PHASE 10: Certificate Authority + Certificate Templates

Build a secure internal PKI infrastructure with Active Directory Certificate Services (AD CS), issue certificates for Wi-Fi (802.1x), BitLocker recovery, VPN, RDP, and user/device authentication.

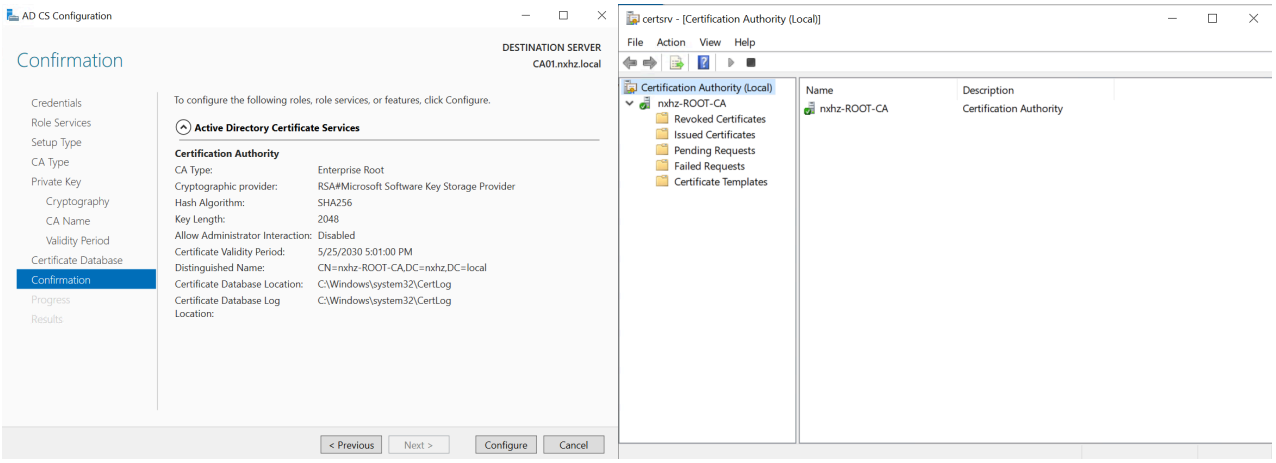
We will:

- Deploy an Enterprise Root CA on Windows Server
- Create and issue custom certificate templates
- Enable auto-enrollment via GPO and Intune
- Test and document certificate deployment

I. Setup Enterprise Root Certificate Authority (CA)

Actions Completed:

1. Provision CA01 VM (Repeat Phase 9: Step 1)
    - Deployed a Windows Server 2022 VM named CA01 (2 vCPUs, 4 GB RAM, 127 GB disk) and joined it to dipeshcorp.local.
2. Install AD CS Role
    - Installed Active Directory Certificate Services
    - AD CA Confuguration:
        - Selected Change and put DC01 Administrator Credential
        - Select > Certification Authority
        - Setup Type: Enterprise Root CA with RSA 2048-bit.
        - CA Name: dipeshcorp-ROOT-CA
3. Start CA Service: Opened certsrv.msc and verified dipeshcorp-ROOT-CA is running.



II. Create & Issue Certificate Templates

Actions Completed:

Step 1: Opened Certificate Templates Management

1. Opened the Certificate Authority Console:
   - Pressed Win + R, typed certsrv.msc, and hit Enter.
   - This opened the Certificate Authority management console.
2. Navigated to Certificate Templates:
   - In the left pane, expanded the Certificate Authority node.
   - Right-clicked on Certificate Templates and selected Manage. This opened the Certificate Templates Console.

Step 2: Duplicated Certificate Templates

Once I was in the Certificate Templates Console:

1. Located the Template to Duplicate:
   - Expanded the list under Certificate Templates to locate the template I wanted to duplicate. For example:

        - "Basic EFS" for BitLocker recovery.
        - "Computer" for Wi-Fi/VPN.
        - "User" for User Logon Certificates.

🛑 Error:

"You do not have sufficient permissions to modify the certificate templates".

✔️ Resolution:

- Open Active Directory Users and Computers on DC01, locate Dipesh's account, and right-click to select Properties.
- Go to the Member Of tab, click Add, type Enterprise Admins, and click Check Names, then click OK.
- On CA01, open Command Prompt or PowerShell and run gpupdate /force to update the policy.

