

Report: Certificate Services & Secure Authentication

1. Introduction

As organizations increasingly adopt digital communication and identity-driven security models, the need for a reliable and secure authentication infrastructure becomes paramount. Certificate-based authentication using Public Key Infrastructure (PKI) is one of the most effective ways to ensure data confidentiality, integrity, and user trust within a Windows domain environment. Active Directory Certificate Services (AD CS) is a Microsoft server role that enables the creation and management of a PKI, including issuing and managing digital certificates used in encryption, digital signing, and secure authentication.

This section of the project focuses on establishing an internal Certificate Authority (CA) using AD CS, configuring it to issue certificates for users and computers, and implementing automated certificate enrollment. This setup is crucial for enabling secure services such as HTTPS, secure email, smart card logon, and mutual authentication within the enterprise environment.

2. Objective

The main goal of this task is to implement a secure and scalable certificate infrastructure using Active Directory Certificate Services. First, the AD CS role is installed and configured to serve as a Root CA, which becomes the trusted anchor point for all certificates issued within the network. This is followed by the creation and issuance of digital certificates for domain-joined users and machines to facilitate secure authentication and encrypted communications.

Finally, the auto-enrollment feature is configured through Group Policy, allowing users and computers to automatically request and renew certificates without manual intervention. This approach not only strengthens the overall security posture of the domain but also simplifies certificate lifecycle management for IT administrators.

Key goals include:

- **Establish a Secure Certificate Authority (CA) Infrastructure**

To provide a trusted internal Public Key Infrastructure (PKI) by setting up an enterprise Root Certification Authority (CA), enabling secure digital certificate issuance and management across the domain.

- **Enable Secure Domain Authentication**

To issue computer and user certificates that facilitate secure authentication to Active Directory services, helping protect against credential theft and ensuring communication integrity.

- **Automate Certificate Enrollment and Renewal**

To configure Group Policy-based auto-enrollment for user and machine certificates, reducing administrative overhead and ensuring timely and consistent certificate deployment.

- **Support Enterprise Security Services (e.g., TLS, EFS, VPN, Wi-Fi)**

To enable services such as SSL/TLS, encrypted file systems, VPN access, and secure wireless authentication by deploying valid certificates to domain resources.

- **Ensure Compliance and Centralized Management**

To meet organizational security policies and compliance requirements by enforcing standardized certificate templates and maintaining centralized control over certificate lifecycle management.

3. Methodology

In modern enterprise environments, secure authentication and encryption are crucial to ensure the safety and integrity of data. One of the best ways to achieve secure authentication is by using certificates. **Active Directory Certificate Services (AD CS)** allows the creation and management of Public Key Infrastructure (PKI) for issuing and managing certificates. In this report, we will walk

through the process of setting up AD CS, issuing certificates for domain authentication, and configuring auto-enrollment for both user and machine certificates to simplify certificate management.

3.1 Installation and Configuration of AD Certificate Services (AD CS)

To install the AD Certificate Services role on the server and configure it as a **Root Certification Authority (CA)**. This will establish the core foundation for issuing and managing certificates in the organization.

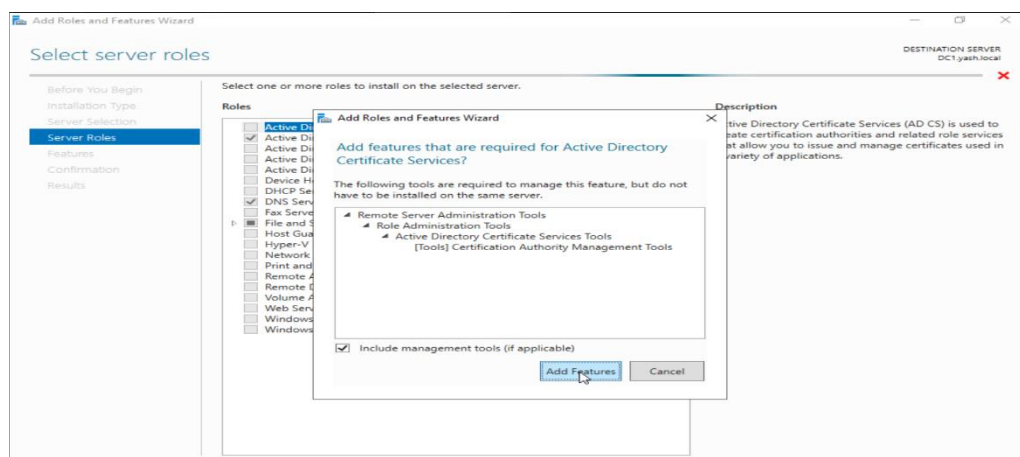
- **Download and Install AD Certificate Services (AD CS)**

The first step in setting up AD CS is to install the AD Certificate Services role on a Windows Server. The installation of this role allows the server to act as a **Certification Authority (CA)**, which will issue and manage certificates for your organization.

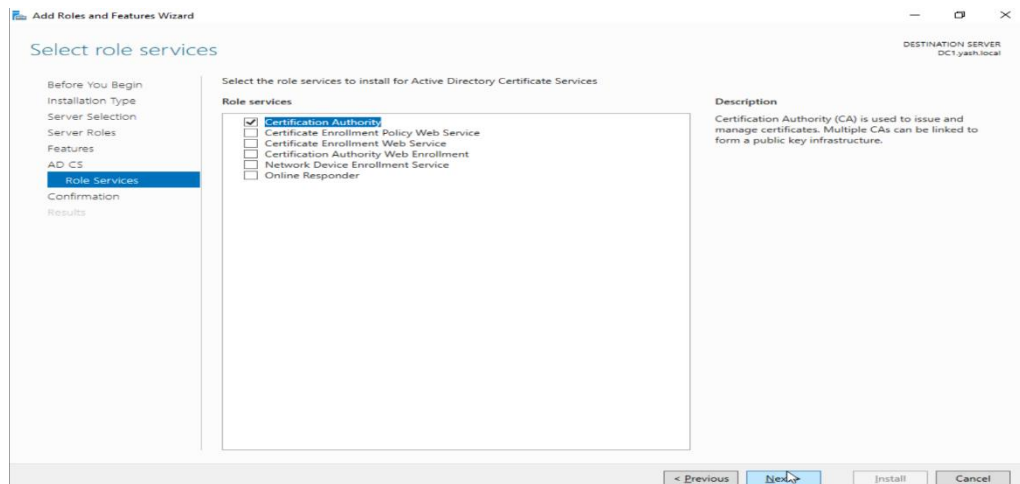
Navigation Path:

Server Manager > Manage > Add Roles and Features > Select Active Directory Certificate Services

