To create a new certificate template

1. Open the Certificate Templates snap-in.
2. Right-click the template to copy from, and then click **Duplicate Template**.
3. Choose the minimum version of CA that you want to support.
4. Type a new name for this certificate template.
5. Make any necessary changes, and click **OK**.

To delete a certificate template

1. Open the Certificate Templates snap-in.
2. Right-click the template you want to delete, and then click **Delete**.
3. Click **Yes** to confirm that you want to delete the template.

Install the Certificate Templates Snap-In

4 out of 9 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

The Certificate Templates snap-in allows you to view and manage critical information about all the certificate templates in a domain.

Important fields in the Certificate Templates snap-in include:

- **Template Display Name**. This field describes the purpose of the certificate. When an organization creates a custom certificate template, it may be useful to use a naming convention that helps administrators identify the certification authority (CA) or portion of the organization associated with the template.

- **Minimum Supported CAs**. The configurable options in Windows-based certificate templates differ based on the operating system version. Therefore, not all certificate templates are supported by all Windows Server–based CAs.

- **Version**. If certificate template configurations evolve over time, the ability to track version information becomes important for compatibility and support.

You must be a local administrator to install the Certificate Templates snap-in and a member of **Domain Admins** to use the Certificate Templates snap-in. For more information, see Implement Role-Based Administration.

To install the Certificate Templates snap-in

1. Click **Start**, click **Run**, and then type **mmc**.

2. On the **File** menu, click **Add/Remove Snap-in**.
3. On the **Add and Remove Snap-ins** dialog box, double-click the **Certificate Templates** snap-in to add it to the list. Click **OK**.

By default, the Certificate Templates snap-in is installed automatically when a CA is installed on a server. The Certificate Templates snap-in can be installed on a different server by using Server Manager to install Active Directory Certificate Services (AD CS) tools.

You must be local administrator to install Remote Server Administration Tools. You must be a member of **Domain Admins** to access and administer certificate templates for a domain. For more information, see Implement Role-Based Administration.

To administer certificate templates from a remote server

1. Open Server Manager.
2. Under **Features Summary**, click **Add Features**.
3. Expand **Remote Server Administration Tools** and **Role Administration Tools**.
4. Select the **Active Directory Certificate Services** check box, click **Next**, and then click **Install**.
5. When the installation process is finished, click **Close**.
6. Click **Start**, type **mmc**, and press ENTER.
7. On the **File** menu, click **Add/Remove Snap-in**.
8. Click the **Certificate Templates** snap-in, click **Add**, verify that the domain controller hosting the certificate templates you want to manage is selected, and then click **OK**.

You can use the Certificate Templates snap-in to manage certificate templates in a different domain.

You must be a domain or enterprise administrator for the other domain to complete this procedure. For more information, see Implement Role-Based Administration.

To manage certificate templates in a different domain

1. Right-click the **Certificate Templates** snap-in, and click **Connect to another writable domain controller**.
2. To type the name of a different domain, click **Change**. To select a different domain controller for the existing domain, click **Select a Writable Domain Controller**.
3. If you have previously selected an alternate domain controller, you can revert to the original domain controller by clicking **Default Writable Domain Controller**.

Upgrade Existing Templates

This topic has not yet been rated - Rate this topic

Applies To: Windows Server 2008 R2

When you upgrade a certification authority (CA), you may need to update the Active Directory schema to support new certificate template attributes. For more information about updating the Active Directory schema with Adprep.exe, see the Command Line Reference (http://go.microsoft.com/fwlink/?LinkID=20331).

In addition, you need to upgrade the certificate templates to include and configure these attributes. Upgrading the certificate templates applies the proper security permissions on the existing certificate templates and installs any new certificate templates that are available.

If you do not perform this procedure before upgrading your CAs to Windows Server 2008 R2, you will be prompted when opening the Certificate Templates snap-in. If this procedure has already been performed in your enterprise, you will not receive a prompt when you open Certificate Templates.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure.

