

Active Directory Certificate Services documentation

Active Directory Certificate Services (AD CS) provides public key infrastructure (PKI) for cryptography, digital certificates and signature capabilities.

About Active Directory Certificate Services

WHAT'S NEW

[What's New in Active Directory Certificate Services?](#)

OVERVIEW

[What is Active Directory Certificate Services?](#)

Get started

CONCEPT

[Certification Authority role for AD CS](#)

[Certification Authority Web Enrollment for AD CS](#)

[Certificate Enrollment Web Service for AD CS](#)

[Certificate Enrollment Policy Web Service for AD CS](#)

[Network Device Enrollment Service for AD CS](#)

[Protecting Against Weak Cryptographic Algorithms](#)

HOW-TO GUIDE

[Configure Network Device Enrollment Service to use a domain user account](#)

[Migrate a Certification Authority key to a Key Storage Provider](#)

[Configure trusted root and disallowed certificates](#)

[Use a Policy Module with the Network Device Enrollment](#)

[Perform a Delegated Installation for an Enterprise Certification Authority](#)

More information

TRAINING

[Implement and manage Active Directory Certificate Services](#)

[Deploying an AD CS Two-Tier PKI Hierarchy](#)

[Demonstrating Certificate Key-Based Renewal](#)

REFERENCE

[ADCSAdministration PowerShell module](#)

[ADCSDeployment PowerShell module](#)

What is Active Directory Certificate Services?

Article • 03/21/2023 • 2 minutes to read

Active Directory Certificate Services (AD CS) is a Windows Server role for issuing and managing public key infrastructure (PKI) certificates used in secure communication and authentication protocols.

Issue and manage certificates

Digital certificates can be used to encrypt and digitally sign electronic documents and messages as well as for authentication of computer, user, or device accounts on a network. For example, digital certificates are used to provide:

- Confidentiality through encryption.
- Integrity through digital signatures.
- Authentication by associating certificate keys with the computer, user, or device accounts on a computer network.

Key features

AD CS provides the following important features:

- **Certification authorities:** Root and subordinate Certificate Authorities (CAs) are used to issue certificates to users, computers, and services, and to manage certificate validity.
- **Web enrollment:** Web enrollment allows users to connect to a CA with a Web browser in order to request certificates and retrieve certificate revocation lists (CRLs).
- **Online Responder:** The Online Responder service decodes revocation status requests for specific certificates, evaluates the status of these certificates, and sends back a signed response containing the requested certificate status information.
- **Network Device Enrollment Service:** The Network Device Enrollment Service allows routers and other network devices that don't have domain accounts to obtain certificates.

- **TPM key attestation:** Lets the certification authority verify the private key is protected by a hardware-based TPM and that the TPM is one that the CA trusts. TPM key attestation prevents the certificate from being exported to an unauthorized device and can bind the user identity to the device.
- **Certificate Enrollment Policy Web Service:** The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information.
- **Certificate Enrollment Web Service:** Certificate Enrollment Web Service enables users and computers to perform certificate enrollment through a web service. Together with the Certificate Enrollment Policy Web Service, this enables policy-based certificate enrollment when the client computer isn't a member of a domain or when a domain member isn't connected to the domain.

Benefits

You can use AD CS to enhance security by binding the identity of a person, computer, or service to a corresponding private key. AD CS gives you a cost-effective, efficient, and secure way to manage the distribution and use of certificates. In addition to binding of identities and private keys, AD CS also includes features that allow you to manage certificate enrollment and revocation.

You can use existing endpoint identity information in Active Directory to register certificates, meaning you can have information automatically inserted into certificates. AD CS can also be used to configure Active Directory group policies to designate which users and machines are allowed which types of certificates. Group policy configuration enables role-based or attribute-based access control.

Applications supported by AD CS include Secure/Multipurpose Internet Mail Extensions (S/MIME), secure wireless networks, virtual private network (VPN), Internet Protocol security (IPsec), Encrypting File System (EFS), smart card sign in, Secure Socket Layer/Transport Layer Security (SSL/TLS), and digital signatures.

Next steps


- [Certification Authority role for AD CS](#)
- [Implement and manage Active Directory Certificate Services](#)
- [All AD CS role services run on any version](#)
- [All AD CS role services can be run on Server Core](#)
- [Windows PowerShell Reference for Certificate Services](#)

What is Network Device Enrollment Service for Active Directory Certificate Services?

Article • 03/31/2023 • 3 minutes to read

Applies To: Windows Server (All supported versions)

The Network Device Enrollment Service (NDES) is one of the role services of Active Directory Certificate Services (AD CS). NDES acts as a Registration Authority to enable the software on routers and other network devices running without domain credentials to get certificates based on the Simple Certificate Enrollment Protocol (SCEP).