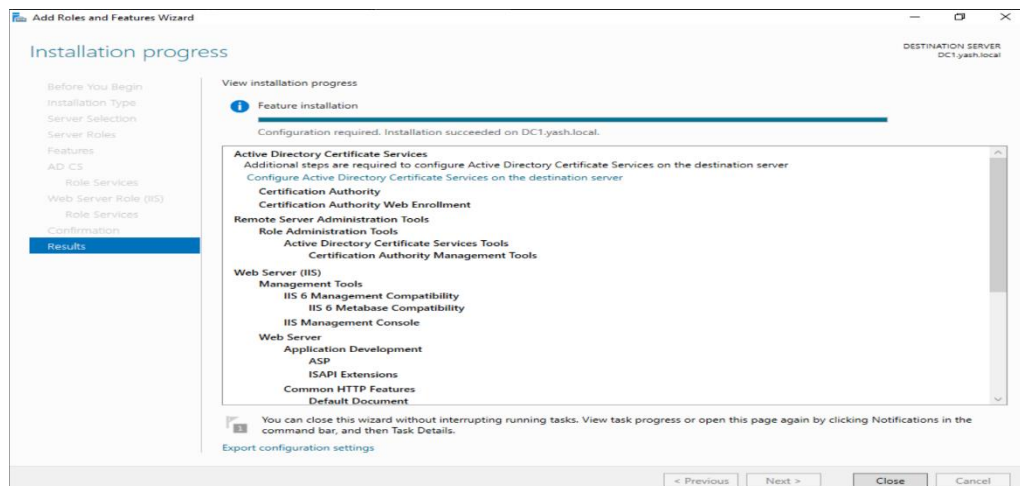
(Add roles and features – Active Directory Certificate Services)



(Check the Certificate Authority option.)



(Installation completed)



- **Configure AD CS as a Root Certification Authority (CA)**

Once the AD CS role is installed, it needs to be configured as a **Root Certification Authority**. The **Root CA** is the trusted authority at the top of the certificate chain and signs all certificates issued within the organization. It's critical that the Root CA is highly secure, as it validates the entire trust model for your PKI.

AD CS Configuration

DESTINATION SERVER
DC1.yash.local

Credentials

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials:

[More about AD CS Server Roles](#)

< Previous Next > Configure Cancel

AD CS Configuration

DESTINATION SERVER
DC1.yash.local

Role Services

Select Role Services to configure

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous Next > Configure Cancel

AD CS Configuration

DESTINATION SERVER
DC1.yash.local

Setup Type

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

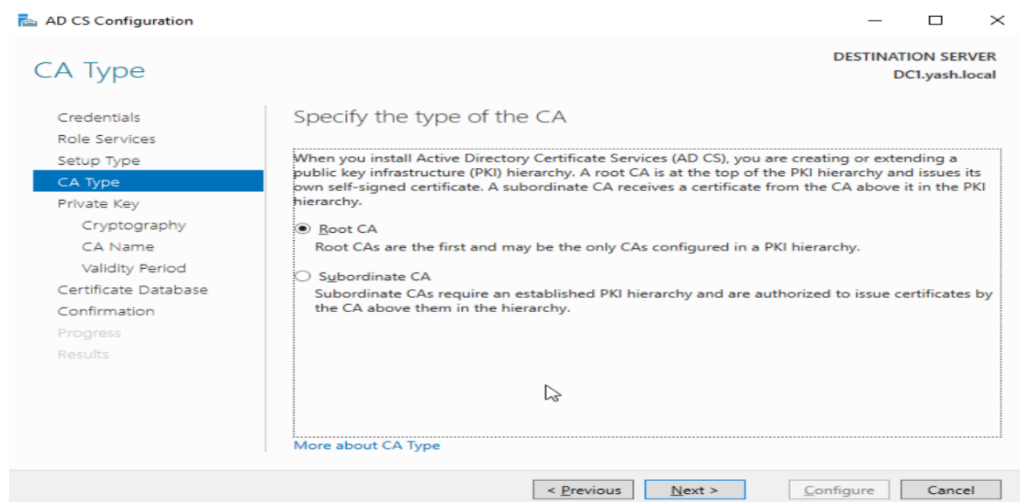
☒ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

< Previous Next > Configure Cancel

(The server is set as a Root CA)



AD CS Configuration

DESTINATION SERVER
DC1.yash.local

CA Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

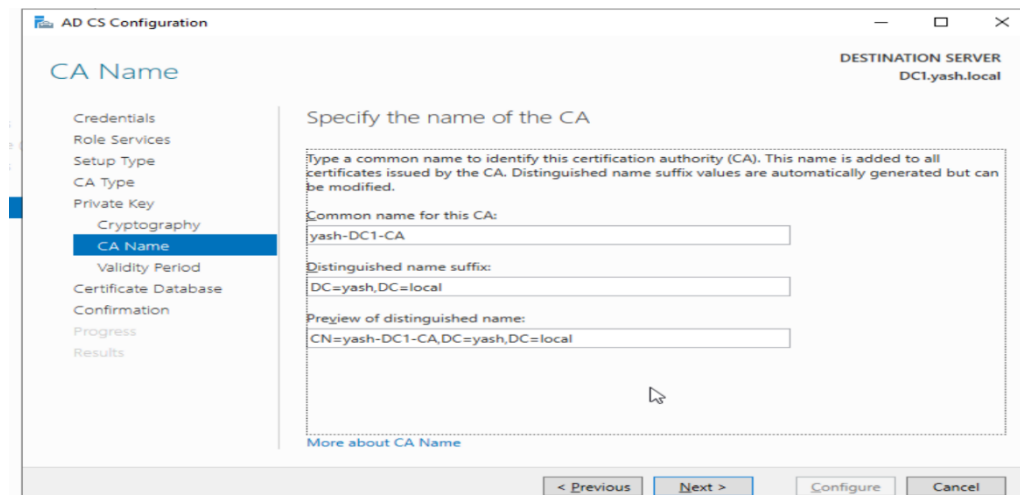
☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

(Enter the Certificate Authority name)



AD CS Configuration

DESTINATION SERVER
DC1.yash.local

CA Name

Credentials
Role Services
Setup Type
CA Type
CA Name
Private Key
Cryptography
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
yash-DC1-CA

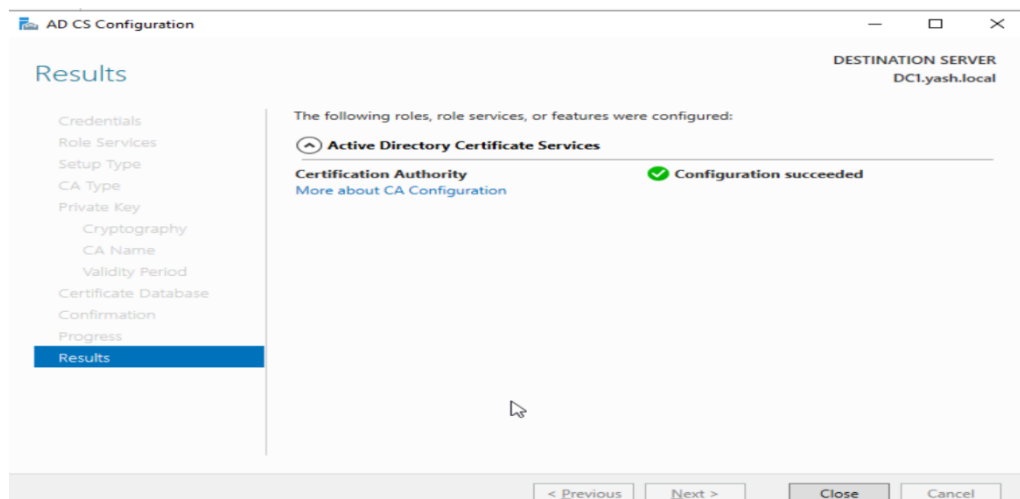
Distinguished name suffix:
DC=yash,DC=local