To install new templates and upgrade existing templates

1. Open the Certificate Templates snap-in.
2. When prompted to install new certificate templates, click **OK**.

Rename a Certificate Template

0 out of 1 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

The names of custom certificate templates can be changed by an administrator. The names of default certificate templates cannot be changed. Use the **Change Names** dialog box to change the template name and the template display name.

The template name is the common name attribute of the certificate template object in Active Directory Domain Services (AD DS), and only that template object is updated when the template name is changed. If the modified template was previously published to issuing certification authorities (CAs) or added to a superseded templates list, then those actions must be repeated to maintain the consistency of the public key infrastructure (PKI) environment.

To change a certificate template name

1. On the CA, open the Certificate Templates snap-in.
2. Click the certificate template you want to modify. On the **Action** menu, click **Change Names**.

   Note

When a default certificate is selected, **Change Names** is not displayed. The names of default certificate templates cannot be changed.

3. Type a new name in the **Template name** box or the **Template display name** box, or both.
4. Click **OK** to save changes.

Certificate Template General Properties

This topic has not yet been rated - Rate this topic

Applies To: Windows Server 2008 R2

The **General** tab contains validity and renewal information for certificates that will be issued based on a certificate template.

The default validity and renewal period settings for certificates issued by Active Directory Certificate Services (AD CS) are designed to meet most security needs. However, you might want to specify different validity and renewal settings, such as shorter lifetime or renewal periods for certificates that are used by certain user groups.

Membership in **Domain Admins** or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To modify the validity or renewal period for a certificate template

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template that you want to change, and then click **Properties**.
3. On the **General** tab, check the current validity period and renewal period values, modify them as needed, and then click **Apply**.

The **Publish certificate in Active Directory** option determines whether information about the certificate template will be made available throughout the enterprise.

The **Do not automatically re-enroll if a duplicate certificate exists in Active Directory** option is applied when the subject attempts to enroll for a certificate based on this template from a computer running Windows XP or later. With this option, certificate autoenrollment will not submit a re-enrollment request if a duplicate certificate exists in Active Directory Domain Services (AD DS). This allows certificates to be renewed but prevents multiple duplicate certificates from being issued.

The **Smart card certificate keys** option enables the existing key to be used if a new key cannot be created during renewal of a smart card certificate. This option helps prevent smart card certificate renewal failures that could result when a smart card runs out of disk space.

Membership in **Domain Admins** or **Enterprise Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To configure certificate publishing in AD DS

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template that you want to change, and then click **Properties**.
3. On the **General** tab, select the appropriate Active Directory setting, and then click **Apply**.

Certificate Template Extensions

1 out of 1 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

A certification authority (CA) processes each certificate request by using a defined set of rules. Certificate templates can be customized with a number of extensions that regulate their use. These extensions can include:

- **Issuance policies**. An issuance policy (also known as an enrollment or certificate policy) is a group of administrative rules that are implemented when issuing certificates. They are represented in a certificate by an object identifier (also known as an OID) that is defined at the CA. This object identifier is included in the issued certificate. When a subject presents its certificate, it can be examined by the target to verify the issuance policy and determine if that level of issuance policy is sufficient to perform the requested action. For more information, see Issuance Requirements.

- **Application policies**. Application policies give you the important ability to decide which certificates can be used for certain purposes. This allows you to issue certificates widely without being concerned that they are misused for an unintended purpose. Application policies are sometimes called extended key usage or enhanced key usage. Because some implementations of public key infrastructure (PKI) applications cannot interpret application policies, both application policies and enhanced key usage sections appear in certificates issued by a Windows Server–based CA. For more information, see Application Policy.

- **Key usage**. A certificate enables the subject to perform a specific task. To help control the usage of a certificate outside its intended purpose, restrictions are automatically placed on certificates. Key usage is a restriction method and determines what a certificate can be used for. This allows the administrator to issue certificates that can only be used for specific tasks or to issue certificates that can be used for a broad range of functions. For more information, see Key Usage.

