# What's New in Certificate Services in Windows Server 2012

114 out of 141 rated this helpful - Rate this topic

Published: May 13, 2012

Updated: October 1, 2013

Applies To: Windows Server 2012, Windows Server 2012 R2

This document describes new public key infrastructure (PKI) features that available in Windows Server® 2012, Windows Server® 2012 R2, and Windows® 8 and Windows® 8.1.

**Note**
To comment on this content or ask questions about the information presented here, please use our Feedback guidance.

## Role description

Active Directory Certificate Services (AD CS) provides customizable services for issuing and managing public key infrastructure (PKI) certificates used in software security systems that employ public key technologies. The AD CS server role includes six role services:

- Certification Authority (CA)
- Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service

For an overview of AD CS, see the Active Directory Certificate Services (AD CS).

## New and changed functionality

The new and changed functionality in AD CS and PKI includes the following.

## Integration with Server Manager

Server Manager provides a centralized graphical user interface for installing and managing the AD CS server role and its six role services.

**What value does this change add?**

AD CS server role and its role services are integrated into Server Manager, which allows you to install the AD CS role service from the **Manage** menu using **Add Roles and Features**. Once the server role is added, AD CS appears in the Server Manager dashboard as one of the roles that can be managed. This provides you a central location from which you can deploy and manage AD CS and its role services. Further, the new Server Manager allows you to manage multiple servers from one location and you can see the AD CS role services installed on each server, review related events, and perform management tasks on each server. For more information on how the new Server Manager works, see Manage multiple, remote servers with Server Manager.

**What works differently?**

To add the AD CS Server Role, you can use the **Add Roles and Features** link on the **Manage** menu in Server Manager. The AD CS installation flow is similar to that in the previous version, except for the division of the binary installation process and the configuration process. Previously the installation and configuration was a single wizard. In the new installation

experience, you first install the binary files and then you can launch the AD CS Configuration wizard to configure the role services that have already had their binary files installed. To remove the AD CS Server Role, you can use the **Remove Roles and Features** link on the **Manage** menu.

## Deployment and management capabilities from Windows PowerShell®

All AD CS role services can be configured or have their configurations removed by using the AD CS Deployment Windows PowerShell® cmdlets. These new deployment cmdlets are described in the AD CS Deployment cmdlets Overview topic. The AD CS Administration cmdlet allows you to manage the Certification Authority role service. The new administration cmdlets are described in the AD CS Administration cmdlets Overview topic.

**What value does this change add?**

You can use Windows PowerShell to script deployments of any AD CS role service as well as the ability to manage the CA role service.

**What works differently?**

You can use either Server Manager or Windows PowerShell cmdlets to deploy the AD CS role services.

## All AD CS role services run on any version

All Windows Server 2012 and Windows Server 2012 R2 versions allow you to install all of the AD CS role services.

**What value does this change add?**

Unlike previous versions, you can install AD CS roles on any version of Windows Server 2012 or Windows Server 2012 R2.

**What works differently?**

In Windows Server® 2008 R2 operating system the different role services (previously called components) had different operating system version requirements, as described in Active Directory Certificate Services Overview. In Windows Server 2012 or Windows Server 2012 R2, all six of the roles services work as they would on any Windows Server 2012 or Windows Server 2012 R2 version. The only difference is that you will find AD CS with all six role services available for installation on any version of Windows Server 2012 or Windows Server 2012 R2.

## All AD CS role services can be run on Server Core

All six of the Windows Server 2012 and Windows Server 2012 R2 AD CS role services can be installed and run using the Server Core or the Minimal Server Interface installation options.