Preview of distinguished name:
CN=yash-DC1-CA,DC=yash,DC=local

[More about CA Name](#)

< Previous Next > Configure Cancel

(Configuration completed)



AD CS Configuration

DESTINATION SERVER
DC1.yash.local

Results

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority ✔ Configuration succeeded

[More about CA Configuration](#)

< Previous Next > Close Cancel

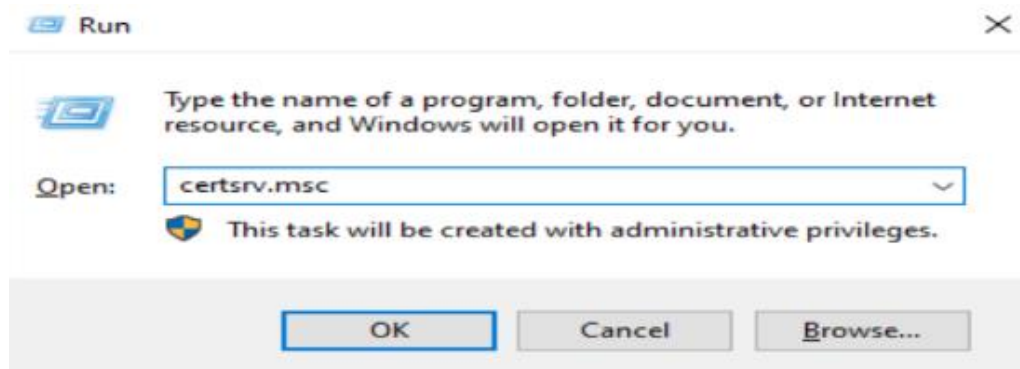
3.2 Issue Certificates for Domain Authentication

To configure certificate templates for domain authentication and issue certificates for both user and computer accounts, allowing secure authentication within the domain.

- **Open the Certificate Services Management Console**

The **Certificate Services Management Console** (certsrv.msc) is used to manage certificate templates, view issued certificates, and configure various CA settings. You will interact with this console to create, issue, and manage certificates for your domain.

(Open the Certificate Services Management Console.)

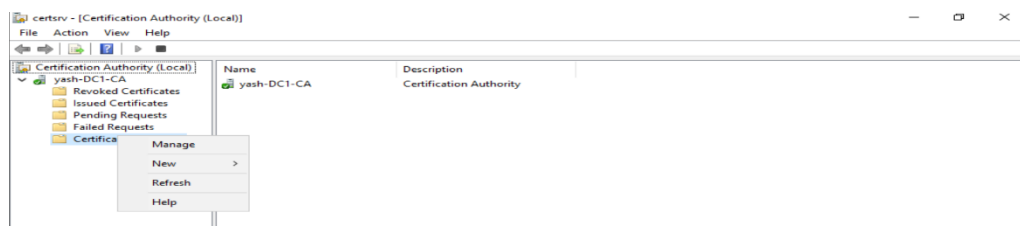


- **Open the Certificate Template Console**

Certificate templates define the properties and settings of certificates issued by the CA. The **Certificate Templates Console** is used to create and manage these templates.

Navigation Path:

certsrv.msc > Certificate Templates > Manage

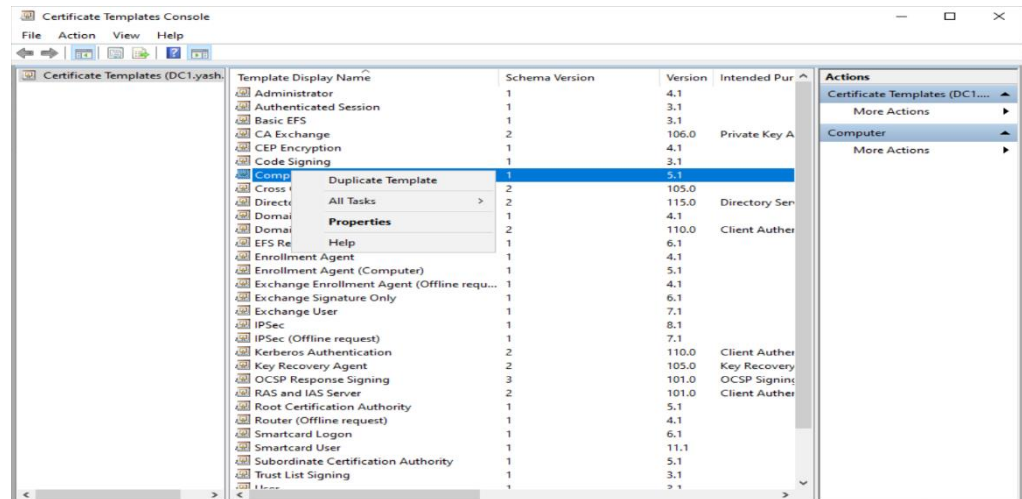


- **Duplicate the Computer Certificate Template**

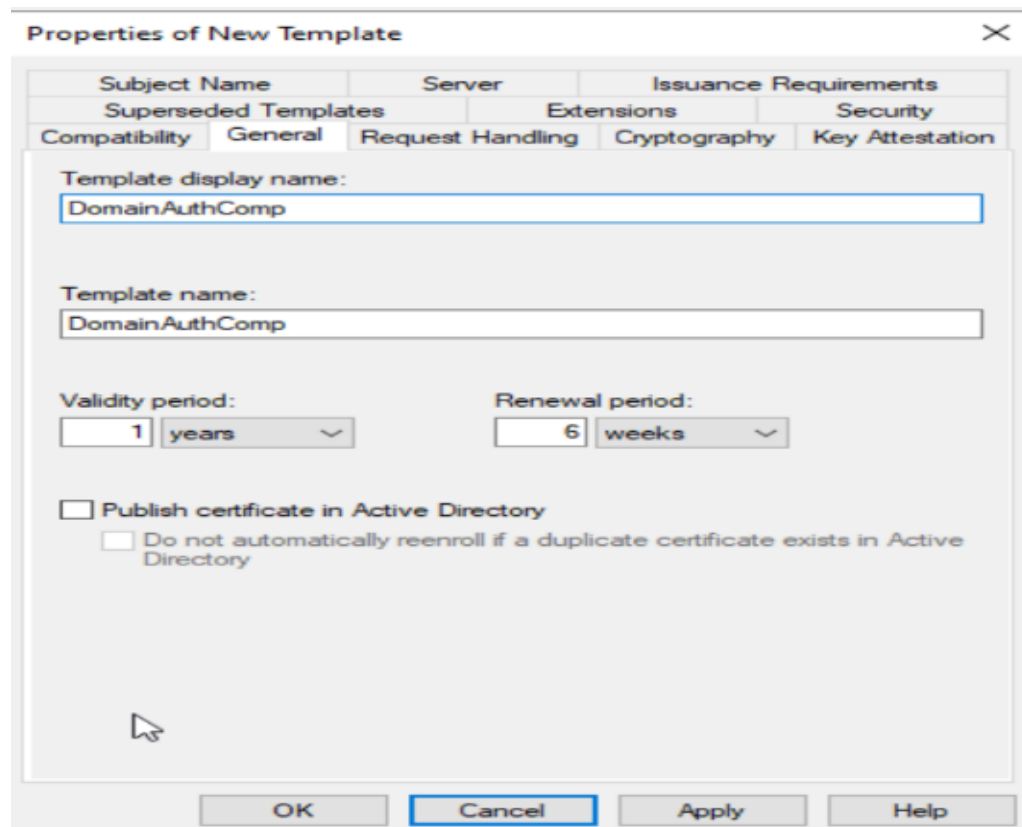
Duplicating the **Computer** certificate template allows you to customize it based on the security requirements of your domain's devices. You can configure settings such as certificate key usage, validity period, and cryptographic settings.

Navigation Path:

Certificate Templates > Right-click > Duplicate Template



(Entered the name of template.)



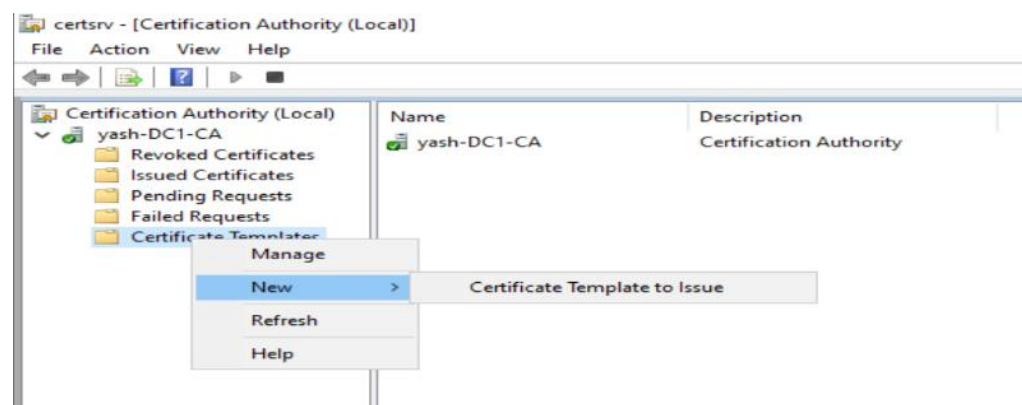
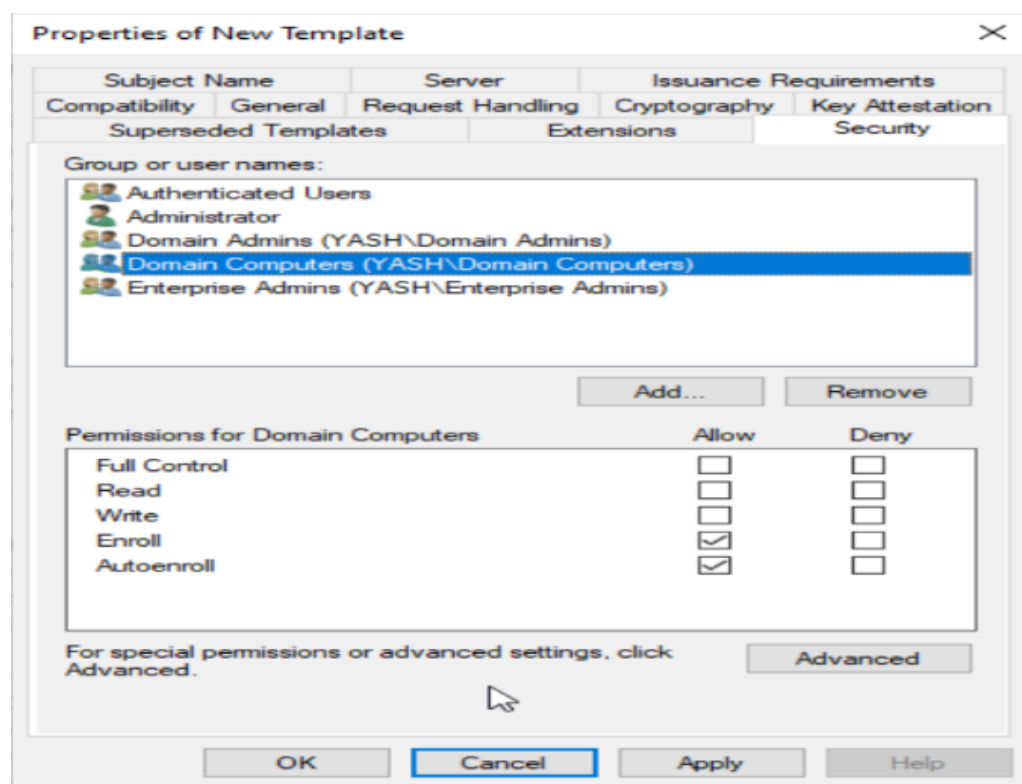
- **Issue the Computer Certificate Template and Enable Auto-Enrollment**

After duplicating and customizing the computer template, it is time to issue it. Enabling **auto-enrollment** will automatically assign certificates to machines as they join the domain.

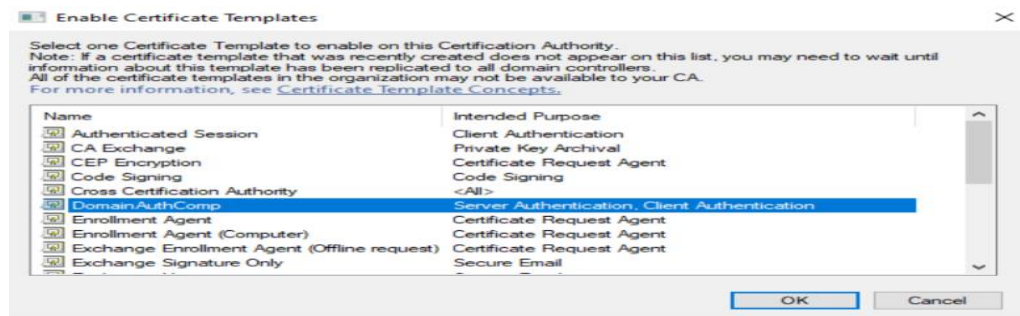
Navigation Path:

Certification Authority > Right-click on Certificate Templates > Certificate Template to Issue

(Check the Enroll and Autoenroll option.)



