

Lesson 20: Managing Certificates

MOAC 70-412: Configuring Advanced
Windows Server 2012 Services

Overview

- Objective 6.3 – Manage certificates.
 - Manage certificate templates
 - Implement and manage certificate deployment, validation, and revocation
 - Manage certificate renewal
 - Manage certificate enrollment and renewal to computers and users using Group Policies
 - Configure and manage key archival and recovery

Managing Digital Certificates

Lesson 20: Managing Certificates

Digital Certificate

- A **digital certificate** is like an electronic identification card used to certify the online identify of individuals, organizations, and computers.
- It contains a person's or an organization's name, a serial number, an expiration date, a copy of the certificate holder's public key (used for encrypting messages and creating digital signatures), and the digital signature of the Certification Authority (CA) that assigned the certificate so that recipients can verify that the certificate is real.

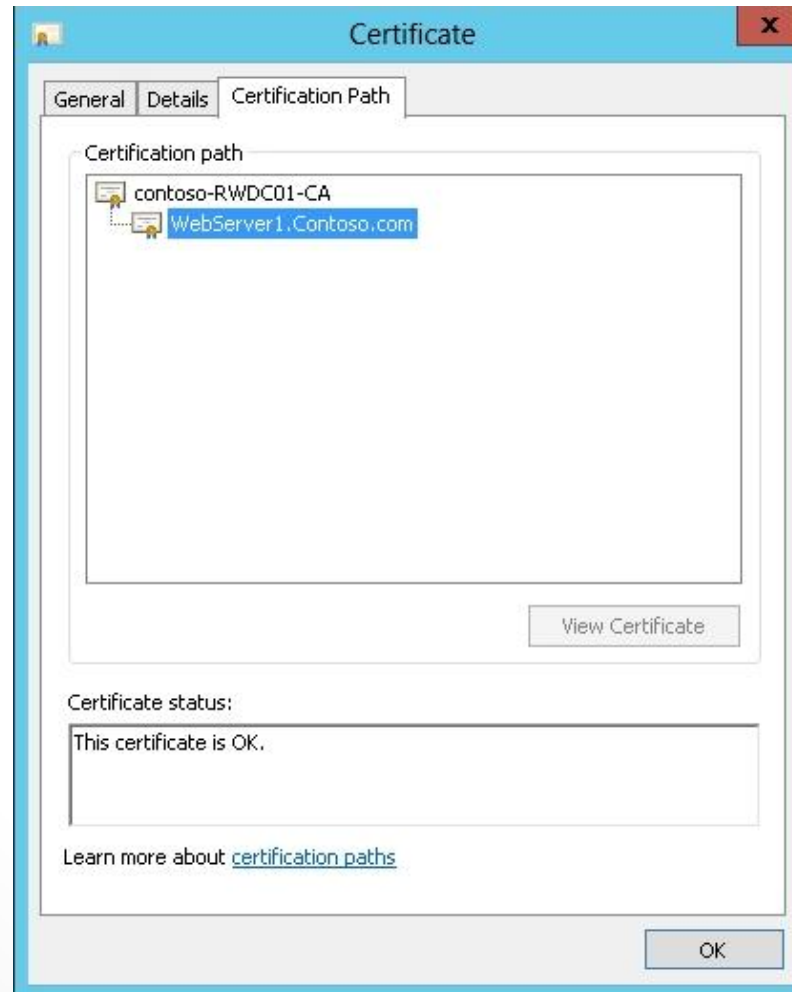
Digital Certificates

- The most common digital certificate is **X.509 version 3**.
- The X.509 version 3 standard specifies the format for the public key certificate, certificate revocation lists, attribute certificates, and a certificate path validation algorithm.

Certificate Chain

- There are only so many root CA certificates assigned to commercial third-party organizations.
- Therefore, when you acquire a digital certificate from a third-party organization, you might need to use a certificate chain to obtain the root CA certificate so that it can be trusted.
- In addition, you might need to install an intermediate digital certificate that links the assigned digital certificate to a trusted root CA certificate.
- The **certificate chain**, also known as the certification path, is a list of certificates used to authenticate an entity.
- It begins with the certificate of the entity and ends with the root CA certificate.