SCEP defines the communication protocol between network devices and a Registration Authority for certificate enrollment. It strives to support the secure issuance of certificates to network devices in a scalable manner, using existing technology in closed networks with trusted endpoints. For more information on SCEP, see [RFC 8894 Simple Certificate Enrollment Protocol](#) .

Understanding the Network Device Enrollment Service

SCEP is a solution to the problem of enabling network devices that don't run with domain credentials to enroll for x509 version 3 certificates from a Certification Authority (CA). NDES provides any network device with a private key and associated certificate issued by a CA. Applications on the device can use the key and its associated certificate to interact with other entities on the network. The most common use of an NDES-issued certificate on a network device is to authenticate the device in an IPSec session.

SCEP was developed to support the secure, scalable issuance of certificates to network devices by using existing certification authorities (CAs). The protocol supports CA and registration authority public key distribution, enrollment, and certificate revocation queries.

NDES performs the following functions:

- Generates and provides one-time enrollment passwords to administrators.
- Submits enrollment requests to the CA.

- Retrieves enrolled certificates from the CA and forwards them to the network device.

NDES is implemented as an Internet Server API (ISAPI) extension. It requires the Internet Information Services (IIS) role to be installed on the same computer. It doesn't require the CA to be installed on the same computer. The ISAPI extension runs in its own application pool, that is, SCEP. This application pool is created during setup and is configured to run with the credentials that were provided during setup.

The SCEP specification doesn't require devices to support TLS. However, the process of retrieving a one-time password from the service should be protected using TLS. Setup creates two virtual applications - one for the device and one for the administrator.

- Devices communication location `https://<hostname>/certsrv/mscep`
- Administrator enrollment password retrieval location `https://<hostname>/certsrv/mscep_admin`

Passwords are used by the service to authenticate the device before forwarding its enrollment request to the CA. Passwords are obtained through a call to the [administration virtual application](#) [↗].

Enrolling certificates through Network Device Enrollment Service is a straightforward process:

1. Device obtains an RSA public-private key pair from the `/certsrv/mscep` web endpoint.
2. Administrator obtains a password from the Network Device Enrollment Service.
3. Administrator sets device with password and sets it to trust the enterprise PKI `/certserv/mscep_admin` web endpoint.
4. Device configured to send enrollment request to NDES.
5. NDES signs enrollment request with Enrollment Agent certificate and sends it to the CA.
6. CA issues the certificate.
7. Device retrieves issued certificate from NDES.

NDES configuration settings

NDES can be configured to run as either of the following after installing the NDES role service:

- A user account that is specified as a service account
- The built-in application pool identity of the Internet Information Services (IIS) computer

Next steps

Now that you've learned about what NDES is here are some articles to help you configure and run NDES successfully.

- [Configure Network Device Enrollment Service for Active Directory Certificate Services](#)
- If you require over-the-air enrollment for mobile devices, see [Using a Policy Module with the Network Device Enrollment Service](#).
- For detailed information about NDES configuration and operation, see [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#) [↗](#).

Certificates and trust in Windows

Article • 04/04/2023 • 3 minutes to read

Applies To: Windows Server (All supported versions), Windows clients, Azure Stack HCI.

The Microsoft Root Certificate Program enables distribution of trusted and untrusted root certificates within Windows operating systems. For more information about the list of members in Windows Root Certificate Program, see [List of Participants - Microsoft Trusted Root Program](#).

Trusted and untrusted root certificates are used by Windows operating systems and applications as a reference when determining whether public key infrastructure (PKI) hierarchies and digital certificates are trustworthy. Untrusted root certificates are certificates that are publicly known to be fraudulent. Trusted and untrusted root certificates functionality works across all environments, whether connected or disconnected.

Trusted and untrusted root certificates are contained in a certificate trust list (CTL). When you want to distribute root certificates, you use a CTL. Windows Server features automatic daily update functionality that includes downloads of latest CTLs. The list of trusted and untrusted root certificates are called the Trusted CTL and Untrusted CTL, respectively. For more information, see [Announcing the automated updater of untrustworthy certificates and keys](#).

Servers and clients access the Windows Update site to update the CTL using the automatic daily update mechanism (CTL updater) discussed in this article. You can take advantage of CTL updater functionality by installing the appropriate software updates. See the article [Configure Trusted Roots and Disallowed Certificates](#) for guidance in installing the software updates on supported operating systems discussed in this article.