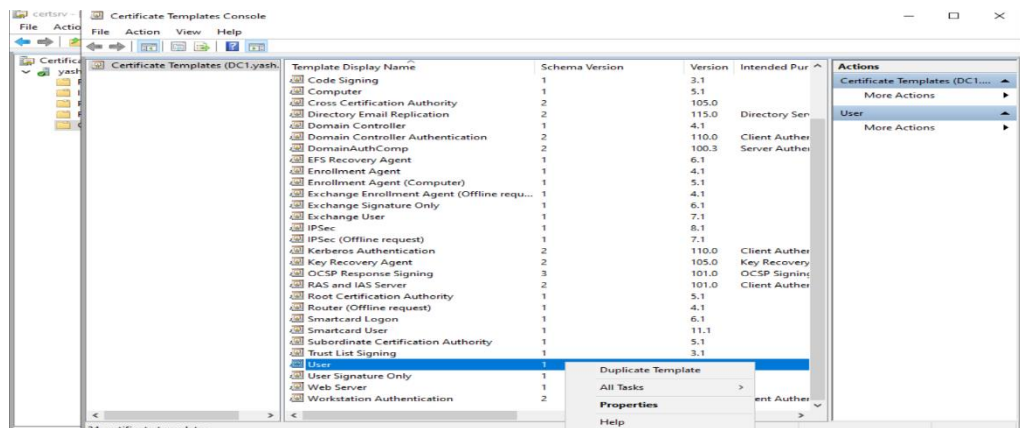
(Showing issuing the Computer certificate template)



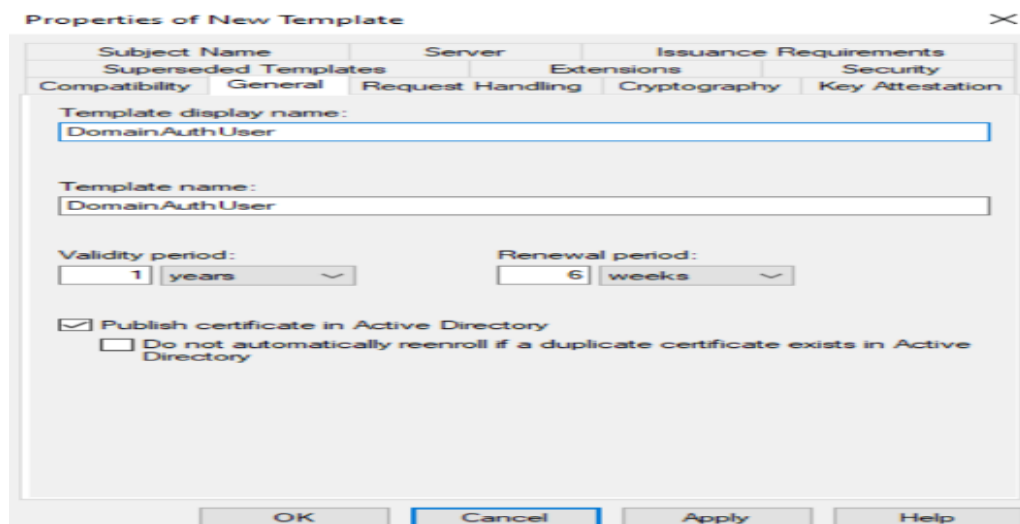
- **Duplicate the User Certificate Template**

Similar to the computer certificate template, the **User** certificate template needs to be duplicated and customized for the domain users to allow secure user authentication.

(Duplicate the user Template)

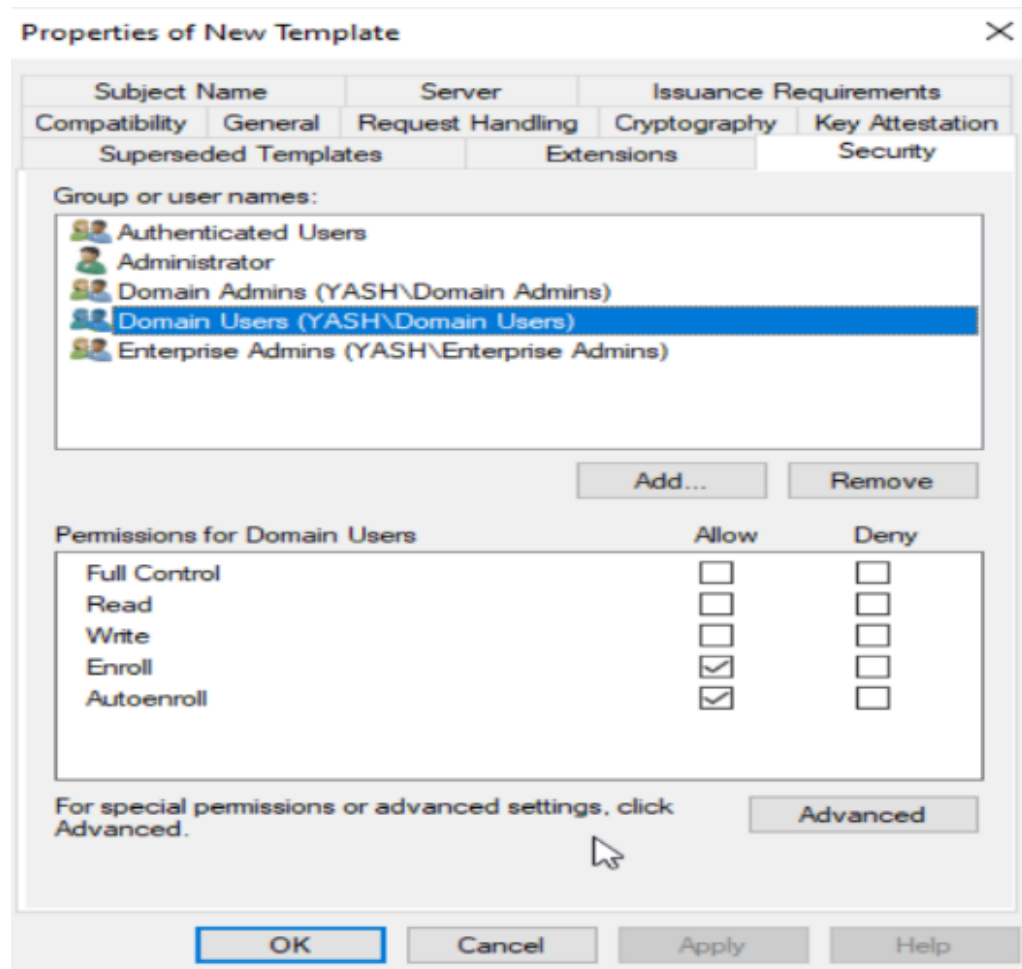


(Name the duplicate template.)

