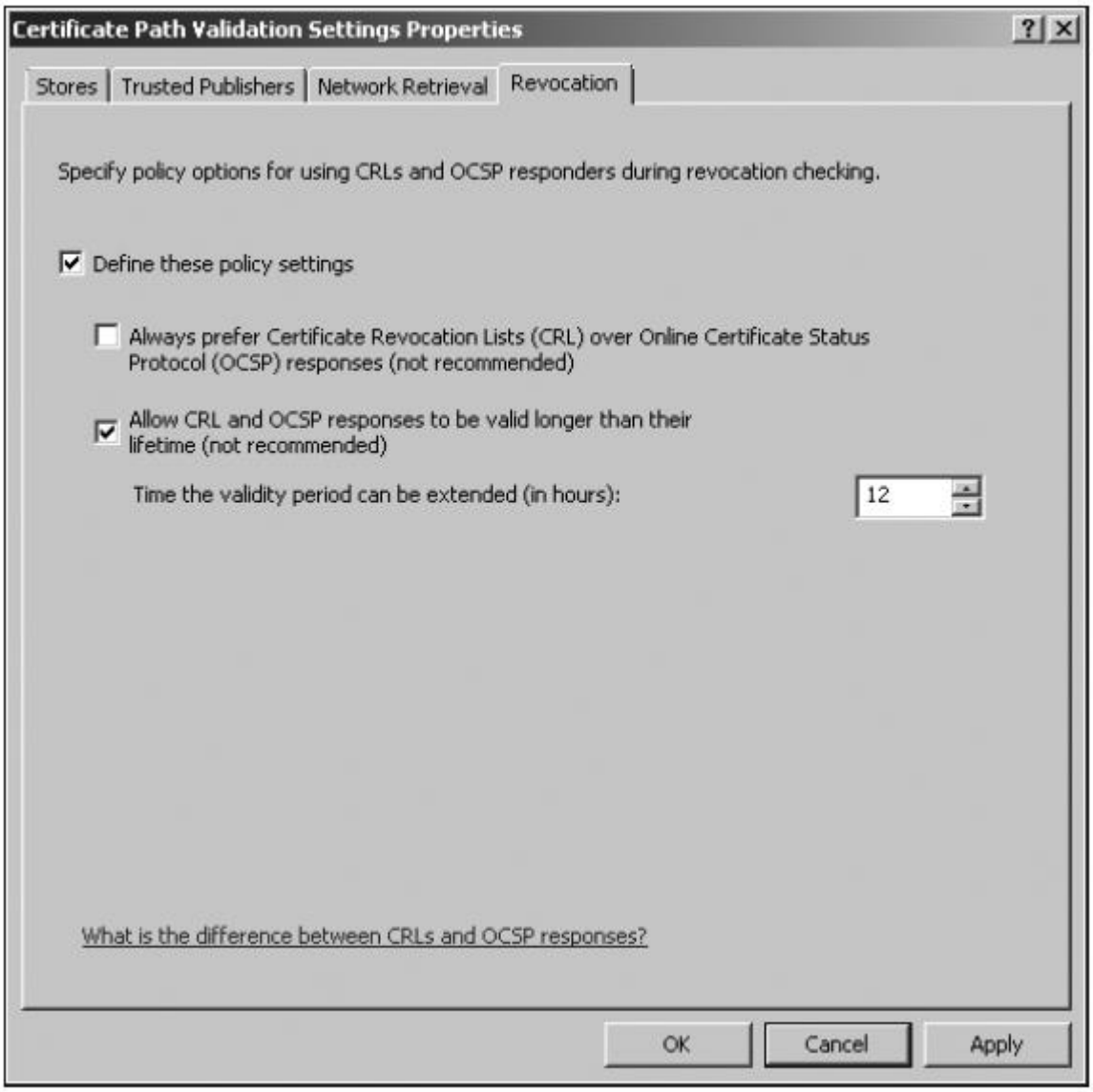

FIGURE 3-17 The Online Responder management console

You should deploy Online Responders after the deployment of CAs but prior to the issuance of client certificates. To deploy the Online Responder service to a computer running Windows Server 2008 or Windows Server 2008 R2, the following conditions must be met:

- IIS must already be installed on the computer that will host the Online Responder service.
- An OCSP Response Signing certificate template must be configured on the CA, and autoenrollment must be used to issue an OCSP Response Signing certificate to the computer that will host the Online Responder service. An Online Responder cannot provide status information for a certificate issued from a CA higher in the CA chain than the one that issued its signing certificate.
- The URL for the Online Responder must be included in the Authority Information Access (AIA) extension of certificates issued by the CA. This URL will be used by clients to locate the Online Responder so that certificate validation can occur.

After you have deployed the Online Responder, you create a revocation configuration for each CA and CA certificate that will be serviced by the Online Responder. Revocation configurations include all settings required to reply to client status requests with respect to certificates issued using a specific CA key. These settings include the CA certificate, signing certificate for the Online Responder, and the revocation provider that provides revocation data used by the revocation configuration. When configuring a single Online Responder for multiple CAs, ensure that the Online Responder has a key and signing certificate for each CA that it supports. In the practice at the end of this lesson, you will configure an Online Responder.

Configuring Responder Arrays

If the Online Responder that you have deployed in your network environment is unable to cope with projected traffic, you can deploy an array of computers functioning as Online Responders. As mentioned earlier in this lesson, an array of Online Responders can handle the revocation traffic of one or more issuing CAs. Online Responder Arrays are also often deployed for fault-tolerance purposes. Nodes in Online Responder Arrays can also be deployed at branch or satellite office locations that have only intermittent network

connectivity to the site that hosts the issuing CA.

Online Responder Arrays have one member of the array configured as the Array controller and the rest as array members. Although each Online Responder in an array can be managed and configured separately when conflicts arise, the configuration settings for the Array controller override configuration settings for array members.

To create an Online Responder Array you need to perform the following general steps:

1. Configure the CAs in your organization that are used to issue certificates to support Online Responders.
2. Add the Online Responder service to all servers that will participate in the planned array.
3. Add the Online Responders to the array by opening the Online Responder console, selecting the Array Configuration Members node, and using the Add Array Members item in the Actions pane.

OCSP Group Policy Settings

Windows Server 2008 and Windows Server 2008 R2 include several Group Policy settings that enhance the management of OCSP and CRL data use. To access these settings, edit Default Domain Policy in the console tree of Server Manager and access the Revocation tab of the Properties dialog box located at Computer Configuration/Policies/Windows Settings/ Security Settings/Public Key Policies/Certificate Path Validation Settings node. This is shown in Figure 3-18.