Certification Path



Certificate Stores

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window Help

Console Root

- Certificates (Local Computer)
 - Personal
 - Certificates
 - Trusted Root Certification Authorities
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification Authoriti
 - Trusted People
 - Client Authentication Issuers
 - Remote Desktop
 - Certificate Enrollment Requests
 - Smart Card Trusted Roots
 - Trusted Devices
 - Web Hosting

Issued To	Issued By	Expiration D...	Intended Purposes	Friendly Name
contoso-RWDC01-CA-1	contoso-RWDC01-CA-1	1/21/2018	<All>	<None>
contoso-RWDC01-CA-1	contoso-RWDC01-CA-1	1/22/2018	<All>	<None>
RWDC01.contoso.com	contoso-RWDC01-CA	1/20/2015	Server Authentication	rwdc01.contoso.co
RWDC01.contoso.com	contoso-RWDC01-CA	1/18/2014	Client Authentication...	<None>
rwdc01.contoso.com	contoso-RWDC01-CA	1/20/2015	Server Authentication	<None>
WebServer1.contoso.com	contoso-RWDC01-CA	1/18/2015	Server Authentication	WebServer1.Conto:

Personal store contains 6 certificates.

Importing and Exporting Digital Certificates

- **Personal Information Exchange (PKCS #12)**
 - Supports secure storage of certificates, private keys, and all certificates in a certification path.
 - The only file format that can be used to export a certificate and its private key.
 - Usually has a .pfx or .p12 filename extension.
- **Cryptographic Message Syntax Standard (PKCS #7)**
 - Supports storage of certificates and all certificates in a certification path.
 - Usually has a .p7b or .p7c filename extension.
- **Distinguished Encoding Rules (DER)-encoded binary X.509**
 - Supports storage of a single certificate.
 - Does not support storage of the private key or certification path.
 - Usually has a .cer, .crt, or .der filename extension.
- **Base64-encoded X.509**
 - Supports storage of a single certificate.
 - Does not support storage of the private key or certification path.

Certificate Templates

- **Certificate templates** are used to
 - Simplify the task of administering a CA by allowing an administrator to identify, modify, and issue certificates preconfigured for selected tasks.
 - Establish a set of rules and format for certificate enrollment that are applied to incoming certificate requests.
- The Certificate Templates snap-in enables you to view and modify the properties for each certificate template and copy and modify certificate templates.

Certificate Templates

- When accessing the Certificate Templates console, there are several preconfigured certificate templates that act as a starting point:
 - **Basic EFS (Template Version 1):** Used by Encrypting File System (EFS) to encrypt data.
 - **Computer Template Version 1:** Allows a computer to authenticate itself to the network.
 - **EFS Recovery Agent (Template Version 1):** Allows the subject to decrypt files that were previously encrypted with EFS.
 - **IPSEC (Template Version 1):** Used by IPsec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied to the request.
 - **Smartcard Logon (Template Version 1):** Allows the holder to authenticate using a smart card.
 - **User (Template Version 1):** Used by users for email, EFS, and client authentication.
 - **Web Server (Template Version 1):** Proves the identity of a web server.

Certificate Template Schema Versions

Version 1 certificate templates

- Support general certificate needs and provide compatibility with clients and issuing CAs running Windows 2000 operating systems or later.
- Are installed by default during CA setup and cannot be deleted.
- Have only one property that can be modified—the set of assigned permissions that control access to the template.

Version 2 certificate templates

- Introduced in Windows Server 2003.
- Can be configured by an administrator to control the way certificates are requested, issued, and used.
- Provide support for certificate auto-enrollment.

Certificate Template Schema Versions

Version 3 certificate templates

- Introduced with Windows Server 2008.
- Support Suite B cryptographic algorithms.
 - Suite B was created by the U.S. National Security Agency to specify cryptographic algorithms that must be used by U.S. government agencies to secure confidential information.

Version 4 certificate templates

- Introduced with Windows Server 2012.
- Allow administrators to separate features supported by operating system version by adding a Compatibility tab to the certificate template Properties tab.
- Support both Cryptographic Service Providers (CSPs) and Key Storage Providers (KSPs).
- Can also be configured to require renewal with a same key.