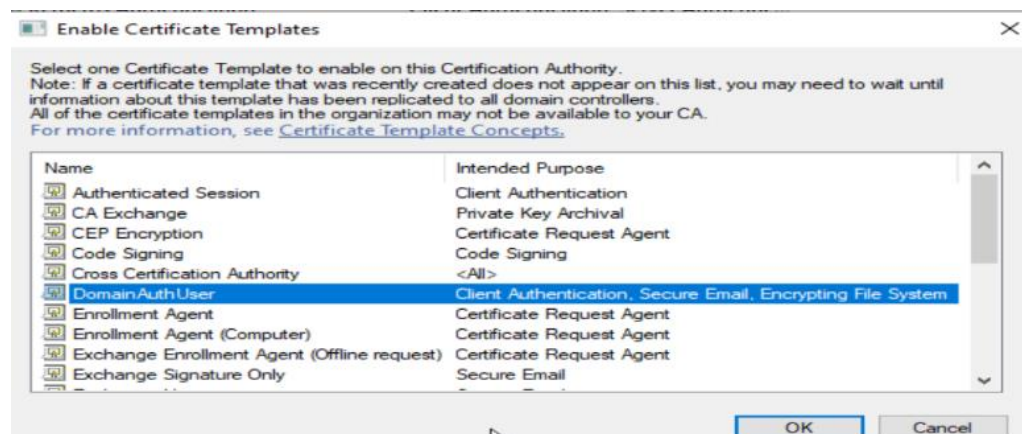


- **Issue the User Certificate Template and Enable Auto-Enrollment**

Issue the **User** certificate template for automatic enrollment to ensure that user devices automatically receive their certificates when they join the domain.



(Showing issuing the User certificate template)

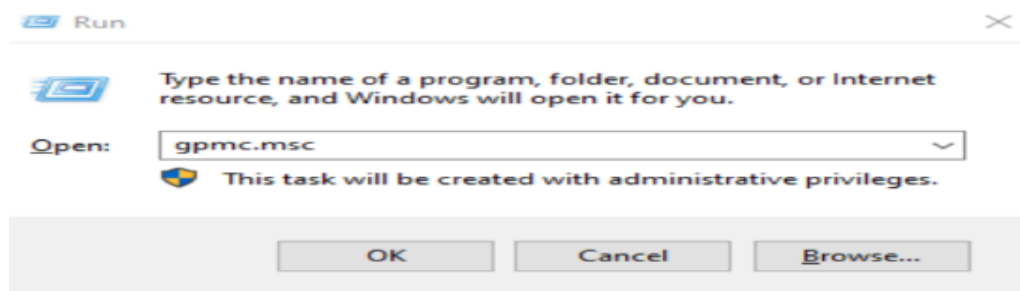


3.3 Configure Auto-Enrollment for User/Machine Certificates

To configure **auto-enrollment** for both user and machine certificates, automating the certificate enrollment and renewal process for both users and computers.

- **Open Group Policy Management Console (GPMC)**

The Group Policy Management Console (GPMC) is used to configure and enforce domain-wide policies. In this step, you'll configure the auto-enrollment policy, which will automate certificate issuance for users and computers.

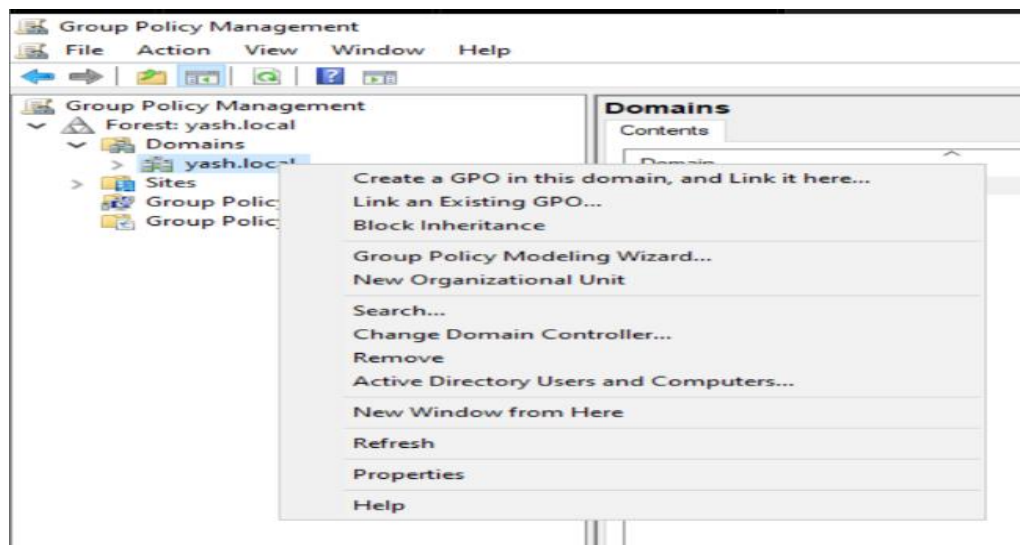


- **Create a New Group Policy Object (GPO) for Auto-Enrollment**

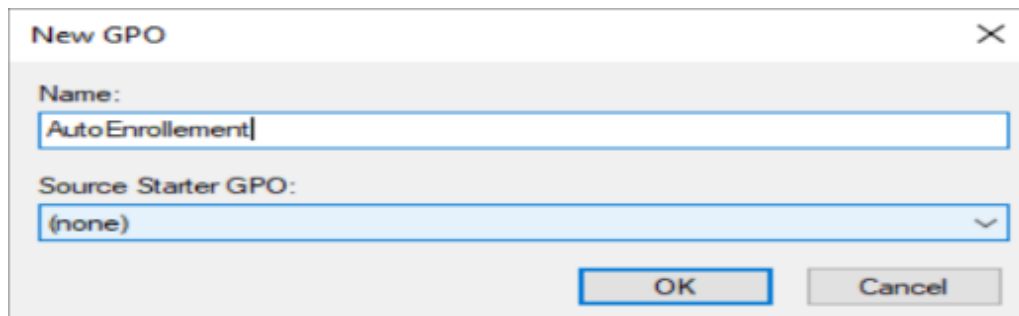
Create a new GPO specifically for auto-enrollment settings. This GPO will enforce the auto-enrollment policy across the domain, ensuring all domain users and computers automatically receive certificates.

Navigation Path:

GPMC > Right-click on the domain > Create a GPO and Link it here



(Name the new GPO.)