- **Key archival**. When subjects lose their private keys, any information that was persistently encrypted with the corresponding public key is inaccessible. To help prevent this, key archival allows you to encrypt and archive a subject's keys in the CA database when certificates are issued. If a subject loses its keys, the information can be retrieved from the database and provided to the subject. This allows the encrypted information to be recovered instead of lost. For more information, see Request Handling.

- **Basic constraints**. Basic constraints are used to ensure that CA certificates are only used in certain applications. An example is the path length that can be specified as a basic constraint. A path length defines the number of CAs that are permitted below the current CA. This path length constraint ensures that CAs at the end of this path can only issue end-entity certificates, not CA certificates. For more information, see Basic Constraints.

- **OCSP No Revocation Checking**. This extension appears only in the new OCSP Response Signing certificate template and duplicates derived from this template. It cannot be added to any other certificate templates. This extension instructs the CA to include the OCSP No Revocation Checking (id-pkix-ocsp-nocheck) extension in the issued certificate and not to include the authority information access and certificate revocation list (CRL) distribution point extensions in the certificate. This is because OCSP Response Signing certificates are not checked for revocation status. This extension only applies if the certificate request contains OCSP Response Signing in the enhanced key usage and application policies.

Request Handling

Updated: November 16, 2012

Applies To: Windows Server 2008 R2

The **Request Handling** tab defines the purpose of a certificate template, the supported cryptographic service providers (CSPs), minimum key length, exportability, autoenrollment settings, and whether strong private key protection should be required.

Certificate purpose

The certificate purpose defines the intended primary use of the certificate and can be one of four settings as described in the following table.

Setting	Purpose
Encryption	Contains cryptographic keys for encryption and decryption.
Signature	Contains cryptographic keys for signing data only.

Signature and encryption	Covers all primary uses of a certificate's cryptographic key, including encryption of data, decryption of data, initial logon, or digitally signing data.
Signature and smart card logon	Allows for initial logon with a smart card, and to digitally sign data; it cannot be used for data encryption.

Note

Key archival is only possible if the certificate purpose is set to **Encryption** or **Signature and encryption**.

Archive settings

Certification authorities (CAs) can archive a subject's keys in their databases when certificates are issued. If subjects lose their keys, the information can be retrieved from the database and securely provided to the subjects.

The key archival settings in the following table are defined in the **Request Handling** tab.

Setting	Purpose
Archive subject's encryption private key	If the issuing CA is configured for key archival, the subject's private key will be archived.
Allow private key to be exported	The subject's private key can be exported to a file for backup or transfer to another computer.
Deleting revoked or expired certificates (do not archive)	If a certificate is renewed due to expiration or revocation, the previously issued certificate is removed from the subject's certificate store. By default, this option is not enabled and the certificate is archived.
Include symmetric algorithms allowed by the subject	When the subject requests the certificate, a list of supported symmetric algorithms can be supplied by the subject. This option allows the issuing CA to include those algorithms in the certificate, even if they are not recognized or supported by that server.

User input settings

The **Request Handling** tab also allows several user input settings described in this table to be defined for a certificate template.

Setting	Purpose
Enroll subject without requiring any user input	This option allows autoenrollment without any user interaction and is the default setting for both computer and user certificates.
Prompt the user during enrollment	This option only affects autoenrollment. It does not prompt during manual enrollment. By disabling this option, users do not have to provide any input for the installation of a certificate based on the certificate template.
Prompt the user during enrollment and require user input when the private key is used	This option enables the user to set a strong private key protection password on the user's private key when the key is generated and requires the user to use it whenever the certificate and private key are used.

Other version 3 request handling settings

The **Request Handling** tab for version 3 certificate templates has been updated to provide support for the new options available on the **Cryptography** tab, along with other changes. The options are listed in the following table.

