ADCS – Manage PKI Certificate Templates

itpro.outsidesys.com/2018/03/21/adcs-manage-pki-certificate-templates

Certificate Templates

Microsoft created certificate templates for you to use as a starting point. They are meant to be duplicated and configured for your specific needs. All Enterprise CA servers issue certificates based on one or more of the certificate templates. You cannot create a new template from scratch.

There is only one set of templates, and they are stored in Active Directory for the entire forest. Each Enterprise CA server in the forest uses the same set of templates, regardless of domain or subdomain membership. However, this doesn't mean you have to enable the same set of templates on all Enterprise CA servers. Instead, you can enable different templates on each Enterprise CA server.

If the same template is enabled on more than one Enterprise CA server, clients will choose the first one to respond to an RPC ping. If the Enterprise CAs are running Server 2012+ and the clients are running Windows 8+, you can implement AD site costs to determine which Enterprise CA the client should use.

Here are some certificate template best practices:

- You should always duplicate an existing template, and then modify the duplicate. Some of the default, out-of-the-box templates can be modified, but this is not recommended. The only exception to this is modifying a default template's security settings. In some circumstances, this is ok.
- When duplicating templates, add a prefix, like your company's name or its abbreviation, to the beginning of the name. This keeps your custom templates grouped together, and makes it easy to recognize them as being duplicated.
- If your organization has a PEN (Private Enterprise Number), consider using it as an OID prefix in your custom templates.
- Always use security groups to control if end-entities (users & computers) are allowed to use a template to enroll (or auto-enroll) for a certificate.
- By default, Enterprise Admins (and Domain Admins in the root tree) can manage the certificate templates. If you don't want them to have this ability, create a security group, and use role separation to give group members the permissions to manage the templates.
- Whenever duplicating or modifying a template, always review the Security tab before saving and enabling it on an Enterprise CA server. You should always verify that the template is only available to the groups of users or computers that will use it.

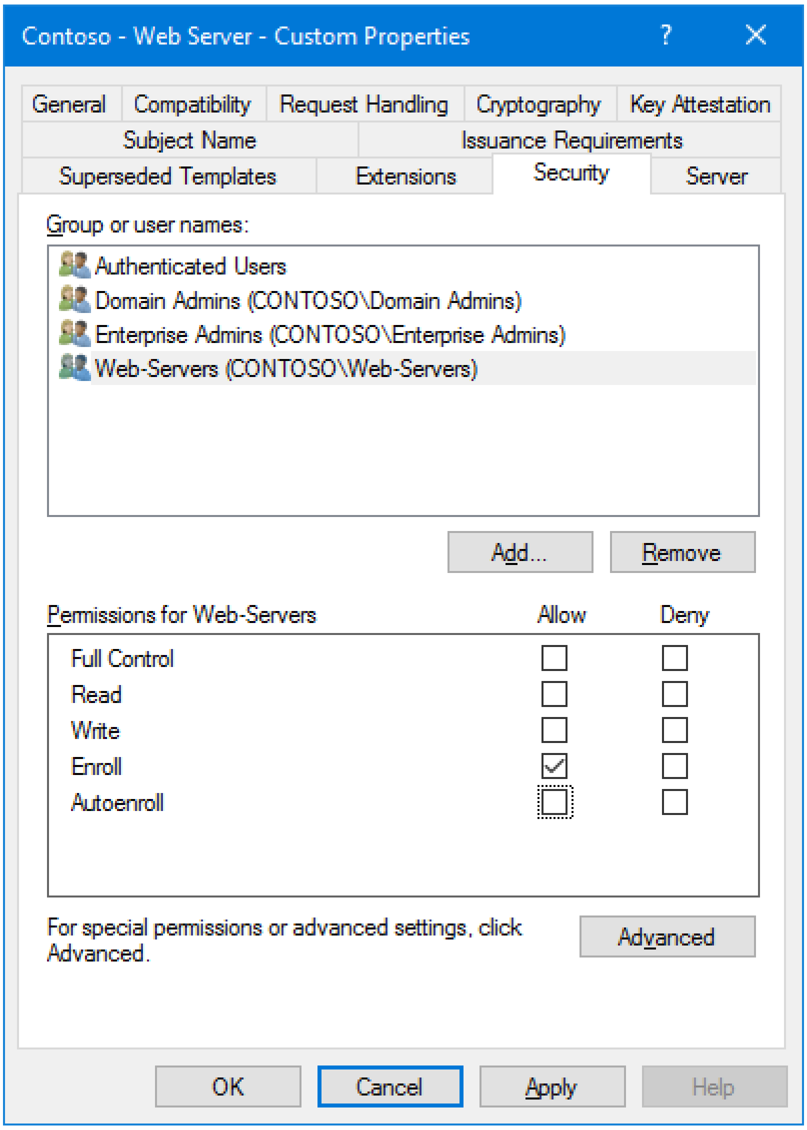
- Do not publish the Subordinate Certification Authority or Root Certification Authority templates on your Enterprise CA servers. If those templates are listed in the “Certificate Templates” folder of the CA Server console, remove them. If you are using Enterprise CA servers in a multi-tier PKI architecture, only publish those templates when you need them.