Certificate Template Properties

- When you access the properties of a certificate template, you have the following tabs:
 - **General:** Specifies the template display name and template name. It allows you to modify the validity period and the renewal period and whether the certificate is published in Active Directory.
 - **Compatibility:** Used to specify the earliest operating system that can use a certificate.
 - **Request Handling:** Specifies the purpose of the digital certificates and gives some control over the certificates made with this template.
 - **Superseded Templates:** Specifies which certificate template the current template will replace.

Certificate Template Properties

- **Extensions:** Specifies the application policies, basic constraints, issuance policies, and key usage.
- **Security:** Specifies whether you can access and use a certificate template.
- **Server:** Allows an administrator not to store certificates, requests, or revocation information in the CA database.
- **Cryptography:** Specifies the minimum key size and which providers can be used.
- **Subject Name:** Specifies what Subject name is used in the certificate.
- **Issuance Requirements:** Specifies if a certificate has to be approved, the number of authorized signatures, and what is required for reenrollment.

Certificate Template Properties

Properties of New Template

Subject Name	Server	Issuance Requirements	
Superseded Templates	Extensions	Security	
Compatibility	General	Request Handling	Cryptography

Template display name:
Copy of Web Server

Template name:
Copy of Web Server

Validity period: 2 years

Renewal period: 6 weeks

Publish certificate in Active Directory

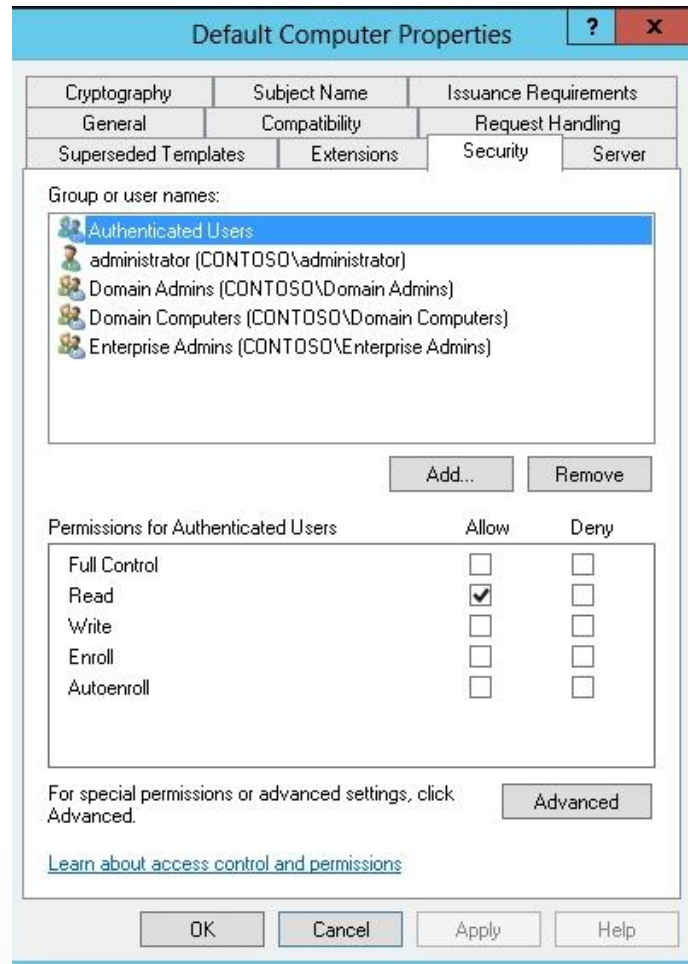
Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

Certificate Template Permissions

- To configure certificate template permissions, you need to define the Discretionary Access Control List (DACL) for each certificate template in the Security tab.
- The permissions that are assigned to a certificate template define which users or groups can read, modify, enroll, or auto-enroll for that certificate template.