**What value does this change add?**

Unlike previous versions, you can now run all AD CS role services on Server Core or the Minimal Server Interface installation options in Windows Server 2012 or Windows Server 2012 R2

**What works differently?**

You can now easily deploy AD CS role services using Server Manager or Windows PowerShell cmdlets working locally at the computer or remotely over the network. In addition, Windows Server 2012 or Windows Server 2012 R2 provides multiple installation options that even allow you to install with a graphical user interface and later switch to a Server Core or Minimal Server Interface installation. For more information on installation options, see Windows Server Installation Options

## Support for key-based renewal

Certificate Enrollment Web Services is a feature that was added in Windows® 7 and Windows Server 2008 R2. This feature allows online certificate requests to come from untrusted Active Directory Domain Services (AD DS) domains or even from computers that are not joined to a domain. AD CS in Windows Server 2012 and Windows Server 2012 R2 build on the Certificate Enrollment Web Services by adding the ability to automatically renew certificates for computers that are part of untrusted AD DS domains or not joined to a domain.

**What value does this change add?**

Administrators no longer need to manually renew certificates for computers that are members of workgroups or possibly joined to a different AD DS domain or forest.

**What works differently?**

Certificate Enrollment Web Services continues to function as it did before, but now computers that are outside of the domain can renew their certificates using their existing certificate for authentication.

Additional information, see the topic key-based renewal. There are also two Test Lab Guides that demonstrate the use of this key-based renewal:

1. Test Lab Guide: Demonstrating Certificate Key-Based Renewal
2. Test Lab Guide Mini-Module: Cross-Forest Certificate Enrollment using Certificate Enrollment Web Services

## Certificate Template Compatibility

AD CS in Windows Server 2012 and Windows Server 2012 R2 include version 4 certificate templates. These templates have several differences from previous template versions. Version 4 certificate templates:

- support both cryptographic service providers (CSPs) and key service providers (KSPs).
- can be set to require renewal with the same key.
- are only available for use by Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2.
- specify the minimum certification authority and certificate client operating systems that can utilize the template.

To help administrators separate what features are supported by which operating system version, the **Compatibility** tab was added to the certificate template properties tab.

**What value does this change add?**

The new version 4 certificate templates provide additional capabilities, such as enforcing renewal with the same key (available to only Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 certificate clients). The new **Compatibility** tab allows administrators to set different combinations of operating system versions for the certification authority and certificate clients and see only the settings that will work with those client versions.

**What works differently?**

The **Compatibility** tab appears in the Certificate Template properties user interface. This tab allows you to select the minimum certification authority and minimum certificate client operating system versions. The **Compatibility** tab configuration does a couple of things:

- It marks options as unavailable in the certificate template properties depending upon the selected operating system versions of certificate client and certification authority.
- For version 4 templates, it determines which operating system versions are able to use the template.

Clients prior to Windows 8 and Windows Server 2012 will not be able to take advantage of the new version 4 templates.

**Note**

There is a statement on the **Compatibility** tab that reads **These settings may not prevent earlier operating systems from using this template**. This statement means that compatibility settings have no restrictive effect on version 1, version 2, or version 3 templates and enrollment may proceed as before. For example, in **Compatibility** tab, if the minimum client operating system version is set to Windows® Vista on a version 2 template, a Windows® XP certificate

client may still enroll for a certificate using the version 2 template.

For more information on these changes, see Certificate Template Versions and Options

## Support for certificate renewal with same key

AD CS in Windows Server 2012 and Windows Server 2012 allow for a certificate to be configured so that it will be renewed with the same key. This allows the same assurance level of the original key to be maintained throughout its lifecycle. Windows Server 2012 and Windows Server 2012 supports generating Trusted Platform Module (TPM)-protected keys using TPM-based key storage providers (KSPs). The benefit of using TPM-based KSP is true non-exportability of keys backed up by the anti-hammering mechanism of TPMs. Administrators can configure certificate templates so that Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 to give higher priority to TPM-based KSPs for generating keys. Also, using renewal with the same key, administrators can remain assured that the key still remains on TPM after renewal.

**Note**
Entering the personal identification number (PIN) incorrectly too many times activates the anti-hammering logic of the TPM. Anti-hammering logic is software or hardware methods that increase the difficulty and cost of a brute force attack on a PIN by not accepting PIN entries until after a certain amount of time has passed.

