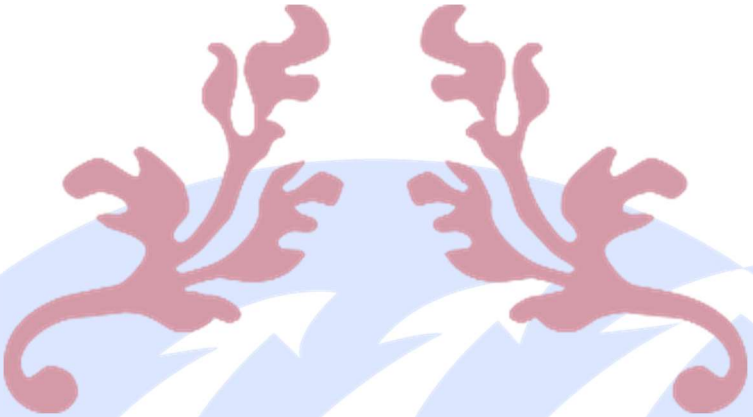
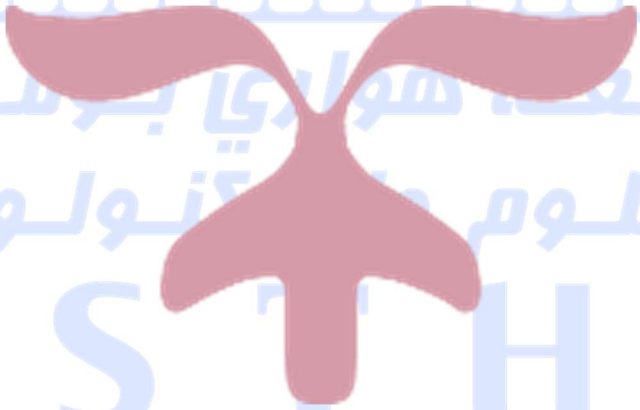


CONFIGURATION OF A CERTIFICATION AUTHORITY AND IIS SERVER

By BOUBEKEUR Mohend



MARCH 17, 2023

FACULTY OF COMPUTER SCIENCE

Contents

Definitions:

Internet Information Services (IIS): Internet Information Services (IIS) is a flexible and versatile web server developed by Microsoft, which runs on Windows systems to serve HTML pages or requested files. We will use it to host our webpage.

Certification Authority (CA): A certification authority is a company, organization, or entity responsible for validating the identities of entities (such as websites, email addresses, businesses, or individuals) and linking them to cryptographic keys by issuing electronic documents called digital certificates. In our case, we will use a local certification authority.

The purpose of using a certification authority in our network is to establish a trusted infrastructure for secure communication and authentication. By implementing a Certification Authority (CA), we ensure that all entities within our network can be verified and authenticated reliably. This enhances the security of our network by:

- **Authenticating Entities:** The CA verifies the identities of various entities such as servers, clients, and users within our network. This ensures that only authorized entities can access resources and services.

- **Secure Communication:** The digital certificates issued by the CA facilitate secure communication by encrypting data transmitted between entities. This encryption helps prevent unauthorized access and eavesdropping, thus protecting sensitive information.

- **Preventing Man-in-the-Middle Attacks:** Through the use of digital certificates signed by the CA, we can detect and prevent man-in-the-middle attacks, where a malicious actor intercepts communication between two parties.