Automatic certificate trust list updates

By default, Windows downloads the CTLs from the Internet via an automatic mechanism called the CTL Updater. The public URLs used by the CTL Updater can be made available to clients:

- `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertst1.cab`

- `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootststl.cab`

Automatic update functionality also can be disabled if necessary, although isn't recommended.

Alternately, you also can create a Group Policy administrative templates (ADMX policy) to redirect to an internal server for updates.

The registry location where trusted and untrusted CTLs are stored as follows:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\EncodedCtl`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertEncodedCtl`

Benefits of CTL Updater

Automatic update functionality using the CTL Updater delivers several benefits:

- **Registry settings for storing CTLs** New settings enable changing the location for uploading trusted or untrusted CTLs from the Windows Update site to a shared location in an organization. See [Registry Settings Modified](#).
- **Synchronization options** If the URL for the Windows Update site is moved to a local shared folder, the local shared folder must be synchronized with the Windows Update folder. This software update adds a set of options in the Certutil tool that you use to enable synchronization. For more information, see the [Certutil -syncWithWU](#) Windows command reference.
- **Tool to select trusted root certificates** This software update introduces a tool for managing the set of trusted root certificates in your enterprise environment. You can view and select the set of trusted root certificates, export them to a serialized certificate store, and distribute them by using Group Policy. For more information, see the [Certutil -generateSSTFromWU SSTFile](#) Windows command reference.
- **Independent configurability** The automatic update mechanism for trusted and untrusted certificates are independently configurable; you can use the automatic update mechanism to download only the untrusted CTLs and manage your own list of trusted CTLs. For more information, see [Registry settings modified](#).

See [Configure Trusted Roots and Disallowed Certificates](#) for guidance in installing the software updates on supported operating systems discussed in this article.

Automatic update functionality can be disabled if necessary, however it isn't recommended.

Next steps

Now you understand more about trusted root and disallowed certificates in Windows, here are some more articles that might help you as configure your systems.

- [Configure trusted roots and disallowed certificates](#)
- [List of Participants - Microsoft Trusted Root Program](#)
- [Controlling the Update Root certificate Certificates Feature to Prevent the Flow of Information to and from the Internet](#) 
- [Event ID 8 — Automatic Root Certificates Update Configuration](#)
- [certutil](#) Windows command reference

Configure Network Device Enrollment Service to use a domain user account

Article • 03/31/2023 • 7 minutes to read

Applies To: Windows Server (All supported versions)

It's recommended that you configure NDES to specify a user account, which requires extra steps. If you select the built-in application pool identity, no other configuration is required.

In this article, learn how to configure Network Device Enrollment Service (NDES) to run as a specified service account.

The NDES allows routers and other network devices to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP) without using domain credentials.

SCEP was developed to support the secure, scalable issuance of certificates to network devices by using existing certification authorities (CAs). The protocol supports CA and registration authority public key distribution, enrollment, and certificate revocation queries.

For more information about NDES and how it works with certificates based using the Simple Certificate Enrollment Protocol, see [What is Network Device Enrollment Service for Active Directory Certificate Services?](#).

Prerequisites

After installing the NDES role service for Active Directory Certificate Services (AD CS), verify that you meet the following prerequisites:

- Be a domain user account.
- Be a member of the local *IIS_IUSRS* group.
- Have Request permissions on the configured Certificate Authority (CA).
- Have Read and Enroll permissions on the NDES certificate template, which is configured automatically.
- If you're using a CNAME or load balanced network name, configure a service principle name (SPN) in Active Directory Domain Services.

Create a domain user account to act as the NDES service account

You next need to create a domain user account as the NDES service account.

1. Sign in to the domain controller or administrative computer with Active Directory Domain Services Remote Server Administration Tools installed. Open **Active Directory Users and Computers** by using an account that has permissions to add users to the domain.
2. In the console tree, expand the structure until you see the container where you want to create the user account. For example, some organizations have a Services OU or similar account. Right-click the container, select **New**, and then select **User**.
3. In the **New Object - User** text boxes, enter appropriate names for all the fields so that it's clear that you're creating a user account. Be sure to follow your organization's policy for creating a service account, if such a policy exists. As an example, you could enter the following, and then select **Next**.
 - **First name:** *Ndes*
 - **Last name:** *Service*
 - **User logon name:** *NdesService*
4. Ensure that you set a complex password for the account and confirm the password. Configure the password options to correspond to your organization's security policies regarding service accounts. If the password is configured to expire, you should have a process in place to ensure that you reset the password at the required intervals.
5. Select **Next**, and then select **Finished**.