Certificate Template Permissions



Deploying Certificates

- The available methods for a user or computer to enroll for a certificate include:
 - Manual enrollment
 - CA Web enrollment
 - Enrollment on behalf (enrollment agent)
 - Auto-enrollment

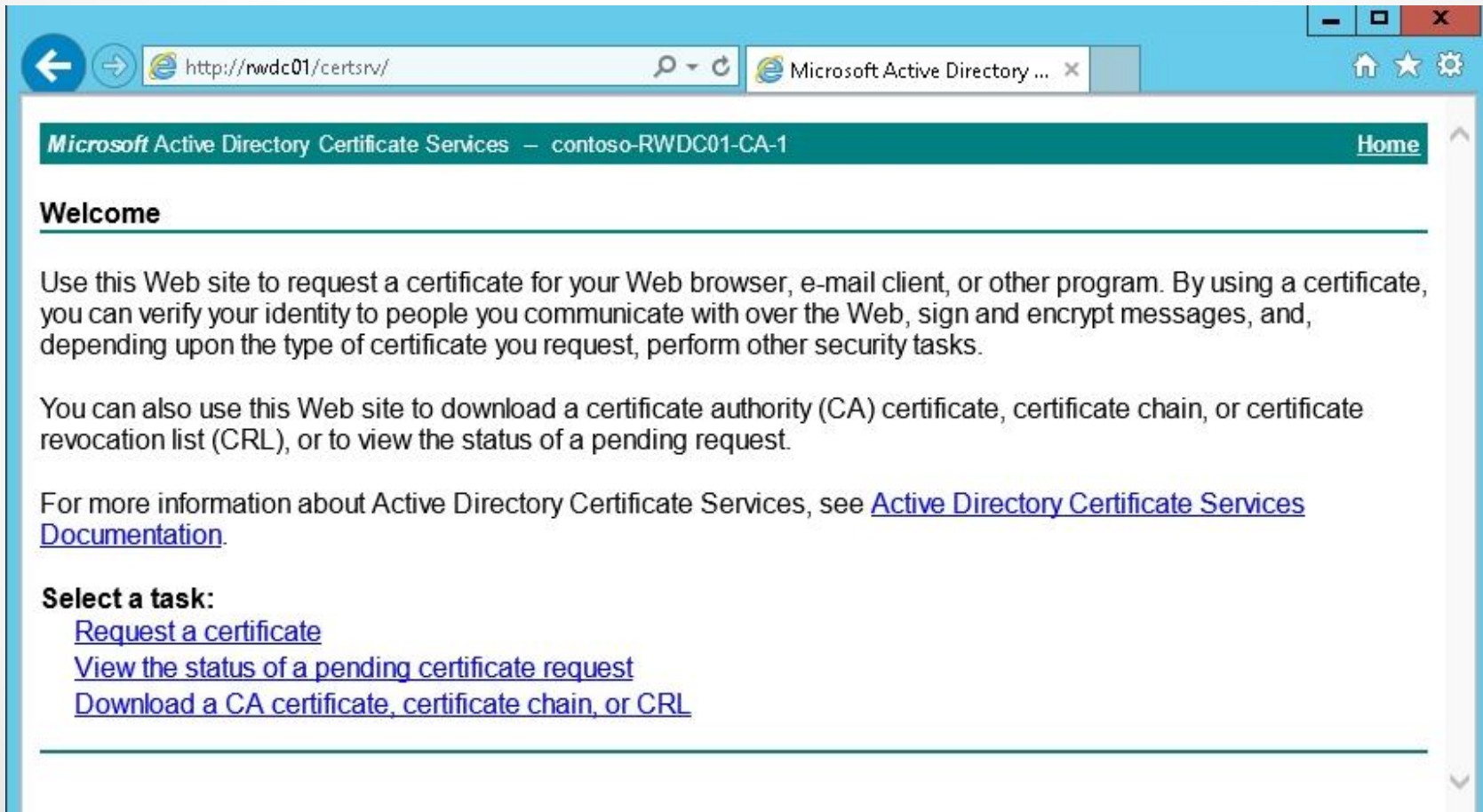
Manual Enrollment

- When you use **manual enrollment**, you create a private key and a certificate request is generated on a device such as a web service or a computer.
- The request is sent to the CA to generate the certificate.
- The certificate is sent back to the device for installation.
- You typically use manual enrollment when the device does not support auto-enrollment, you do not want to wait for auto-enrollment to be applied, or the certificate is not available through auto-enrollment.

CA Web Enrollment

- The **CA Web enrollment** uses a website on a CA to obtain certificates. The website uses Internet Information Server (IIS), and the AD CS web enrollment role has been installed and configured.
- The URL to make a request is `https://<servername>/certsrv`. Like with manual enrollment, CA Web enrollment is used on devices that do not support auto-enrollment or when you do not want to wait for auto-enrollment to be applied.