**What value does this change add?**

This feature allows an administrator to enforce renewal with the same key, which can reduce administrative costs (when keys are renewed automatically) and increase key security (when keys are stored using TPM-based KSPs).

**What works differently?**

Clients that receive certificates from templates that are configured for renewal with the same key must renew their certificates using the same key, or renewal will fail. Also, this option is available only for Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 certificate clients.

**Note**

- For more information, see Certificate Renewal with the Same Key.
- If **Renew with the same key** is enabled on a certificate template and later key archival (**Archive subject's encryption private key**) is also enabled, some renewed certificates may not be archived. To learn more about this situation and how to mitigate it, see Key Archival and renew with the same key.

If **Renew with the same key** is enabled on a certificate template and later key archival (**Archive**

**subject's encryption private key**) is also enabled, renewed certificates will not be archived. To learn more about this situation and mitigation for it, see Key Archival and renew with the same key.

## Support for Internationalized Domain Names

Internationalized names are names that contain characters that cannot be represented in ASCII. AD CS in Windows Server 2012 and Windows Server 2012 R2 supports Internationalized Domain Names (IDNs) in several scenarios.

**What value does this change add?**

The following IDN scenarios are now supported

- Certificate enrollment for computers using IDNs
- Generating and submitting a certificate request with an IDN using the certreq.exe command line tool
- Publishing Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) publishing to servers using IDNs
- The **Certificate** user interface supports IDNs
- The Certificate MMC snap-in also allows for IDNs in **Certificate Properties**

**What works differently?**

There is limited support for IDNs as previously described.

## Increased security enabled by default on the CA role service

When a certificate request is received by a certification authority (CA), encryption for the request can be enforced by the CA via the RPC_C_AUTHN_LEVEL_PKT, as described in MSDN article Authentication-Level Constants (http://msdn.microsoft.com/library/aa373553.aspx). On Windows Server 2008 R2 and earlier versions, this setting is not enabled by default on the CA. On a Windows Server 2012 or Windows Server 2012 R2 CA, this enhanced security setting is enabled by default.

**What value does this change add?**

The CA enforces enhanced security in the requests that are sent to it. This higher security level requires that the packets requesting a certificate are encrypted, so they cannot be intercepted and read. Without this setting enabled, anyone with access to the network can read packets sent to and from the CA using a network analyzer. This means that information could be exposed that might be considered a privacy violation, such as the names of requesting users or machines, the

types of certificates for which they are enrolling, the public keys involved, and so on. Within a forest or domain, leaking these data may not be a concern for most organizations. However, if attackers gain access to the network traffic, internal company structure and activity could be gleaned, which could be used for more targeted social engineering or phishing attacks.

The commands to enable the enhanced security level of RPC_C_AUTHN_LEVEL_PKT on Windows Server® 2003, Windows Server® 2003 R2, Windows Server® 2008, or Windows Server 2008 R2 certification authorities are:

**certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST**
Restart the certification authority
**net stop certsvc**
**net start certsvc**

If you still have Windows XP client computers that need to request certificates from a CA that has the setting enabled, you have two options:

1. Upgrade the Windows XP clients to a newer operating system.

2. Lower the security of the CA by running the following commands:

   **To lower CA security for compatibility with Windows XP clients**

   1. **certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST**
   2. **net stop certsvc**
   3. **net start certsvc**

**What works differently?**

Windows XP clients will not be compatible with this higher security setting enabled by default on a Windows Server 2012 or Windows Server 2012 R2 CA. If necessary, you can lower the security setting as previously described.

## AD DS Site Awareness for AD CS and PKI Clients

Certificate services in Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 can be configured to utilize Active Directory Domain Services (AD DS) sites to help optimize certificate services client requests. This functionality is not enabled by default on either certification authority (CA) or the public key infrastructure (PKI) client computers.

**Note**
For information on enabling AD DS Site Awareness, see TechNet Wiki article AD DS Site Awareness for AD CS and PKI Clients.

**What value does this change add?**

This change enables Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 certificate clients to locate a CA in their local AD DS site.