Tip

- You can also use the **New-ADUser** Windows PowerShell command to add a domain user account.
- Depending upon your Active Directory Domain Service (AD DS) configuration, you may be able to implement a Managed Service Account or Group Managed Service Account for NDES. For more information about Managed Service Accounts, see **Managed Service Accounts**. For more information

about Group Managed Service Accounts, see [Group Managed Service Accounts Overview](#).

Add the NDES service account to the local *IIS_IUSRS* group

After you successfully created a domain user account as the NDES service account, you must add this NDES service account to the local *IIS_IUSRS* group.

1. On the server that is hosting the NDES service, open **Computer Management** (*compmgmt.msc*).
2. In the Computer Management console tree, under **System Tools**, expand **Local User and Groups**. Select **Groups**.
3. In the details pane, select *IIS_IUSRS*.
4. In the **General** tab, select **Add**.
5. In the **Select Users, Computers, Service Accounts, or Groups** text box, type the user sign-in name for the account that you configured to be the service account.
6. Select **Check Names**, select **OK** twice, and then close **Computer Management**.

Tip

You can also use `net localgroup IIS_IUSRS <domain>\<username> /Add` to add the NDES service account to the local *IIS_IUSRS* group. The command prompt or Windows PowerShell must be run as Administrator. For more information, see the [Add-LocalGroupMember](#) PowerShell command.

Set up request permission on the CA

NDES service accounts need to request permission on the CA that is to be used by NDES.

1. On the CA that is to be used by NDES, open the CA console with an account that has Manage CA permissions.
2. Open the Certification Authority console. Right-click the CA, and then select **Properties**.

3. On the **Security** tab, you can see the accounts that have Request Certificates permissions. By default the group **Authenticated Users** has this permission. The service account that you created is a member of **Authenticated Users** when it's in use. You don't need to grant more permissions, if **Authenticated Users** has the Request Certificates permission. However, if that isn't the case, you should grant the NDES service account Request Certificates permission on the CA. To do so:

- Select **Add**.
- In the **Select Users, Computers, Service Accounts, or Groups** text box, type the name of the NDES service account, and select **Check Names**, and then select **OK**.
- Ensure that NDES service account is selected. Ensure that the **Allow** check box that corresponds to **Request Certificates** is selected. Select **OK**.

Verify whether it's necessary to set a service principal name for NDES

You need to configure a service principal name (SPN) in Active Directory if you're using a load balancer or virtual name. In this section, learn how to determine whether it's necessary to set an SPN in Active Directory.

- If you're using a single NDES server and its actual hostname (most common scenario), the account doesn't need an SPN registered. The computer accounts default SPNs for HOST/computerFQDN cover this case. If you're using all other defaults (particularly around IIS kernel-mode authentication), you can skip ahead to the next section of this article.
- If you're using a custom A record as a hostname, or load balancing with a Virtual IP, an SPN needs to be registered against the NDES service account (SCEPSvc). To register an SPN against the NDES service account:

1. Use the Setspn command syntax of: `Setspn -s HTTP/<computerfqdn> <domainname\accountname>` when entering your commands. For example, your domain is `Fabrikam.com`, your NDES CNAME is `NDESFARM`, and you're using a service account named `SCEPSvc`. In the example, you would run the following commands.

- `Setspn -s HTTP/NDESFARM.fabrikam.com fabrikam\SCEPSvc`
- `Setspn -s HTTP/NDESFARM fabrikam\SCEPSvc`

2. Then disable IIS Kernel-mode Authentication for the site.

Set up the NDES role service

After installation completes, you need to do a few steps to finish configuring the NDES computer.

If NDES is installed on a CA, you don't have the opportunity to select a CA because the local CA is used.

When you install NDES on a computer that isn't a CA, you must select the target CA. You can select the CA using the CA name or by the computer name.

To select the CA:

1. Open AD CS Configuration from Server Manager.
2. Select on **CA for NDES**
3. Select **CA name** or **Computer name**, and then select **Select**.
4. The option you choose determines the type of dialog box that is presented next:
 - If you clicked **CA name**, you're presented with the **Select Certification Authority** dialog box, which has a list of CAs from which you can choose.
 - or
 - If you clicked **Computer name**, you see the **Select Computer** dialog box where you can set the **Locations** and enter the computer name that you want to specify as the CA.

You're now ready to complete setup of the NDES role service. The remaining steps are verifying the Registration Authority information and setting up cryptography.

1. Registration Authority (RA) information that you provide is used to construct the signing certificate that is issued to the service. In Server Manager. Select RA information.
2. Check all fields and confirm that the RA information is correct (or is set to the defaults).