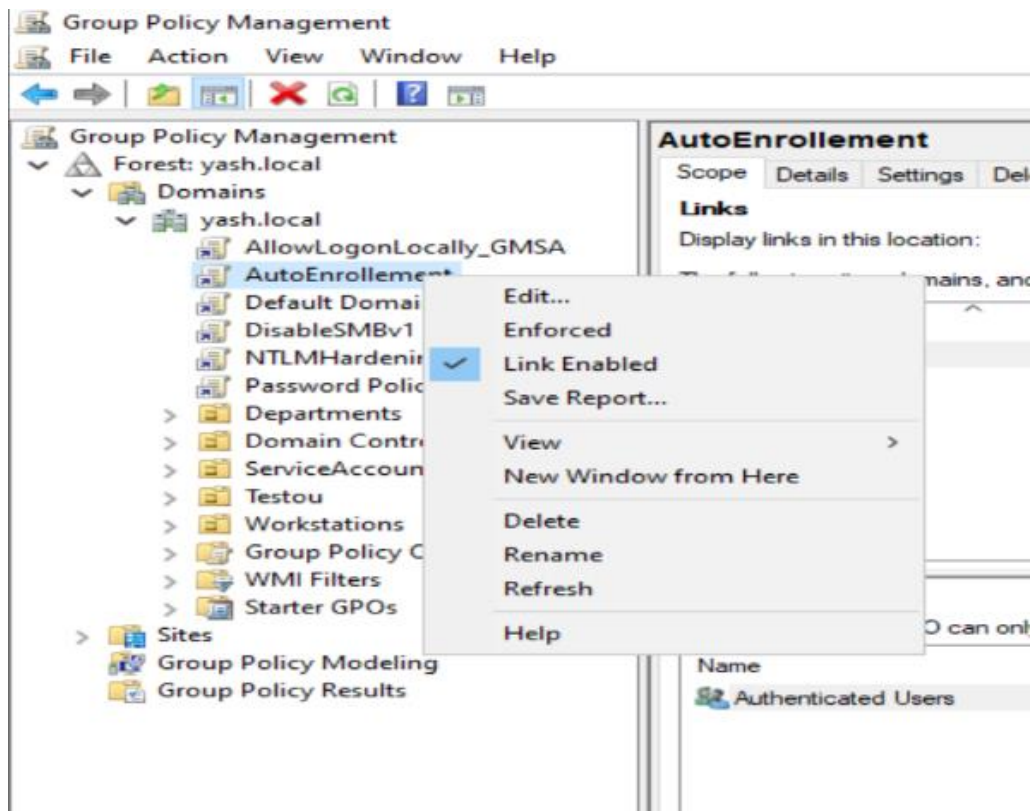


- **Edit the GPO and Enable Auto-Enrollment for Both User and Computer Certificates**

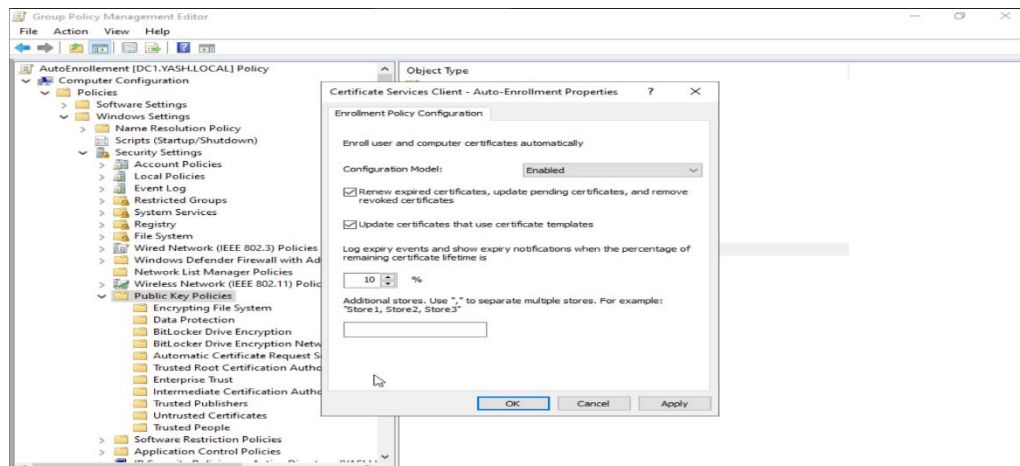
In the newly created GPO, configure the auto-enrollment settings to automatically enroll both users and computers.

Edit the GPO and navigate to:

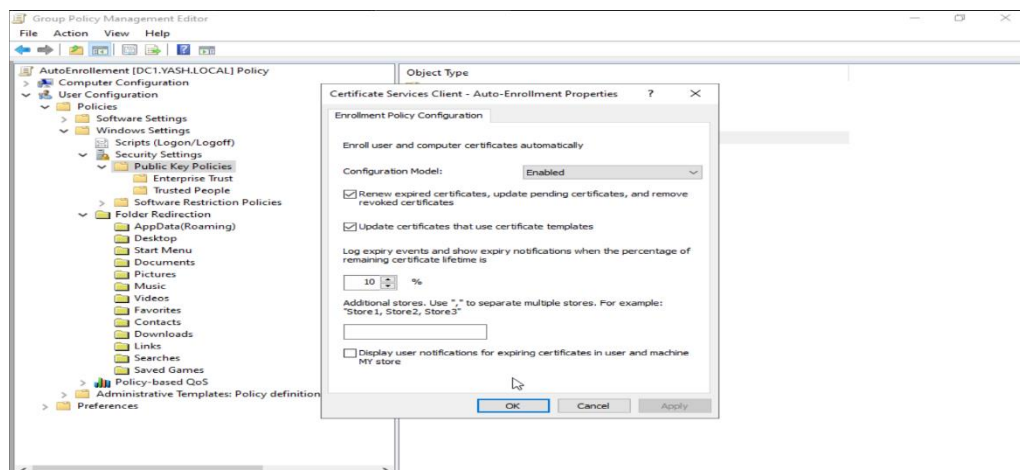
Computer Configuration > Policies > Settings > Security Settings > Public Key Policies



(Enabled the Auto-Enrollement Property for Computers.)

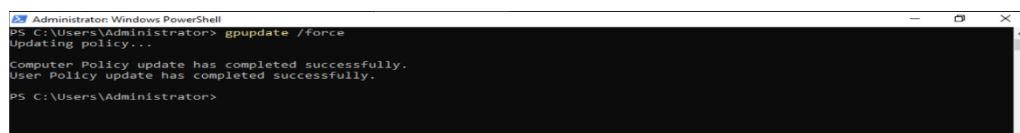


(Open the Auto-Enrollement Property for Users)



- **Force Group Policy Update**

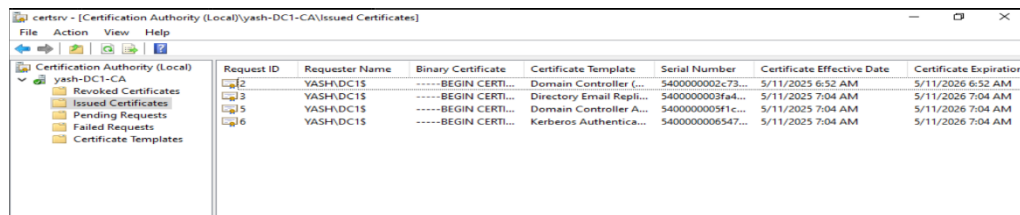
After configuring the GPO, force a Group Policy update to ensure the changes take effect immediately.