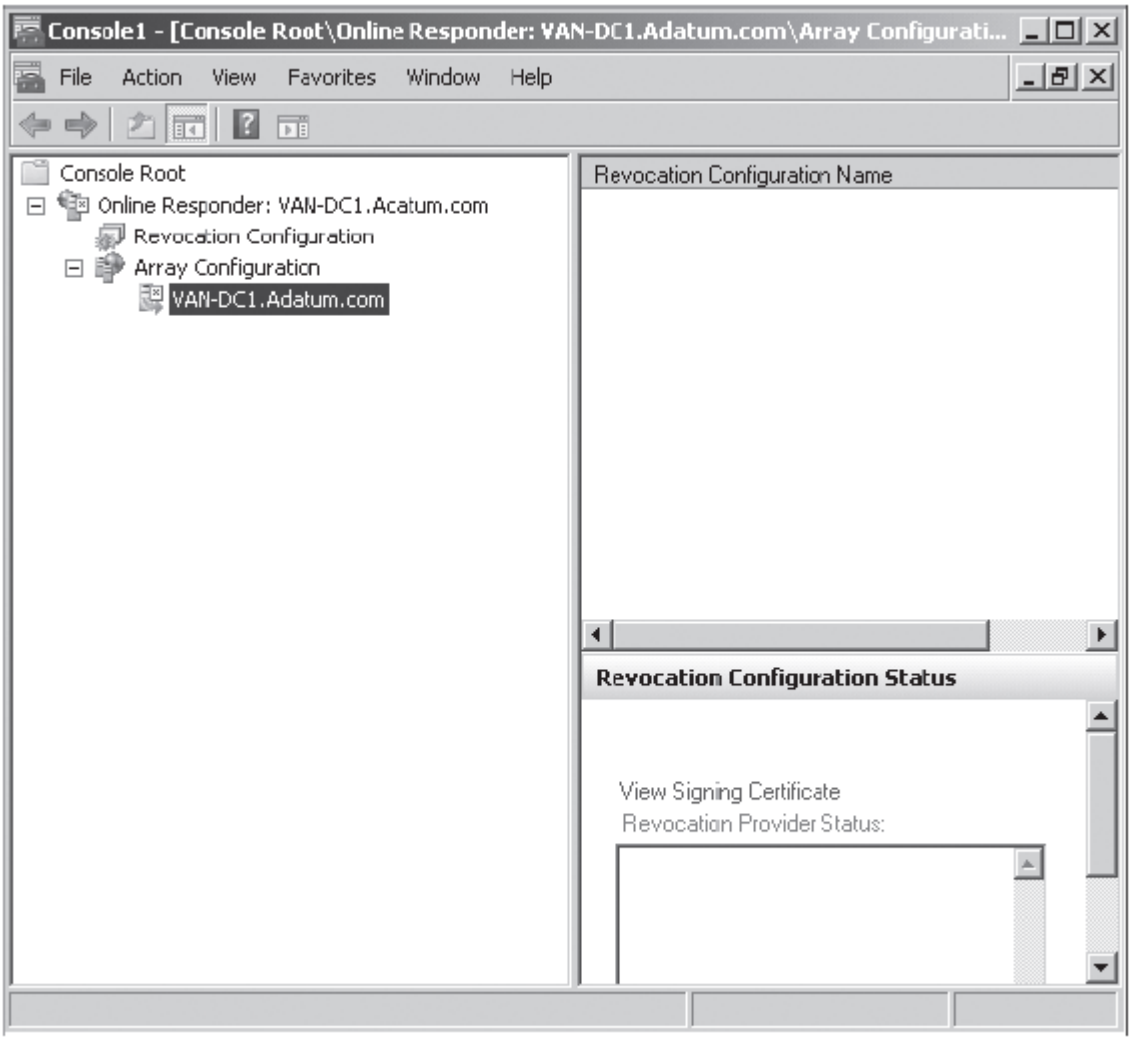

FIGURE 3-18 Group Policy options related to OCSP

One of the reasons for configuring these policies is that CRLs have expiration dates and if the expiration date passes prior to the update becoming available, the certificate chain validation might fail, even with an Online Responder deployed. Problems can occur when an Online Responder is forced to rely upon an expired CRL. By selecting Allow CRL And OCSP Responses To Be Valid Longer Than Their Lifetime, you can effectively issue an extension to CRLs in the event that they are not updated in a timely manner.

Network Device Enrollment Service

The Network Device Enrollment Service allows a Windows Server 2008 or Windows Server 2008 R2 CA to issue and manage certificates for routers and other network devices that do not have accounts within the Active Directory database. The Network Device Enrollment Service allows network devices to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP). The Network Device Enrollment Service provides the following functionalities to a network environment:

- Generates and provides one-time enrollment passwords to administrators of network devices
- Submits SCEP enrollment requests on behalf of network devices to a Windows Server 2008 CA
- Retrieves issued certificates from the CA and directs them to the network device

By default, the Network Device Enrollment Service can cache only five passwords at a time. This limits the number of network devices that can participate in the enrollment process to five. It is possible to flush stored passwords from the cache by restarting IIS, and it is also possible to configure the Network Device Enrollment Service to cache more than five passwords at a time.