The Security Tab

This is by far the most important part of a template’s properties. Improperly configuring the security settings of a template could allow all users or computers to enroll for a certificate they shouldn’t have. This is especially true when a template allows a requester to create their own subject name or subject alternate name for a certificate — you don’t want someone creating a wildcard certificate.

Here are some things to keep in mind:

- The permissions for Authenticated Users should only allow Read (nothing else), and Authenticated Users should never be removed from the template. This allows all users and computers to read the template in Active Directory including your Enterprise CA servers.
- Use security groups to assign Enroll or Autoenroll permissions whenever possible. It makes managing the templates much easier.
- To enroll a certificate, a user or computer must be assigned Enroll permissions, either directly or through group membership. You do not need to allow Read permissions. That is provided with the Authenticated Users group.
- To enroll a certificate with auto-enrollment, a user or computer must be assigned both Enroll and Autoenroll permissions.
- Do not give Authenticated Users Enroll or Autoenroll permissions. To allow all users or computers to enroll or auto-enroll a certificate, add the Domain Users or Domain Computers groups.
- To modify a certificate template, a user must be assigned Write permissions.
- Under normal circumstances, Domain Admins & Enterprise Admins don’t need the Enroll permission. Consider removing this permission from a duplicated template.
- When you duplicate a template, your user account may be added to the Security tab. If your user account already has permissions via another security group, remove your user account.



Group or user names:

- Authenticated Users
- Domain Admins (CONTOSO\Domain Admins)
- Enterprise Admins (CONTOSO\Enterprise Admins)
- Web-Servers (CONTOSO\Web-Servers)

Permissions for Web-Servers	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

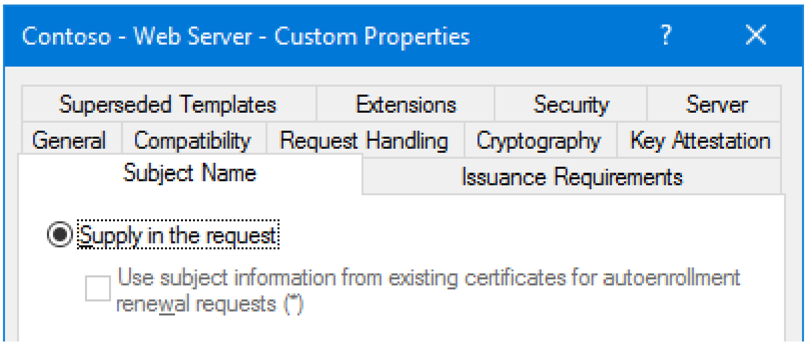
For special permissions or advanced settings, click Advanced.

The Subject Name Tab

Any certificate template that allows the Subject Name to be supplied in the request should be tightly controlled. This is especially true when the template is configured to allow the private key to be exported. You don't want someone creating a wildcard certificate and exporting it for use elsewhere.

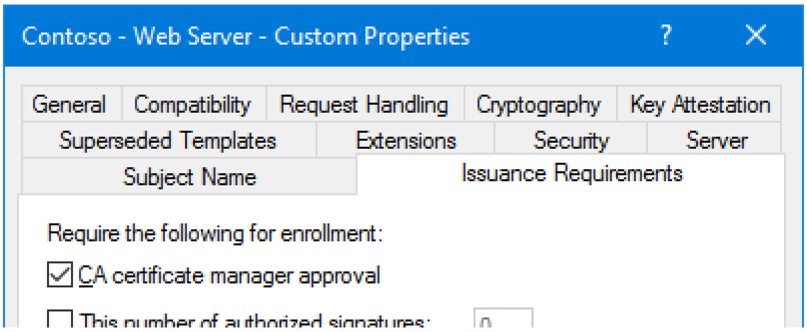
Additionally, on the Issuance Requirements tab, you should enable CA Certificate Manager Approval, and on the Security tab, make sure you're not giving all computers and/or users in your organization the ability to request a certificate using the template.

If you enable CA Certificate Manager Approval, give the computer or user accounts both Enroll & Autoenroll permissions. This allows for retrieval of the certificate via the Certificates MMC after it has been approved/issued.



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)



Require the following for enrollment:

☑ CA certificate manager approval

□ This number of authorized signatures: 0