NDES uses two certificates and their keys to enable device enrollment. Organizations can use different Cryptographic Service Providers (CSPs) to store these keys, or change the length of the keys that is used by the service. Only Cryptographic Application Programming Interface (CryptoAPI) Service Providers are supported for the RA keys—Cryptography API; Next Generation (CNG) providers aren't supported.

1. To configure the cryptography, in Server Manager, select Cryptography for NDES.
2. Enter the values for Signature Key Provider and/or Encryption Key Provider and decide on key length values.
3. Continue through the wizard to complete the installation of NDES.

Now that you've configured the role service, you can learn detailed information about NDES configuration and operation see [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#) [↗](#).

Tip

If you make configuration changes for NDES or to the certificate templates that are used by NDES, you must stop and restart NDES, IIS and the CA service.

Next steps

- [Using a Policy Module with the Network Device Enrollment Service](#)
- [Active Directory Certificate Services \(AD CS\) Public Key Infrastructure \(PKI\) Frequently Asked Questions \(FAQ\)](#) [↗](#)

Configure trusted roots and disallowed certificates in Windows

Article • 04/04/2023 • 14 minutes to read

Applies To: Windows Server (All supported versions), Windows clients, Azure Stack HCI.

Redirect the Microsoft Automatic Update URL to a file or web server hosting Certificate Trust Lists (CTLs), untrusted CTLs, or a subset of the trusted CTL files in a disconnected environment.

To learn more about how the Microsoft Root Certificate Program works to distribute trusted root certificates automatically across Windows operating systems, see [Certificates and trust](#).

Tip

You don't need to redirect the Microsoft Automatic Update URL for environments where computers are able to connect to the Windows Update site directly. Computers that can connect to the Windows Update site are able to receive updated CTLs on a daily basis.

Prerequisites

Before you can configure your disconnected environment to use CTL files hosted on a file or web server, you need to complete the following prerequisites.

Client prerequisites

- At least one computer that is able to connect to the Internet to download CTLs from Microsoft. The computer requires HTTP (TCP port 80) access and name resolution (TCP and UDP port 53) ability to contact `ctldl.windowsupdate.com`. This computer can be a domain member or a member of a workgroup. Currently all the downloaded files require approximately 1.5 MB of space.
- Client machines must be connected to an Active Directory Domain Service domain.
- You must be a member of the local *Administrators* group.

Server prerequisites

- A file server or web server for hosting the CTL files.
- AD Group policy or MDM solution to deploy configuration settings to your client.
- An account that is a member of the *Domain Admins* group or that has been delegated the necessary permissions

Configuration methods

An administrator can configure a file or web server to download the following files by using the automatic update mechanism:

- `authrootstl.cab` contains a non-Microsoft CTL.
- `disallowedcertstl.cab` contains a CTL with untrusted certificates.
- `disallowedcert.sst` contains a serialized certificate store, including untrusted certificates.
- `<thumbprint>.crt` contains non-Microsoft root certificates.

The steps to perform this configuration are described in the [Configure a file or web server to download the CTL files](#) section of this document.

There are several methods to configure your environment to use local CTL files or a subset of trusted CTLs. The following methods are available.

- Configure Active Directory Domain Services (AD DS) domain member computers to use the automatic update mechanism for trusted and untrusted CTLs, without having access to the Windows Update site. This configuration is described in the [Redirect the Microsoft Automatic Update URL](#) section of this document.
- Configure AD DS domain member computers to independently opt-in for untrusted and trusted CTL automatic updates. The independent opt-in configuration is described in the [Redirect the Microsoft Automatic Update URL for untrusted CTLs only](#) section of this document.
- Examine the set of root certificates in the Windows Root Certificate Program. Examining the root certificate set enables administrators to select a subset of certificates to distribute by using a Group Policy Object (GPO). This configuration is described in the [Use a subset of the trusted CTLs](#) section of this document.

- The settings described in this document are implemented by using GPOs. These settings are not automatically removed if the GPO is unlinked or removed from the AD DS domain. When implemented, these settings can be changed only by using a GPO or by modifying the registry of the affected computers.
- The concepts discussed in this document are independent of Windows Server Update Services (WSUS).

Configure a file or web server to download the CTL files

To facilitate the distribution of trusted or untrusted certificates for a disconnected environment, you must first configure a file or web server to download the CTL files from the automatic update mechanism.

Retrieve the CTL files from Windows Update

1. Create a shared folder on a file or web server that is able to synchronize by using the automatic update mechanism and that you want to use to store the CTL files.

Tip

Before you begin, you may have to adjust the shared folder permissions and NTFS folder permissions to allow the appropriate account access, especially if you're using a scheduled task with a service account. For more information on adjusting permissions, see [Managing Permissions for Shared Folders](#).