Web Enrollment Page



The screenshot shows a web browser window with the address bar containing <http://rwdc01/certsrv/>. The page title is "Microsoft Active Directory Certificate Services - contoso-RWDC01-CA-1". The page content includes a "Welcome" section, a paragraph explaining the purpose of the site, a paragraph about downloading certificates, and a "Select a task:" section with three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

Microsoft Active Directory Certificate Services – contoso-RWDC01-CA-1 [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Web Enrollment Page

The screenshot shows a web browser window with the URL `https://rwdc01/certsrv`. The page title is "Microsoft Active Directory Certificate Services - contoso-RWDC01-CA-1". The main heading is "Advanced Certificate Request".

Certificate Template:
User

Key Options:
 Create new key set Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0
Key Usage: Exchange
Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512 1024 2048 4096 8192 16384)
 Automatic key container name User specified key container name
 Mark keys as exportable
 Enable strong private key protection

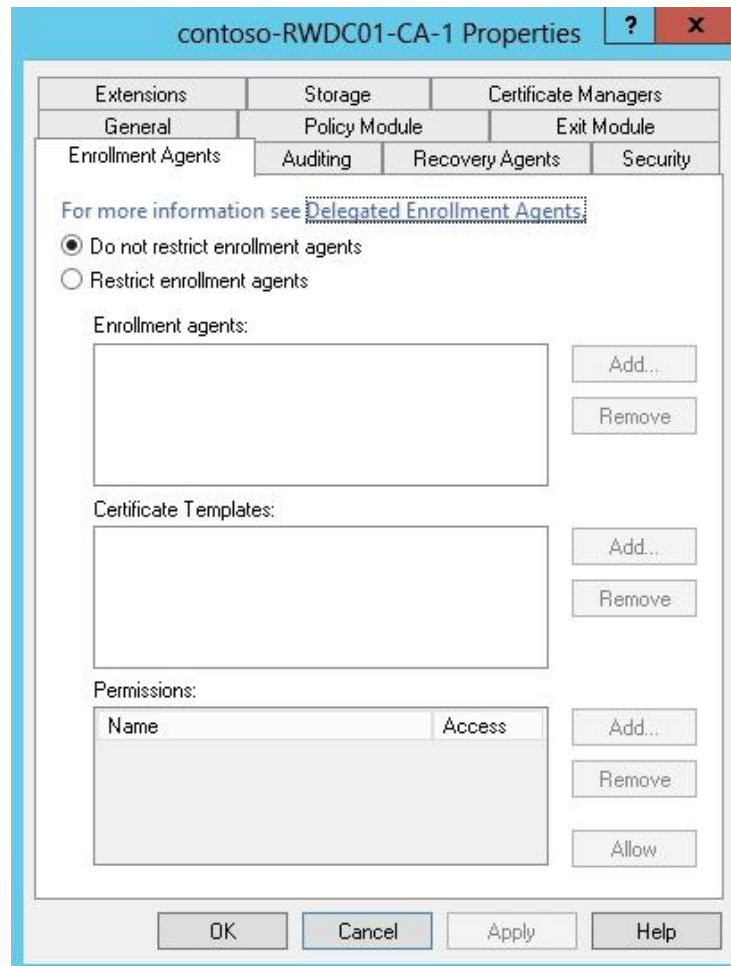
Additional Options:
Request Format: CMC PKCS10
Hash Algorithm: sha1
Only used to sign request.
 Save request
Attributes: [Empty list box]
Friendly Name: [Empty text box]

Submit >

Enrollment Agents

- When you use **enrollment on behalf (enrollment agent)**, the CA administrator creates an enrollment agent account for the user.
- The user with enrollment agent rights can then enroll for certificates on behalf of other users such as when the administrator needs to preload logon certificates on new employees' smart cards.
- The **restricted enrollment agent** allows you to limit the permissions for users (usually administrators and help desk personnel) who are designated as enrollment agents to enroll for smart card certificates on behalf of other users.