- **Verify Through Issued Certificates**

After applying the GPO and forcing the update, verify that certificates have been issued and auto-enrolled for users and computers.

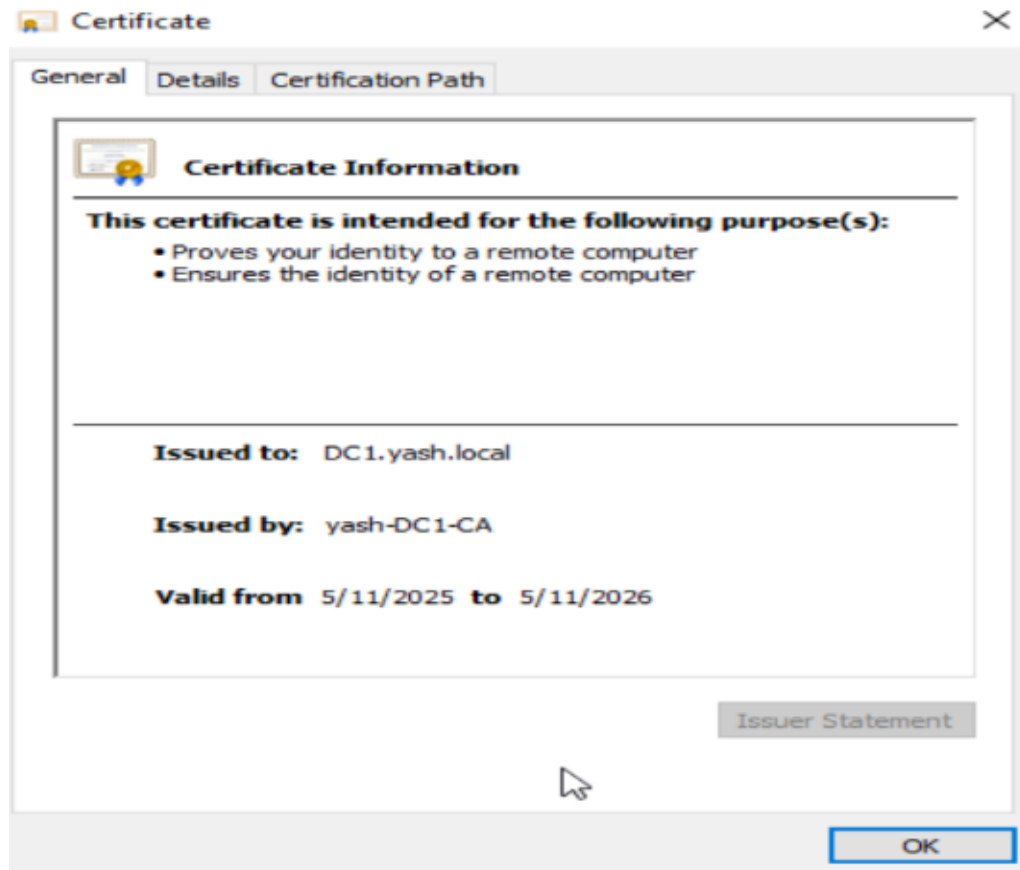
(Verify the certificate which was issued)



The screenshot shows the 'certsrv - [Certification Authority (Local)\yash-DC1-CA\Issued Certificates]' window. The left pane shows the tree structure with 'Issued Certificates' selected. The right pane displays a table of issued certificates.

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration
42	YASH.DC15	-----BEGIN CERTI...	Domain Controller (...)	5400000002c73...	5/11/2025 6:52 AM	5/11/2026 6:52 AM
3	YASH.DC15	-----BEGIN CERTI...	Directory Email Repl...	5400000009f4...	5/11/2025 7:04 AM	5/11/2026 7:04 AM
5	YASH.DC15	-----BEGIN CERTI...	Domain Controller A...	5400000005f1c...	5/11/2025 7:04 AM	5/11/2026 7:04 AM
16	YASH.DC15	-----BEGIN CERTI...	Kerberos Authentica...	5400000006547...	5/11/2025 7:04 AM	5/11/2026 7:04 AM

(Issued by Root CA)



4. Results And Findings

This section presents the observed outcomes after implementing Active Directory Certificate Services (AD CS), issuing domain certificates, and configuring auto-enrollment. The findings are based on system behavior, certificate issuance status, and policy application.

- **Successful Installation of AD CS and Root CA**

The Root CA was installed and configured successfully on the domain controller, laying the foundation for issuing internal certificates.

- **Custom Certificate Templates Created and Issued**

Both user and computer certificate templates were duplicated, customized, and successfully published for auto-enrollment.

- **Auto-Enrollment via Group Policy Functioned as Intended**

After GPO configuration and gpupdate, both domain users and computers automatically received their respective certificates.

- **Issued Certificates Verified in Certificate Store**

Certificates appeared correctly under **certmgr.msc** for both users and machines, confirming proper issuance and trust by the CA.

- **Seamless Integration With AD Environment**

The certificate system integrated smoothly with Active Directory, with no manual intervention needed post-GPO setup.

5. Recommendations

This section outlines suggested actions to optimize and maintain the certificate infrastructure based on the implementation findings. These recommendations aim to improve security, performance, and manageability.

- **Regularly Audit Certificate Usage and Expiry**

Periodically check issued certificates to ensure compliance and to identify any expired or unused certificates.

- **Implement Certificate Revocation Policies**

Set up Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) for real-time revocation checking.

- **Use Role Separation for CA Administration**

Assign different roles to manage CA tasks (e.g., auditing, template management) to improve security and control.

- **Backup CA Private Key and Configuration**

Take regular backups of the CA's private key, certificate database, and configuration to ensure disaster recovery readiness.

- **Consider Deploying a Subordinate CA (Optional)**

For larger environments, introduce a subordinate CA to offload certificate issuance and reduce exposure of the root CA.

6. Conclusion

The implementation of Active Directory Certificate Services (AD CS) has successfully laid the groundwork for a robust and secure certificate-based authentication system within the domain environment. By configuring a standalone Root Certification Authority (CA), the organization now has centralized control over the issuance, renewal, and management of digital certificates. The customization and publication of user and computer certificate templates ensured that certificates meet specific organizational security policies, allowing for tailored certificate usage and compatibility with various enterprise services such as secure email, VPN, TLS encryption, and wireless authentication.

One of the most significant outcomes of this deployment is the successful configuration of certificate auto-enrollment using Group Policy. This eliminates the need for manual certificate requests and ensures that both users and devices automatically receive and renew certificates with minimal administrative intervention. This not only improves operational efficiency but also strengthens security by maintaining up-to-date credentials across the domain.

Moreover, the ability to monitor issued certificates and verify their presence through tools like certmgr.msc provides assurance of the system's reliability and correct configuration. The implementation aligns with best practices in enterprise security, supports compliance with

regulatory frameworks, and prepares the organization for scalable and future-ready identity and access management enhancements. Overall, the project has significantly improved the organization's cybersecurity posture and has established a foundation that can support broader PKI services in the future.