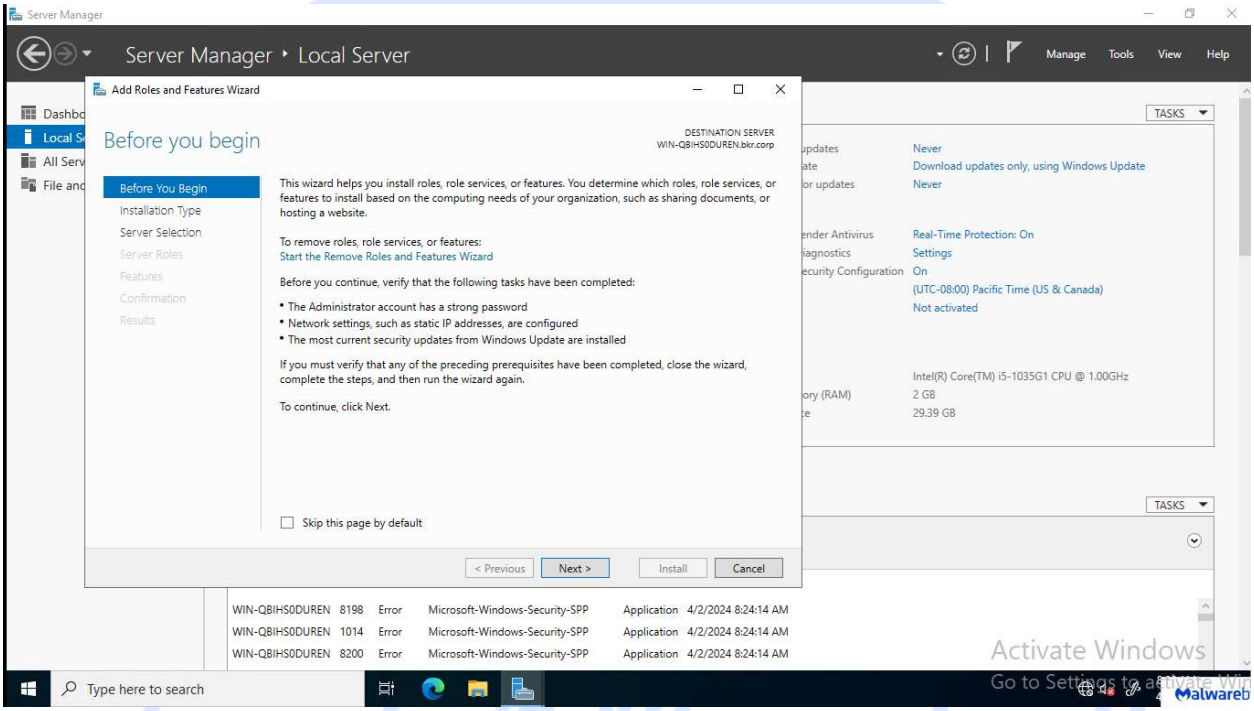
Configuration Steps:

Below are step-by-step instructions. You will simply need to replicate the screenshots.