**What works differently?**

When enrolling for a template-based certificate, the client queries AD DS for the template and the CA objects. The client then uses a DsGetSiteName function call to get its own site name. For CAs with the msPKI-Site-Name attribute already set, the certificate services client determine the AD DS site link cost from the client site to each target CA site. A DsQuerySitesByCost function call is used to make this determination. The certificate services client uses the returned site costs to prioritize the CAs that allow the client the Enroll permission and support the relevant certificate template. The higher cost CAs are tried to be contacted last (only if former CAs are unavailable).

**Note**
A CA may return no site cost if the msPKI-Site-Name attribute is not set on the CA. If no site cost is available for an individual CA, then the highest possible cost is assigned to that CA.

## Group-protected PFX format

Previously, a PKCS#12 standard (also known as PFX) format was only protected by a password that had the following limitations:

- Difficult to automate
- Not very secure, because usually an administrator used a weak password
- Difficult to share among multiple users

Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 can protect certificates and associated private keys by combining an existing PFX format with a new data protection feature. This allows encrypting the contents of the PFX file with a key that belongs to a group or to an individual, instead of protecting it with a password.

**Note**

- To implement this feature, at least one domain controller must be running Windows Server 2012 or Windows Server 2012 R2.
- For more information, see the TechNet Wiki article Certificate PFX Export and Import using AD DS Account Protection.

**What value does this change add?**

By using this feature, administrators will be able to:

- Deploy, manage, and troubleshoot certificates remotely and across server farms by using Windows PowerShell.

- Share certificates and keys securely across server farms running Windows Server 2012 or Windows Server 2012 R2by using Windows APIs.

Earlier versions of Windows can consume this PFX because internally the operating system assigns a strong random password. The password is included in the PFX, and it is protected by a set of security identifiers (SIDs) with data protection APIs. Any user that has access to the PFX can see that password and share it with previous Windows versions.

**What works differently?**

A PFX file can now be protected to a security principal instead of just a password. The user interface for certificate export has been updated to allow for the selection of a security principal during export.

## Certificate lifecycle notifications

In Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2, certificates provide life cycle notifications in **MY** store from the certificate enrollment API and Windows PowerShell levels. The notifications include expiration, deletion, new, renewal, replacement, close to expiration, archive, and export. Administrators and developers can manage (view, install, copy, request, and delete) certificates and their associated private keys remotely by using Windows PowerShell. This feature allows a script or an executable to launch in response to a certificate lifecycle notification.

**Note**

- The expiration notification is supported by stores in addition to **MY** store.

- For more information, see the TechNet Wiki article Certificate Services Lifecycle Notifications.

**What value does this change add?**

For an application and server-workload developers who use certificates in their product, integrating with the certificate life cycle in Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 is easy and reliable, and it can be done remotely. Developers can develop applications that reconfigure themselves any time a certificate is renewed or replaced with another certificate—by autoenrollment or by a manual or scripted action by an administrator. The investment needed to integrate with the certificate management interfaces is very small.

For an administrator who manages applications that use certificates, Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 certificates are used by those applications

automatically. This occurs because applications integrate with Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 certificate notifications or when the administrator's script is triggered by a certificate event.

**What works differently?**

Notifications can now be enabled to alert system administrators before certificates expire.

## CA private keys are included in the System State Backup image

Windows Server Backup feature can be installed on the certification authority (CA) to create a System State Backup that includes the CA private keys.

**What works differently?**

In Windows Server 2012 and Windows Server 2012 R2 the System State Backup feature automatically backs up the CAs private key when an administrator or backup operator uses Windows Server Backup feature to perform a System State Backup.

**What works differently?**

The Windows Server Backup feature now includes the CA private keys.

**Tip**

- To add this functionality to Windows Server 2008 R2 or Windows Server® 2008, apply the appropriate update listed in document 2603469 in the Microsoft Knowledge Base.

- For details on using this feature, see Windows Server 2012 Active Directory Certificate Services System State Backup and Restore