Enrollment Agents



Auto-Enrollment

- Most certificates will be assigned through **auto-enrollment**, which is deployed using group policies, specifically
 - *Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Services Client—Auto-Enrollment*
 - *User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Services Client—Auto-Enrollment.*
- However, auto-enrollment can be applied only to enterprise CA (not stand-alone CA), and you have to deploy schema template version 2 or higher.
- In addition, the user needs Read, Enroll, and Auto-enroll permissions for the certificate to be deployed.

Credential Roaming

- **Credential roaming** allows user certificates and private keys to be stored in Active Directory.
- When using credential roaming, the certificates and keys are downloaded when a user logs on, and if desired, the certificate and keys are removed when the user logs off.
- The advantage of credential roaming is that the certificate and key will follow the user no matter which computer the user logs on to.
- Credential roaming is supported in Windows 7 and newer Windows operating systems.
- To enable credential roaming, use the following settings in a GPO User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Credential Roaming.

Credential Roaming

- Credential roaming is triggered during the following operations:
 - Logging on and logging off
 - Locking and unlocking the workstation
 - Updating the group policy cycle (or forcing an update by typing the gpupdate command)
 - Running the regular update cycle (eight hours by default)
 - Using the command `certutil -user -pulse`

Network Device Enrollment Service (NDES)

- The Network Device Enrollment Service (NDES) is the Microsoft implementation of Simple Certificate Enrollment Protocol (SCEP), which is used for network devices such as switches and routers to enroll for an X.509 digital certificate from a CA.
- For example, if you want to use port security based on 802.1x for your switches and access points, or if you need SSH to connect to a switch or router, you can use NDES to install certificates using SCEP.

