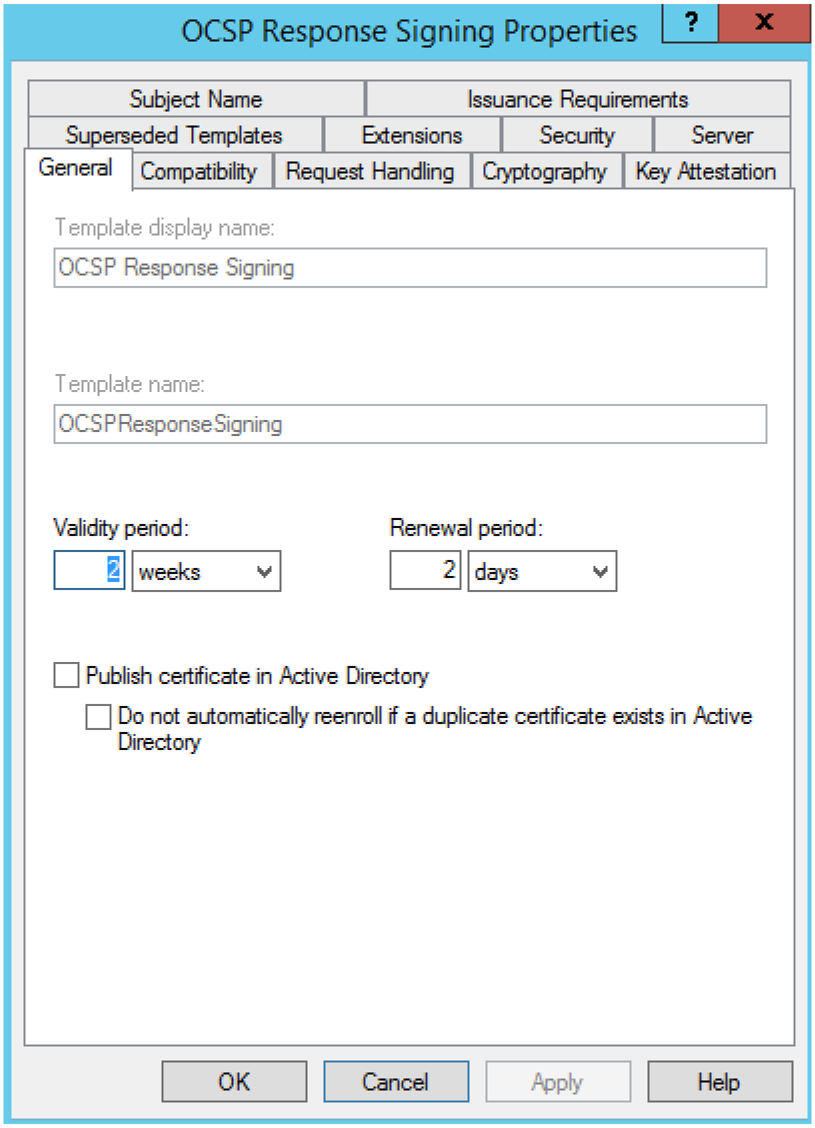
Managaing Certificate Templates

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

Click on the properties of a certificate to view the different tabs and fields for each tab.



Template display name: OCSP Response Signing

Template name: OCSPResponseSigning

Validity period: 2 weeks

Renewal period: 2 days

□ Publish certificate in Active Directory

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

You must be a local administrator to install the Certificate Templates snap in and a member of Domain Admins to use the Certificate Templates snapin.

To install the Certificate Templates snap-in.

1. Mmc
2. Add/Remove snap-in
3. Select cerificate templates and add
4. Close snapin

To create a new certificate template

1. Open the Certificate Templates snapin.
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 snapin.

2.Right click the template you want to delete, and then click
Delete

5. 3.Click Yes to confirm that you want to delete the template.
6. **Note:** Prior to Windows Server 2008 R2, only the Enterprise editions of Windows Server supported management of certificate templates. In Windows

Server 2008 R2 and Windows Server 2012, you can also manage certificate templates in the Standard editions.

Certificate Template Versions in Windows Server 2012

The CA in Windows Server 2012 Certification Authority supports four versions of certificate templates.

Certificate templates versions 1, 2 and 3 are legacy from previous versions of Windows Server, while version 4 is new to Windows Server 2012.

Certificate template versions correspond to the Windows Server operating system version. Windows 2000 Server, Windows Server 2003, Windows Server 2008, and Windows Server 2012 correspond to version 1, version 2, version 3, and version 4 respectively.