2. Duplicated the Template:
    - Right-clicked on the template (e.g., "Basic EFS", "Computer", or "User") and selected Duplicate Template.
3. Modified the Duplicate Template:
    - After duplicating the template, I modified the settings based on the requirements.
4. For each template:
    - Template 1: BitLocker Recovery Agent (Duplicated "Basic EFS"):
        - Set Encryption: Under the Cryptography tab, enabled encryption.
        - Published: Ensured the template was published to Active Directory by checking the Publish in Active Directory option in the template properties.
    - Template 2: Wi-Fi/VPN (Computer Auth) (Duplicated "Computer"):
        - Set Signature and Encryption: Under the Cryptography tab, ensured Signature and Encryption were enabled.
        - Smartcard Settings: Under the Request Handling tab, checked Allow Smartcard.
        - Enrollment Permissions: Under the Security tab, set Domain Computers with Enroll and Read permissions.
    - Template 3: User Logon Certificate (Duplicated "User"):

- Set Subject as UPN: Under the Subject Name tab, set the subject to User Principal Name (UPN) for the certificate to be issued based on the user's email/UPN.
- Enrollment for Authenticated Users: Under the Security tab, set Authenticated Users with Enroll permissions.

Step 3: Published the Templates

1. Published the Templates in Certificate Authority:

○ Went back to Certificate Authority (the first window opened).

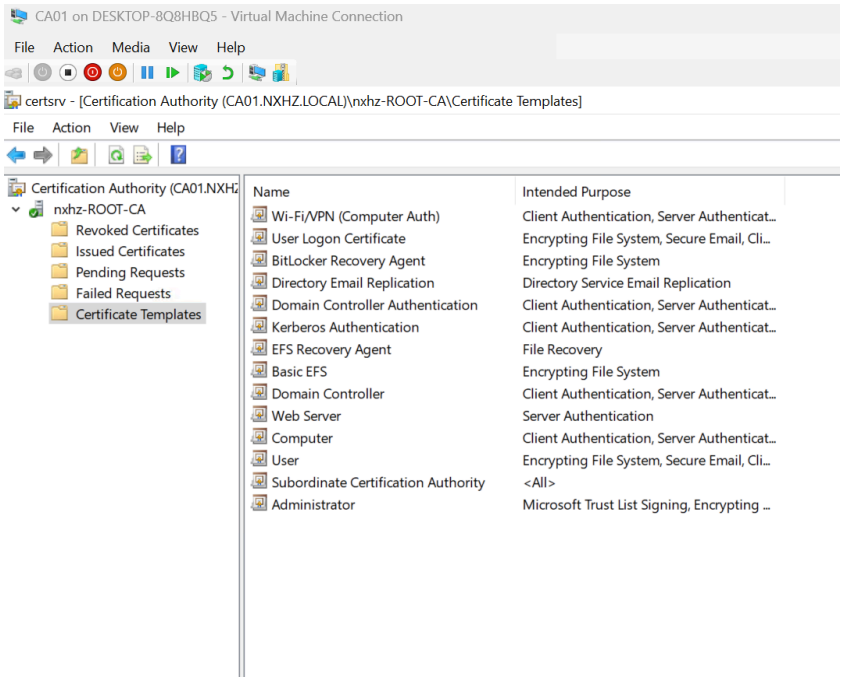
○ Right-clicked on Certificate Templates and selected New → Certificate Template to Issue.

○ In the window that appeared, selected the 3 templates (e.g., BitLocker, Wi-Fi/VPN, User Logon) and clicked OK.

2. Verified the Templates:

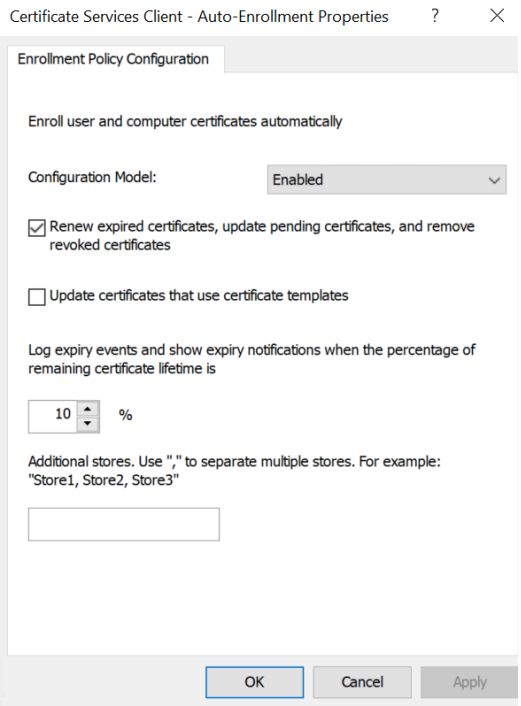
○ Checked AD CA to verify that the templates were listed under Certificate Templates.

○ Ensured that the templates were available for enrollment across the domain and ready to issue certificates for BitLocker recovery, VPN authentication, and user logon.



III. Enable Auto-Enrollment

- GPO for On-Prem Devices
  - Step 1: Create GPO
    - On DC01 → Group Policy Management → Created GPO: “AutoEnroll Certificates” → Linked to OU=Workstations
  - Step 2: Enable Auto-Enrollment Policy
    - Navigated to: Computer Config → Policies → Windows Settings → Security Settings → Public Key Policies → Enabled Auto-Enrollment and set to renew/remove revoked



✅ Now, domain-joined and Intune-managed devices will auto-enroll.