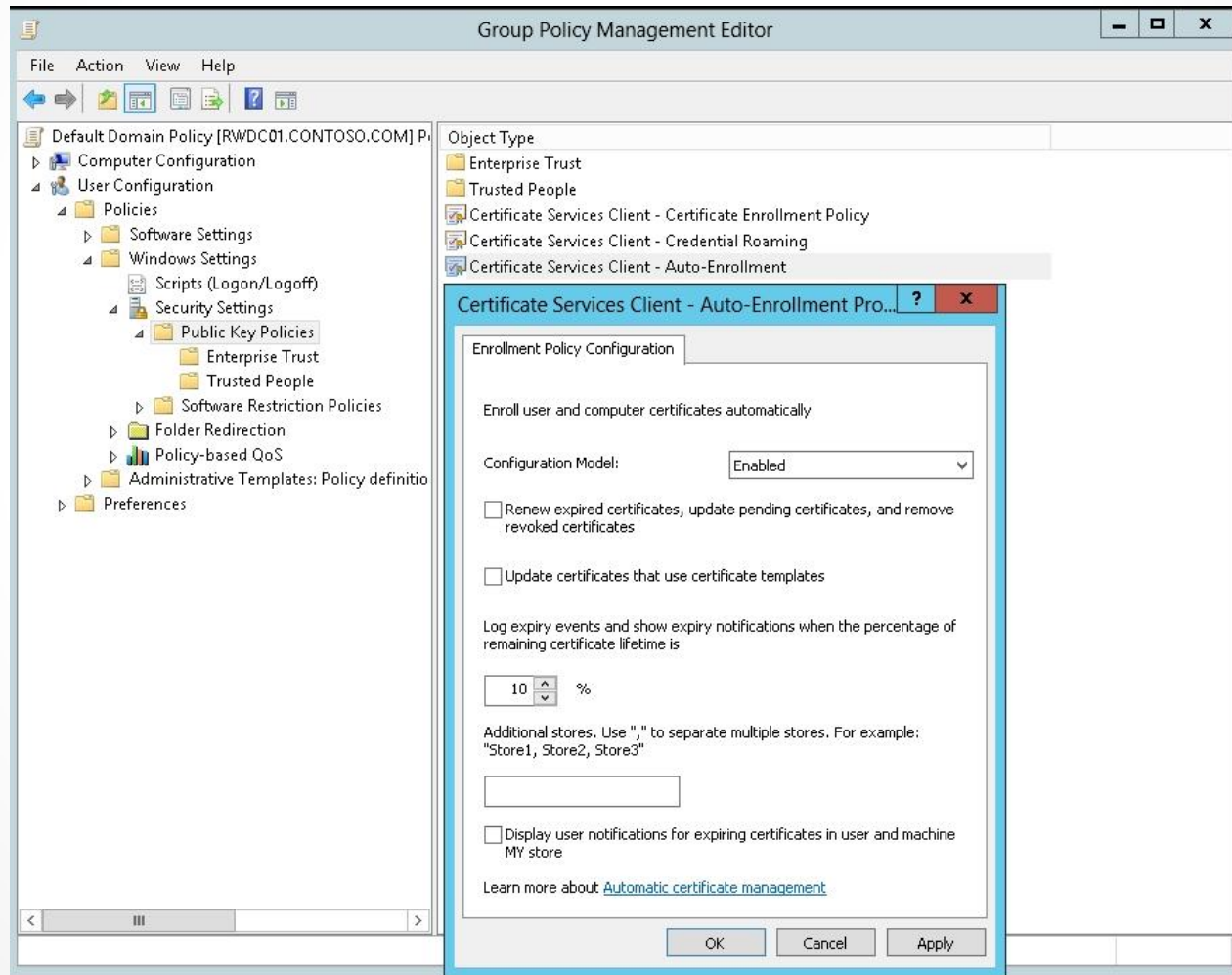
Certificate Renewal

- Every certificate has a validity period and a finite life.
- At the end of the validity period, the certificate is no longer considered acceptable, and the certificate will have to be renewed.
- Of course, it is always best to renew the certificate before the certificate actually expires.