Aside from corresponding with Windows Server operating system versions, certificate template versions also have some functional differences as follows:

> Windows 2000 Advanced Server operating system provides support for version 1 certificate templates. The only modification allowed to version 1 templates is changing permissions to either allow or disallow enrollment of the certificate template.
>
> When you install an enterprise CA, version 1 certificate

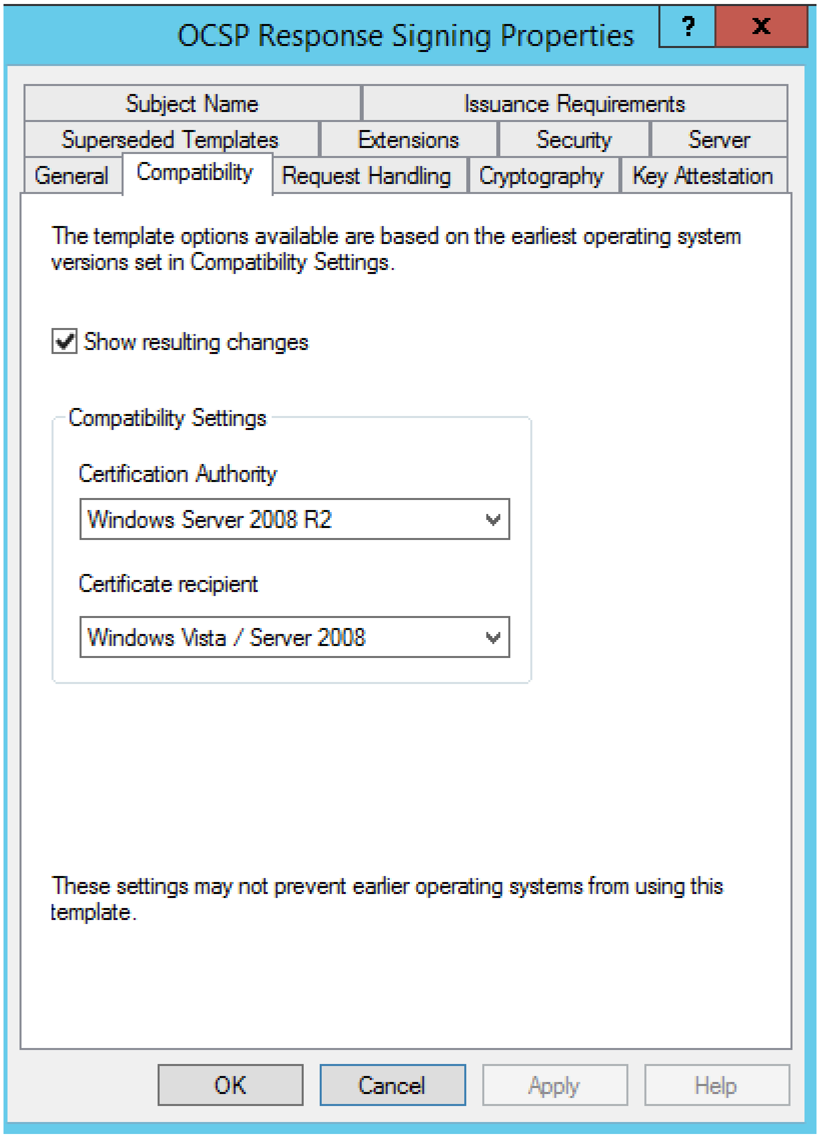
templates are created by default. As of July 13, 2010, Windows 2000 Server is no longer supported by Microsoft.

- Windows Server 2003 Enterprise Edition operating systems provide support for version 1 and version 2 templates. You can customize several settings in the version 2 templates. The default installation provides several preconfigured version 2 templates. You can add version 2 templates based on the requirements of your organization. Alternatively, you can duplicate a version 1 certificate template to create a new version 2 of the template. You can then modify and secure the newly created version 2 certificate template. When new templates are added to a Windows Server 2003 enterprise CA, they are version 2 by default.

- Windows Server 2008 Enterprise operating systems bring support for new, version 3 certificate templates. Additionally, support for version 1 and version 2 is provided. Version 3 certificate templates support several features of a Windows Server 2008 enterprise CA, such as CNG. CNG provides support for Suite B cryptographic algorithms such as elliptic curve cryptography (ECC). In Windows Server 2008 Enterprise, you can duplicate default version 1 and version 2 templates to bring them up to version 3.

Windows Server 2008 provides two new certificate templates by default: Kerberos Authentication and OCSP Response Signing. The Windows Server 2008 R2 operating system version was also able to support certificate templates. When you use version 3 certificate templates, you can use CNG encryption and hash algorithms for the certificate requests, issued certificates, and protection of private keys for key exchange and key archival scenarios.

- **Windows Server 2012 operating systems provide support for version 4 certificate templates, and for all other versions from earlier editions of Windows Server**. **These certificate templates are available only to Windows Server 2012 and Windows 8.** To help administrators separate what features are supported by which operating system version, the Compatibility tab was added to the certificate template Properties tab.



The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

Certification Authority

Windows Server 2008 R2

Certificate recipient

Windows Vista / Server 2008

These settings may not prevent earlier operating systems from using this template.

It marks options as unavailable in the certificate template properties, depending upon the selected operating system versions of certificate client and CA. Version 4 certificate templates also support both CSPs and KSPs. They can also be configured to require renewal with a same key.

> Upgrading certificate templates is a process that applies only in situations where the CA has been upgraded from Windows Server 2008 or 2008 R2 to Windows Server 2012. After the upgrade, you can upgrade the certificate templates by launching the CA Manager console and clicking Yes at the upgrade prompt.