2. From an elevated PowerShell prompt, run the following command:

```
PowerShell  
  
Certutil -syncWithWU \\<server>\<share>
```

Substitute the actual server name for `<server>` and shared folder name for `<share>`. For example, for a server named `Server1` with a shared folder named CTL, you'd run the command:

```
PowerShell
```

```
Certutil -syncWithWU \\Server1\CTL
```

3. Download the CTL files on a server that computers on a disconnected environment can access over the network by using a FILE path (for example, `FILE://\\Server1\CTL`) or an HTTP path (for example, `https://Server1/CTL`).

ⓘ Note

- If the server that synchronizes the CTLs is not accessible from the computers in the disconnected environment, you must provide another method to transfer the information. For example, you can allow one of the domain members to connect to the server, then schedule another task on the domain member computer to pull the information into a shared folder on an internal web server. If there is absolutely no network connection, you may have to use a manual process to transfer the files, such as a removable storage device.
- If you plan to use a web server, you should create a new virtual directory for the CTL files. The steps to create a virtual directory by using Internet Information Services (IIS) are nearly the same for all the supported operating systems discussed in this document. For more information, see [Create a Virtual Directory \(IIS7\)](#) ↗.
- Certain system and application folders in Windows have special protection applied to them. For example, the *inetpub* folder requires special access permissions, which make it difficult to create a shared folder for use with a scheduled task to transfer files. An administrator can create a folder location at the root of a logical drive system to use for file transfers.

Redirect the Microsoft Automatic Update URL

The computers in your network might be configured in a disconnected environment and therefore unable to use the automatic update mechanism or download CTLs. You can implement a GPO in AD DS to configure these computers to obtain the CTL updates from an alternate location.

The configuration in this section requires that you already completed the steps in [Configure a file or web server to download the CTL files](#).

To configure a custom administrative template for a GPO

1. On a domain controller, create a new administrative template. Open a text file in Notepad and then change the file name extension to `.adm`. The contents of the file should be as follows:

ADM

```
CLASS MACHINE
CATEGORY !!SystemCertificates
    KEYNAME "Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate"
    POLICY !!RootDirURL
        EXPLAIN !!RootDirURL_help
        PART !!RootDirURL EDITTEXT
            VALUENAME "RootDirURL"
        END PART
    END POLICY
END CATEGORY
[strings]
RootDirURL="URL address to be used instead of default
ctldl.windowsupdate.com"
RootDirURL_help="Enter a FILE or HTTP URL to use as the download
location of the CTL files."
SystemCertificates="Windows AutoUpdate Settings"
```

2. Use a descriptive name to save the file, such as `RootDirURL.adm`.
 - Ensure that the file name extension is `.adm` and not `.txt`.
 - If you haven't already enabled file name extension viewing, see [How To: View File Name Extensions](#).
 - If you save the file to the `%windir%\inf` folder, it's easier to locate in the following steps.
3. Open the Group Policy Management Editor. Select **Start > Run**, type **GPMC.msc**, then press ENTER.

Warning

You can link a new GPO to the domain or to any organizational unit (OU). The GPO modifications implemented in this document alter the registry settings of the affected computers. You can't undo these settings by deleting or unlinking the GPO. The settings can only be undone by reversing them in the GPO settings or by modifying the registry using another technique.

4. Expand the **Forest** object, expand the **Domains** object, and then expand the specific domain that contains the computer accounts that you want to change. If you have a specific OU that you want to modify, then navigate to that location.
5. Right-select and then select **Create a GPO in this domain, and Link it here** to create a new GPO.
6. In the navigation pane, under **Computer Configuration**, expand **Policies**.
7. Right-select **Administrative Templates**, then select **Add/Remove Templates**.
8. In **Add/Remove Templates**, select **Add**.
9. In the **Policy Templates** dialog box, select the `.adm` template that you previously saved. Select **Open**, then select **Close**.
10. In the navigation pane, expand **Administrative Templates**, and then expand **Classic Administrative Templates (ADM)**.
11. Select **Windows AutoUpdate Settings**, and in the details pane, double-select **URL address to be used instead of default ctldl.windowsupdate.com**.
12. Select **Enabled**. In the Options section, enter the URL to the file server or web server that contains the CTL files. For example, `https://server1/CTL` or `file://\\server1\CTL`.
13. Select **OK**.
14. Close the Group Policy Management Editor.

The policy is effective immediately, but the client computers must be restarted to receive the new settings, or you can type `gpupdate /force` from an elevated command prompt or from Windows PowerShell.