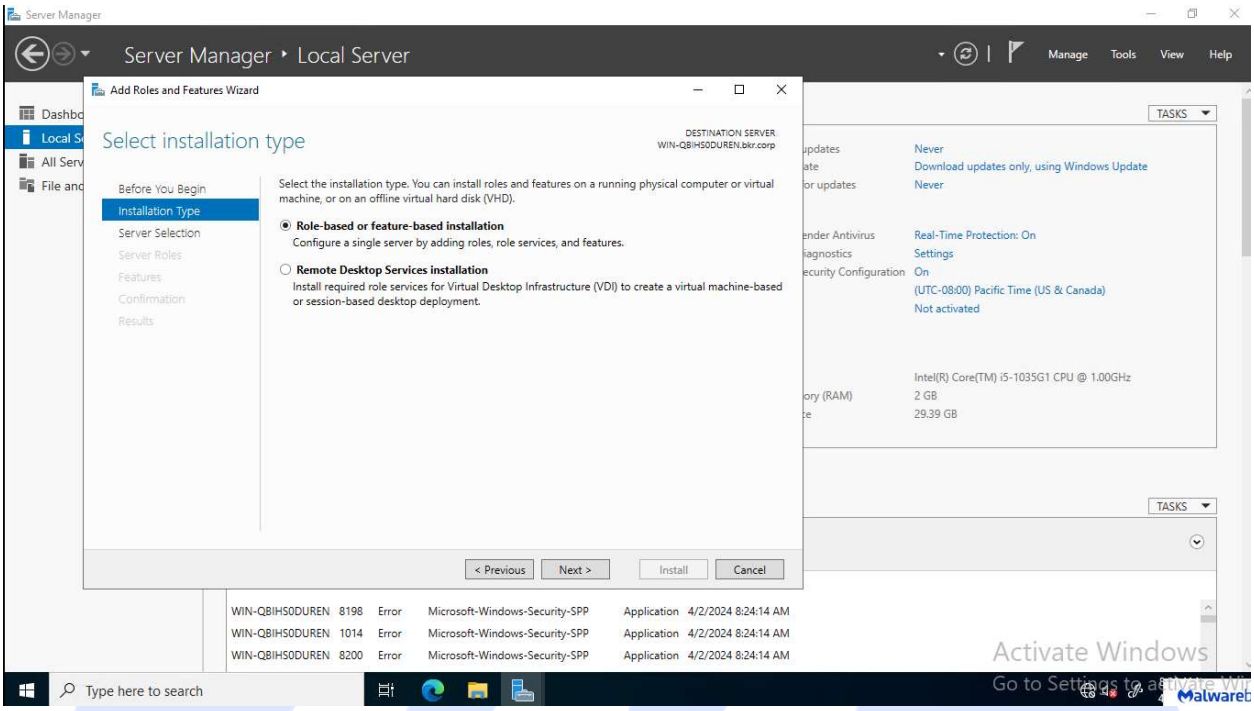
- **Step 1: Creating a Domain and Promoting Your Current Machine to a Domain Controller:**

To begin, we will create a domain and transform your current machine into a domain controller.

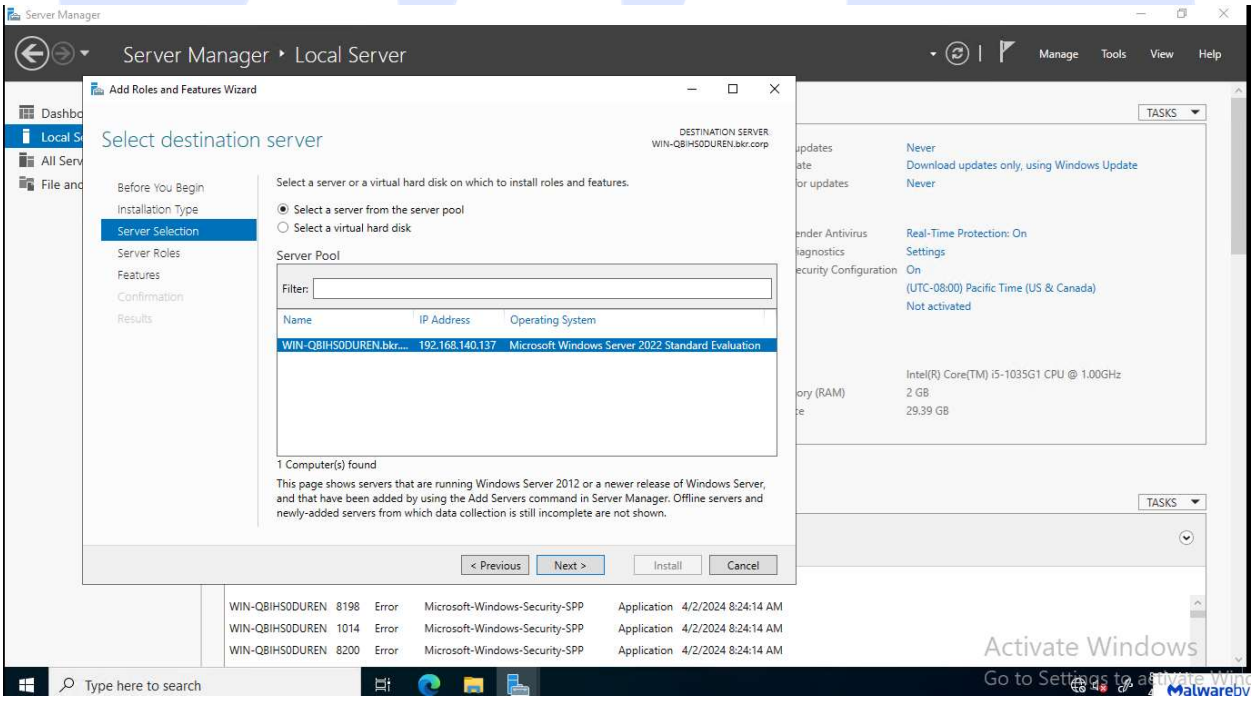
- Open the "Server Manager" by clicking on the "Start" menu, selecting "Windows Administrative Tools," and then clicking on "Server Manager."
- In the Server Manager window, click on "Add roles and features" from the Dashboard or the Manage menu.