Using Enterprise PKI to Monitor CA Health

You can add the Enterprise PKI snap-in to a custom console (shown in Figure 3-19) to monitor the health of all CAs within a PKI. The Enterprise PKI tool allows you to view the status of your organization's PKI environment. In an organization that has multiple levels of issuing CAs, having an at-a-glance view of all certificate servers allows administrators to manage the CA hierarchy and troubleshoot CA errors easily and effectively. The Enterprise PKI snap-in provides data on the validity or accessibility of AIA locations and CRL distribution points.

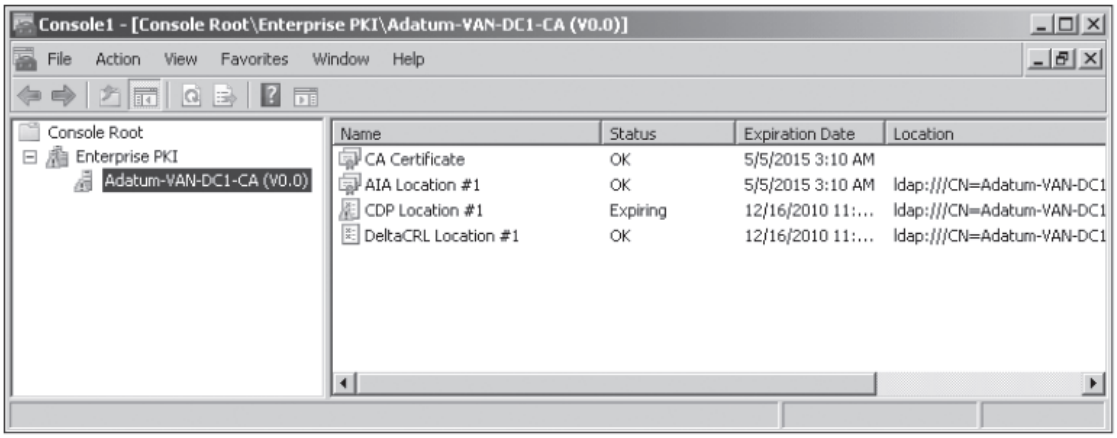

FIGURE 3-19 Enterprise PKI custom console

The Enterprise PKI snap-in works on both Windows Server 2008 and Windows Server 2003 Enterprise CAs. The Enterprise PKI tool provides the following status information about each CA in the PKI hierarchy:

- **Question Mark** Health status is being evaluated.
- **Green Indicator** CA is problem-free.
- **Yellow Indicator** CA has a non-critical problem.
- **Red Indicator** CA has a critical problem.
- **Red Cross Over CA Icon** CA is offline.

The most common configuration problems are likely to be the second AIA location, the second delta CRL location, and the CDP location. When confronted with CA configuration issues, you should use the following strategies in an attempt to resolve the issue:

- If the issue is CA-related, such as problems connecting to a current CRL, use the Certification Authority console to manage the problem by connecting to the CA experiencing the problem.
- If the issue relates to the Online Responder, use the Online Responder Management console to resolve the issue.
- If the Enterprise PKI console reports that CA certificates are about to expire, you should use the Certificates snap-in of a custom console to renew these certificates.
- It is possible to enable CryptoAPI 2.0 diagnostics to obtain detailed information about PKI-related issues. This is done by enabling the Operational log under Applications And Service Logs/Microsoft/Windows/CAPI2 log in Event Viewer, shown in Figure 3-20.