Important

The trusted and untrusted CTLs can be updated on a daily basis, so ensure that you keep the files synchronized by using a scheduled task or another method (such as a script that handles error conditions) to update the shared folder or web virtual directory. For more information about creating a scheduled task using PowerShell, see [New-ScheduledTask](#). If you plan to write a script to make daily updates, see the [certutil](#) Windows command reference.

Redirect the Microsoft Automatic Update URL for untrusted CTLs only

Some organizations might want only the untrusted CTLs (not the trusted CTLs) to be automatically updated. To automatically update only the untrusted CTLs, create two `.adm` templates to add to Group Policy.

In a disconnected environment, you can use the following procedure with the previous procedure (redirect the Microsoft Automatic Update URL for trusted CTLs and untrusted CTLs). This procedure explains how to selectively disable the automatic update of trusted CTLs.

You also can use this procedure in a connected environment in isolation to selectively disable the automatic update of trusted CTLs.

To selectively redirect only untrusted CTLs

1. On a domain controller, create the first new administrative template by starting with a text file and then changing the file name extension to `.adm`. The contents of the file should be as follows:

ADM

```
CLASS MACHINE
CATEGORY !!SystemCertificates
    KEYNAME "Software\Policies\Microsoft\SystemCertificates\AuthRoot"
    POLICY !!DisableRootAutoUpdate
        EXPLAIN !!Certificates_config
        VALUENAME "DisableRootAutoUpdate"
        VALUEON NUMERIC 0
        VALUEOFF NUMERIC 1

    END POLICY
END CATEGORY
[strings]
DisableRootAutoUpdate="Auto Root Update"
Certificates_config="By default automatic updating of the trusted CTL
is enabled. To disable the automatic updating trusted CTLe, select
Disabled."
SystemCertificates="Windows AutoUpdate Settings"
```

2. Use a descriptive name to save the file, such as `DisableAllowedCTLUpdate.adm`.
 3. Create a second new administrative template. The contents of the file should be as follows:
-

ADM

```
CLASS MACHINE
CATEGORY !!SystemCertificates
    KEYNAME "Software\Policies\Microsoft\SystemCertificates\AuthRoot"
    POLICY !!EnableDisallowedCertAutoUpdate
        EXPLAIN !!Certificates_config
        VALUENAME "EnableDisallowedCertAutoUpdate"
        VALUEON NUMERIC 1
        VALUEOFF NUMERIC 0

    END POLICY
END CATEGORY
[strings]
EnableDisallowedCertAutoUpdate="Untrusted CTL Automatic Update"
Certificates_config="By default untrusted CTL automatic update is
enabled. To disable trusted CTL update, select Disabled."
SystemCertificates="Windows AutoUpdate Settings"
```

4. Use a descriptive file name to save the file, such as

EnableUntrustedCTLUpdate.adm.

- Ensure that the file name extensions of these files are `.adm` and not `.txt`.
- If you save the file to the `%windir%\inf` folder, it's easier to locate in the following steps.

5. Open the Group Policy Management Editor.

6. Expand the **Forest** object, expand the **Domains** object, and then expand the specific domain that contains the computer accounts that you want to change. If you have a specific OU that you want to modify, then navigate to that location.

7. In the navigation pane, under **Computer Configuration**, expand **Policies**.

8. Right-select **Administrative Templates**, then select **Add/Remove Templates**.

9. In **Add/Remove Templates**, select **Add**.

10. In the **Policy Templates** dialog box, select the `.adm` template that you previously saved. Select **Open**, then select **Close**.

11. In the navigation pane, expand **Administrative Templates**, then expand **Classic Administrative Templates (ADM)**.

12. Select **Windows AutoUpdate Settings**, then in the details pane, double-click **Auto Root Update**.

13. Select **Disabled**, then select **OK**.

14. In the details pane, double-click **Untrusted CTL Automatic Update**, then select **Enabled** and **OK**.

The policy is effective immediately, but the client computers must be restarted to receive the new settings, or you can type `gpupdate /force` from an elevated command prompt or from Windows PowerShell.

Important

The trusted and untrusted CTLs can be updated on a daily basis, so ensure that you keep the files synchronized by using a scheduled task or another method to update the shared folder or virtual directory.

Use a subset of the trusted CTLs

This section describes how you can produce, review, and filter the trusted CTLs that you want computers in your organization to use. You must implement the GPOs described in the previous procedures to make use of this resolution. This resolution is available for disconnected and connected environments.

There are two procedures to customize the list of trusted CTLs.

1. Create a subset of trusted certificates
2. Distribute the trusted certificates by using Group Policy

To create a subset of trusted certificates

Here's how to generate SST files by using the automatic Windows update mechanism from Windows. For more information about generating SST files, see the [Certutil](#) Windows commands reference.