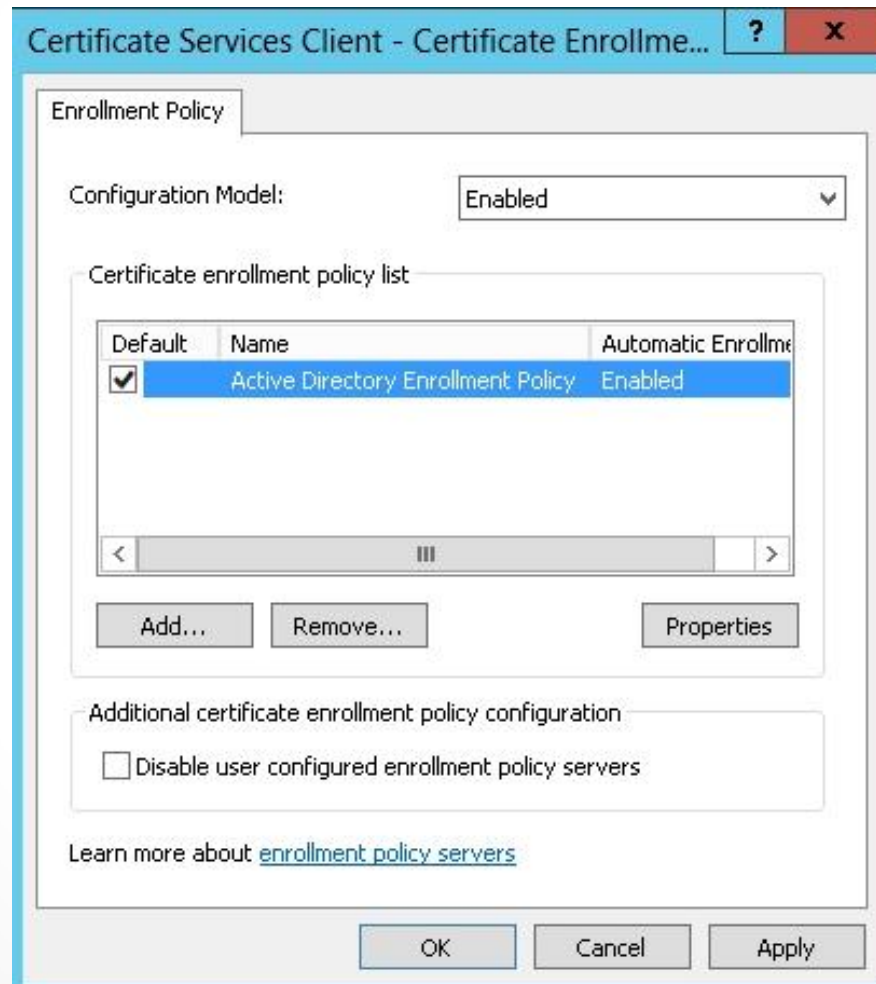
Certificate Enrollment and Renewal

- You can use a group policy object (GPO) to perform auto-enrollment of certificates and the renewal of certificates.
- Remember that auto-enrollment can be used only with enterprise CA and when you have been deploying schema template version 2 or higher.
- In addition, the user needs Enroll and Auto-enroll permissions for the certificate to be deployed.
- You can use the Default Domain Policy to install certificates for users and computers.
- However, for more control, you can use a new GPO.
- For example, with a different GPO, you can assign certificates to specific OUs and use filtering.

Auto-Enrollment Policy



Certificate Enrollment Policy



Key Archival and Recovery

- Because certificates often provide keys to the kingdom, you do not want to lose the keys. Therefore, you need to provide key archival and recovery when needed.
- To recover lost keys, use a key archival and recovery agent.
- You can also use automatic or manual key archival and key recovery methods to ensure that you can gain access to data in the event that your keys are lost.
- It should also be emphasized that restoring a key, does not provide data recovery.
- The restored key provides the ability to read a restored file but you need to use another mechanism (e.g., Windows Backup) to actually back up the encrypted data.

Key Recovery Agent (KRA)

- To recover private keys, you need to archive (or back them up). Then you use a **Key Recovery Agent (KRA)**, which is a designated user who is able to retrieve the original certificate, private key, and public key that was used to encrypt the data from the CA database.
- Similar to setting up an EFS recovery agent, you can apply a key archival in a version 2 certificate template, which then makes the CA store the subject's private key in the CA database as certificates are requested.
- Then during the key recovery process, the KRA retrieves the encrypted file containing the certificate and private key from the CA database and returns the certificate and private key to the user.

Key Recovery Agent (KRA)

- To perform key archival, you must
 1. Configure the KRA certificate template.
 2. Configure certificate managers.
 3. Enable KRA.
 4. Configure user templates.

Lesson Summary

- A digital certificate is like an electronic identification card used to certify the online identity of individuals, organizations, and computers.
- The digital certificate contains a person's or organization's name, a serial number, an expiration date, a copy of the certificate holder's public key (used for encrypting messages and creating digital signatures), and the digital signature of the certificate authority (CA) that assigned the certificate so that recipients can verify that the certificate is real.
- Certificate templates are used to simplify the task of administering a CA by allowing an administrator to identify, modify, and issue certificates preconfigured for selected tasks.

Lesson Summary

- Active Directory Certificate Services (AD CS) provides four schema versions of certificate templates.
- To support auto-enrollment, you need to use the Version 2 certificate template schema version or higher.
- To configure certificate template permissions, you need to define the Discretionary Access Control List (DACL) for each certificate template in the Security tab.

Lesson Summary

- The available methods for a user or computer to enroll for a certificate include: manual enrollment, CA Web enrollment, enrollment on behalf (enrollment agent), and auto-enrollment.
- The CA Web enrollment uses a website on a CA to obtain certificates. The website uses Internet Information Server (IIS) and the AD CS web enrollment role has been installed and configured.
- When you use enrollment on behalf (enrollment agent), the CA administrator creates an enrollment agent account for the user. The user with enrollment agent rights can then enroll certificates on behalf of other users such as when the administrator needs to preload logon certificates on new employees' smart cards.
- Most certificates will be assigned through auto-enrollment, which is deployed using group policies.

Lesson Summary

- Credential roaming allows user certificates and private keys to be stored in Active Directory.
- The Network Device Enrollment Service (NDES) is the Microsoft implementation of Simple Certificate Enrollment Protocol (SCEP), which is used for network devices such as switches and routers to enroll for an X.509 digital certificate from a CA.

Lesson Summary

- Every certificate has a validity period and a finite life. At the end of the validity period, the certificate is no longer considered acceptable, and the certificate has to be renewed. Of course, it is always best to renew the certificate before the certificate actually expires.
- To recover private keys, you need to archive them (or back them up). Then you use a Key Recovery Agent (KRA), which is a designated user who is able to retrieve the original certificate, private key, and public key used to encrypt the data from the CA database.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.