Configuring Certificate Template Permissions

To configure certificate template permissions, you need to define the DACL on the **Security** tab for each certificate template. The permissions that are assigned to a certificate template will define which users or groups can read, modify, enroll, or autoenroll for that certificate template.

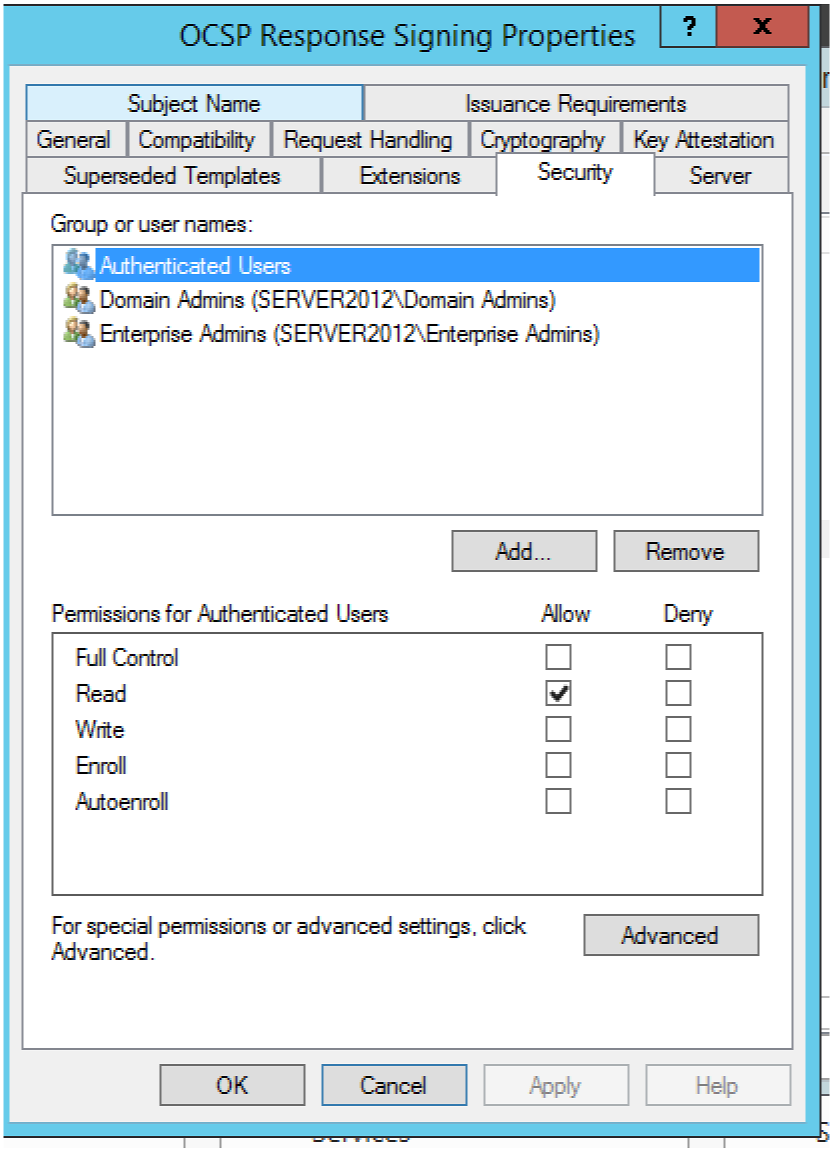
You can assign the following permissions to certificate templates:

- **Full Control**. The **Full Control** permission allows a security principal to modify all attributes of a certificate template, which includes permissions for the certificate template itself. It also includes permission to modify the security descriptor of the certificate template.
- **Read**. The **Read** permission allows a user or computer to view the certificate template when enrolling for certificates. The **Read** permission is also required by the certificate server to find the certificate templates in AD DS.
- **Write**. The **Write** permission allows a user or computer to modify the attributes of a certificate template, which includes permissions assigned to the certificate template itself.

- **Enroll**. The **Enroll** permission allows a user or computer to enroll for a certificate based on the certificate template. However, to enroll for a certificate, you must also have **Read** permissions for the certificate template.
- **Autoenroll**. The **Autoenroll** permission allows a user or computer to receive a certificate through the autoenrollment process. However, the **Autoenroll** permission requires the user or computer to also have both **Read** and **Enroll** permissions for a certificate template.

As a best practice, you should assign certificate template permissions to global or universal groups only. This is because the certificate template objects are stored in the configuration naming context in AD DS. You cannot assign permissions by using domain local groups that are found within an Active Directory domain. You should never assign certificate template permissions to individual user or computer accounts.

As a best practice, keep the **Read** permission allocated to the Authenticated Users group. This permission allocation allows all users and computers to view the certificate templates in AD DS. This permission assignment also allows the CA that is running under the System context of a computer account to view the certificate templates when assigning certificates.



Group or user names:

- Authenticated Users
- Domain Admins (SERVER2012\Domain Admins)
- Enterprise Admins (SERVER2012\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	□	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.