Setting	Purpose
Use advanced Symmetric algorithm to send the key to the CA	This option allows the administrator to choose the Advanced Encryption Standard (AES) algorithm to encrypt private keys while they are transferred to the CA for key archival. If this option is selected, the client will use AES-256 symmetric encryption (along with the CA's exchange certificate for asymmetric encryption) to send the private key to the CA for archival. If this option is not selected, the 3DES symmetric algorithm is used. Because key archival is intended for encryption keys (not signing keys), this option is enabled only when the certificate purpose is set to **Encryption**.
Authorize additional service accounts to access the private key	This option allows a custom access control list (ACL) to be defined on the private keys of computer certificates based on any version 3 computer certificate template except the root CA, subordinate CA, or cross-CA templates. A custom ACL is necessary only when a service account that requires access to the private key is not included in the default permissions. The default permissions applied to the private key by the Microsoft certificate enrollment client and software key storage provider include Full Control permission for the Administrators group and the Local System account. Non-Microsoft providers may apply different default permissions and may not support custom ACLs defined by using this option. Refer to your provider's documentation for more information.

Note

This option has replaced the **Add Read permissions to Network Service on the private key** option. In Windows Server 2008 R2, the default permissions applied to the private key of OCSP Response Signing certificates include Read permission for Online Responder service account and Full Control permission for the Administrators group and the Local System account.

For more information about options associated with version 3 certificate templates, see Cryptography.

Other version 2 request handling settings

In addition to key archival settings, you can define general options that affect all certificates based on version 2 certificate templates. The options are listed in the following table.

Setting	Purpose
Minimum key size	This specifies the minimum size, in bits, of the key that will be generated for this certificate.
Cryptographic service providers	This is a list of cryptographic service providers (CSPs) that will be used to enroll certificates for the given template. Selecting one or more CSPs configures the certificate to only work with those CSPs. The CSP must be installed on the client computer for the CSP to be used during enrollment. If a specific CSP is chosen and not available on a client computer, enrollment will fail.

Cryptography

This topic has not yet been rated - Rate this topic

Applies To: Windows Server 2008 R2

The **Cryptography** tab is available for version 3 certificate templates. This tab replaces the cryptographic service provider (CSP) selection dialog box used to select CSPs for version 2 certificate templates. The **Cryptography** tab is used to configure the following properties:

- **Algorithm name**. Select an algorithm that the issued certificate's key pair will support. The list displays only algorithms that support the cryptographic operations required for the certificate

purpose that is selected on the **Request Handling** tab. The following table describes the relationship between the certificate purpose and the available algorithms.

Purpose	Algorithms
Encryption	ECDH_P256 ECDH_P384 ECDH_P521 RSA
Signature	DSA ECDSA_P256 ECDSA_P384 ECDSA_P521 RSA
Signature and encryption	ECDH_P256 ECDH_P384 ECDH_P521 RSA
Signature and smart card logon	ECDH_P256 ECDH_P384 ECDH_P521 RSA

- **Minimum key size**. This option allows you to specify a minimum required size for the keys used with the chosen algorithm. By default, the minimum key length supported on the computer for the chosen algorithm will be used.

- **Providers**. Version 2 templates offer a list of CryptoAPI CSPs, while version 3 templates offer a dynamically populated list of Cryptography Next Generation (CNG) providers. This list is populated with all providers available on the computer that meet the criteria specified by a combination of the following configuration options: **Algorithm name** and **Minimum key size** on the **Cryptography** tab, and **Purpose** and **Allow private key to be exported** on the **Request Handling** tab.

- **Hash algorithm**. This option allows you to choose an advanced hash algorithm. By default, the following algorithms are available: AES-GMAC, MD2, MD4, MD5, SHA1, SHA256, SHA384, and SHA512.

- **Use alternate signature format**. When the RSA algorithm is selected, this check box allows you to specify that certificate requests created for this template include a discrete signature in PKCS #1 V2.1 format.

  Note

  This setting applies to the certificate request only, not the certificate that is issued by the CA

from this template.

Supersede Templates

0 out of 3 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

There may be times when you want to modify the properties of a type of certificate that has already been issued to clients. You can do this by creating an updated certificate template for that certificate purpose and specifying that you want subjects of certificates based on the old template to obtain new certificates based on the new template. This procedure forces subjects to obtain a new certificate before the renewal date specified in the original certificate template.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To supersede templates

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template that you want to change, and then click **Properties.**
3. Click the **Superseded Templates** tab.
4. Click **Add.**
5. Click one or more templates to supersede, and then click **OK**.
6. Make any other changes to the template that you want to include, and click **OK**.