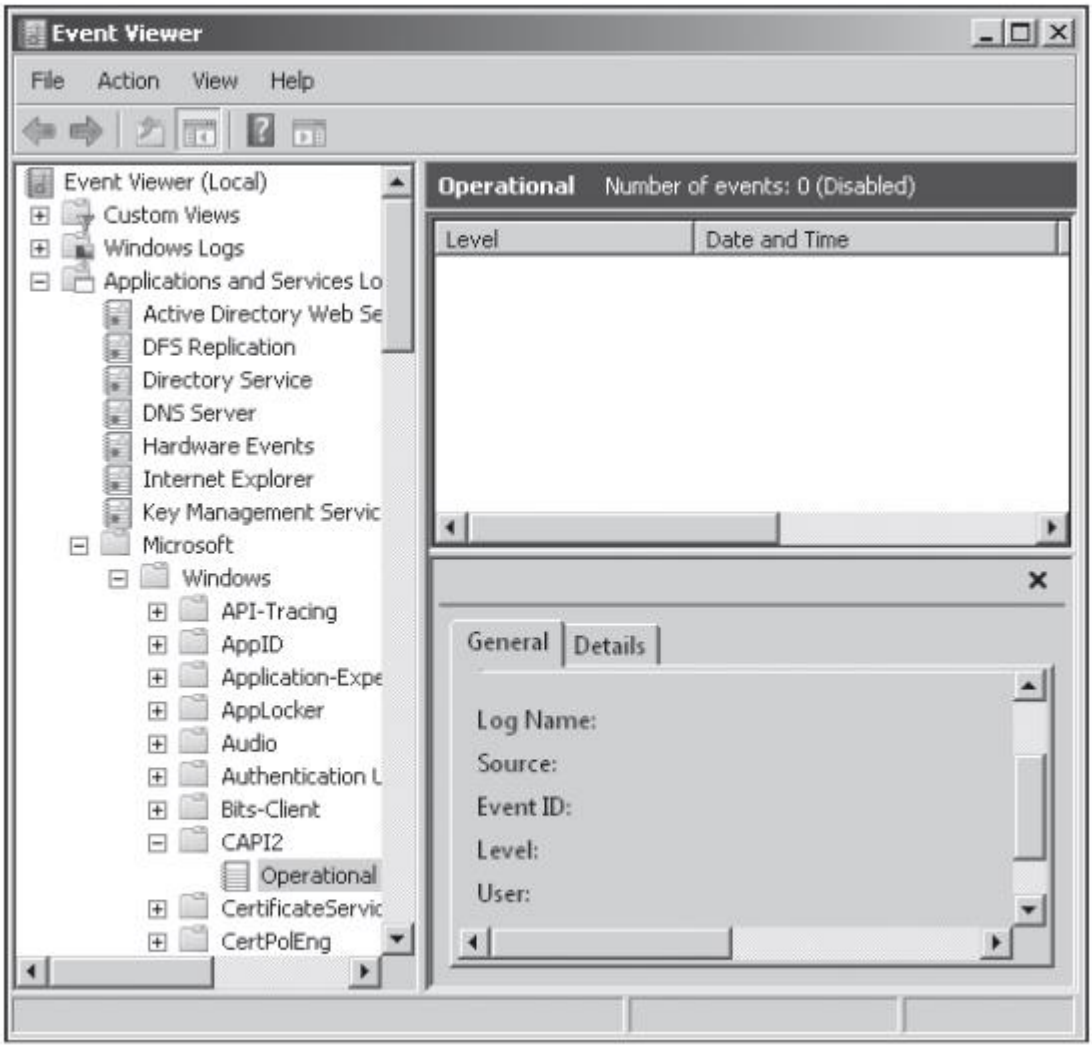

FIGURE 3-20 The operational log for CryptoAPI 2.0 diagnostics

Lesson Summary

- Enterprise CAs are used to support Active Directory. Enterprise CAs are added automatically to the domain user's trusted certificate stores. Most certificate service deployments in Windows Server 2008 and Windows Server 2008 R2 network environments use Enterprise CAs.
- Standalone CAs do not require the deployment of Active Directory and cannot be configured to use certificate templates.
- Online Responders process requests for CRL data more efficiently than traditional CRL publishing methods.
- Credential caching ensures that a user's certificates are up to date by frequently comparing local certificates with certificates stored in Active Directory.
- Autoenrollment allows certificates to be deployed automatically, without user or administrator intervention, to eligible clients. Autoenrollment has to be enabled within a certificate template and within Group Policy.
- Windows Server 2008 R2 introduces AD CS features and services that allow more flexible PKI deployments, reduce administration costs, and provide better support for NAP deployments.