1. From a computer that is connected to the Internet, open Windows PowerShell as an Administrator or open an elevated command prompt, and type the following command:

```
PowerShell
```

```
Certutil -generateSSTFromWU WURoots.sst
```

2. Run the following command in Windows Explorer to open `WURoots.sst`:

PowerShell

```
start explorer.exe wuroots.sst
```

Tip

You also can use Internet Explorer to navigate to the file and double-click it to open it. Depending on where you stored the file, you may also be able to open it by typing `wuroots.sst`.

3. Open Certificate Manager.

4. Expand the file path under **Certificates - Current User** until you see **Certificates**, then select **Certificates**.

5. In the details pane, you can see the trusted certificates. Hold down the **CTRL** key and select each of the certificates that you want to allow. When you've finished selecting the certificates you want to allow, right-click one of the selected certificates, select **All Tasks**, then select **Export**.

- You must select a minimum of two certificates to export the `.sst` file type. If you select only one certificate, the `.sst` file type isn't available, and the `.cer` file type is selected instead.

6. In the Certificate Export Wizard, select **Next**.

7. On the **Export File Format** page, select **Microsoft Serialized Certificate Store (.SST)**, and then select **Next**.

8. On the **File to Export** page, enter a file path and an appropriate name for the file, such as `C:\AllowedCerts.sst`, then select **Next**.

9. Select **Finish**. When you're notified that the export was successful, select **OK**.

10. Copy the `.sst` file that you created to a domain controller.

To distribute the list of trusted certificates by using Group Policy

1. On the domain controller that has the customized `.sst` file, open the Group Policy Management Editor.

2. Expand the **Forest, Domains**, and specific domain object that you want to modify. Right-click **Default Domain Policy GPO**, then select **Edit**.
3. In the navigation pane, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, then expand **Public Key Policies**.
4. Right-click **Trusted Root Certification Authorities**, then select **Import**.
5. In the Certificate Import Wizard, select **Next**.
6. Enter the path and file name of the file that you copied to the domain controller, or use the **Browse** button to locate the file. Select **Next**.
7. Confirm that you want to place these certificates in the **Trusted Root Certification Authorities** certificate store by selecting **Next**. select **Finish**. When you're notified that the certificates imported successfully, select **OK**.
8. Close the Group Policy Management Editor.

The policy is effective immediately, but the client computers must be restarted to receive the new settings, or you can type `gpupdate /force` from an elevated command prompt or from Windows PowerShell.

Registry settings modified

The settings described in this document configure the following registry keys on the client computers. These settings aren't automatically removed if the GPO is unlinked or removed from the domain. These settings must be reconfigured, if you want to change them.

- Enable or disable the Windows AutoUpdate of the trusted CTL:
 - **Key:** `HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate`
 - **Type:** `REG_DWORD`
 - **Name:** `DisableRootAutoUpdate`
 - **Data:** `0` to enabled or `1` to disable.
 - **Default:** There is no key present by default. Without a key present, the default is enabled.
- Enable or disable the Windows AutoUpdate of the untrusted CTL:
 - **Key:** `SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot`
 - **Type:** `REG_DWORD`

- **Name:** EnableDisallowedCertAutoUpdate
- **Data:** 0 to enabled or 1 to disable.
- **Default:** There is no key present by default. Without a key present, the default is enabled.
- Set the shared CTL file location (HTTP or the FILE path):
 - **Key:**
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\RootDirUrl
 - **Type:** REG_SZ
 - **Name:** RootDirUrl
 - **Data:** Enter a valid HTTP or file URI.
 - **Default:** There is no key present by default. Without a key present, the default behavior used Windows Update.

Deleting Trusted and Untrusted CTLs

It may be necessary for various reasons to delete all Trusted and Untrusted CTLs from a client machine. The following Certutil options can be used to delete all Trusted and Untrusted CTLs from a client machine.

PowerShell

```
certutil -verifyCTL AuthRoot
certutil -verifyCTL Disallowed
```

Checking Last Sync Time

To check the most recent sync time on the local machine for either Trusted or Untrusted CTLs, run the following Certutil command:

PowerShell

```
certutil -verifyctl AuthRoot | findstr /i "lastsynctime"
certutil -verifyctl Disallowed | findstr /i "lastsynctime"
```

Related links

- [Certificates and trust](#)
- [List of Participants - Microsoft Trusted Root Program](#)

- [certutil](#) Windows command reference
- [Windows Root certificate Certificate Program - Members List \(All CAs\)](#) ↗
- [Controlling the Update Root certificate Certificates Feature to Prevent the Flow of Information to and from the Internet](#) ↗