Subject Names

8 out of 17 rated this helpful - Rate this topic

Applies To: Windows 7, Windows Server 2008 R2

The holder of the private key associated with a certificate is known as the subject. This can be a user, a program, or virtually any object, computer, or service.

Because the subject name can vary greatly depending on who or what the subject is, some flexibility is needed when providing the subject name in the certificate request. Windows can build the subject name automatically from subject information stored in Active Directory Domain Services (AD DS) or the subject name can be supplied manually by the subject (for example, by using certificate enrollment Web pages to create and submit a certificate request).

Enterprise certification authorities (CAs) include the Certificate Templates snap-in to configure certificate templates. Use the **Subject Name** tab on the certificate template properties sheet to configure subject name options.

Supply in the request

When the **Supply in the request** option is selected, the **Use subject information from existing certificates for autoenrollment renewal requests** option is available to simplify the task of adding the subject name to the certificate renewal request and to allow computer certificates to be renewed automatically. Subject information from existing certificates is not used for automatic renewal of user certificates.

The **Use subject information from existing certificates for autoenrollment renewal requests** option causes the certificate enrollment client to read subject name and subject alternative name information from an existing computer certificate based on the same certificate template when creating renewal requests automatically or using the Certificates snap-in. This applies to computer certificates that are expired, revoked, or within their renewal period.

Build from AD DS

When the **Build from this Active Directory information** option is selected, the following additional options can be configured.

Subject name format

Setting	Description
Common name	The CA creates the subject name from the common name (CN) obtained from AD DS. This should be unique within a domain but might not be unique within an enterprise.
Fully distinguished name (DN)	The CA creates the subject name from the fully distinguished name obtained from AD DS. This ensures that the name is unique within an enterprise.
Include e-mail name in subject name	If the E-mail name field is populated in the Active Directory user object, this e-mail name will be included with either the common name or fully distinguished name as part of the subject name.
None	A name value is not required for this certificate.

Include this information in alternate subject name

Setting	Description
E-mail name	If the E-mail name field is populated in the Active Directory user object, this e-mail name will be used.
DNS name	This is the fully qualified domain name (FQDN) of the subject that requested the certificate. This is most frequently used in computer

	certificates.
User principal name (UPN)	The user principal name is part of the Active Directory user object and will be used.
Service principal name (SPN)	The service principal name is part of the Active Directory computer object and will be used.

Certificate Template Server

This topic has not yet been rated - Rate this topic

Applies To: Windows Server 2008 R2

High-volume certificate issuance scenarios such as Network Access Protection (NAP) deployments with Internet Protocol security (IPsec) enforcement create unique public key infrastructure (PKI) needs. To address these needs, the following options introduced in Windows Server 2008 R2 can be used to configure certificate templates for use by high-volume certification authorities (CAs). These options are available on the **Server** tab of a certificate template's property sheet.

Do not store certificates and requests in the CA database

Certificates issued in high-volume scenarios typically expire within hours of being issued, and the issuing CA processes a high volume of certificate requests. By default, a record of each request and issued certificate is stored in the CA database. A high volume of requests increases the CA database growth rate and administration cost.

The **Do not store certificates and requests in the CA database** option configures the template so that the CA processes certificate requests without adding records to the CA database.

Important

The issuing CA must be configured to support certificate requests that have this option enabled. On the issuing CA, run the following command: **CertUtil.exe –SetReg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS**.

Do not include revocation information in issued certificates

Revocation of certificates by some high-volume CAs is not beneficial because the certificates typically expire within hours of being issued.

The **Do not include revocation information in issued certificates** option configures the template so that the CA excludes revocation information from issued certificates. This prevents checking revocation status during certificate validation and reduces validation time.

Note

This option is recommended whenever the **Do not store certificates and requests in the CA database** option is used.