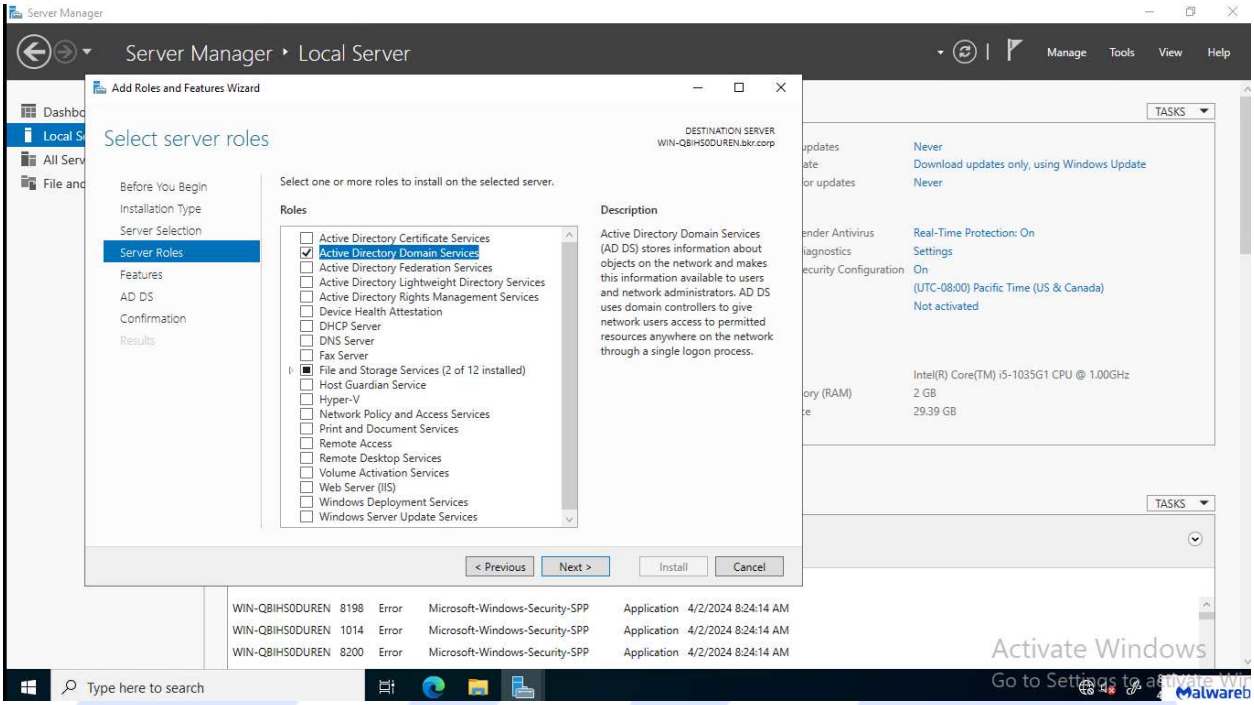
The Add Roles and Features Wizard will appear. Click "Next" to proceed.



Select "Role-based or feature-based installation" and click "Next."



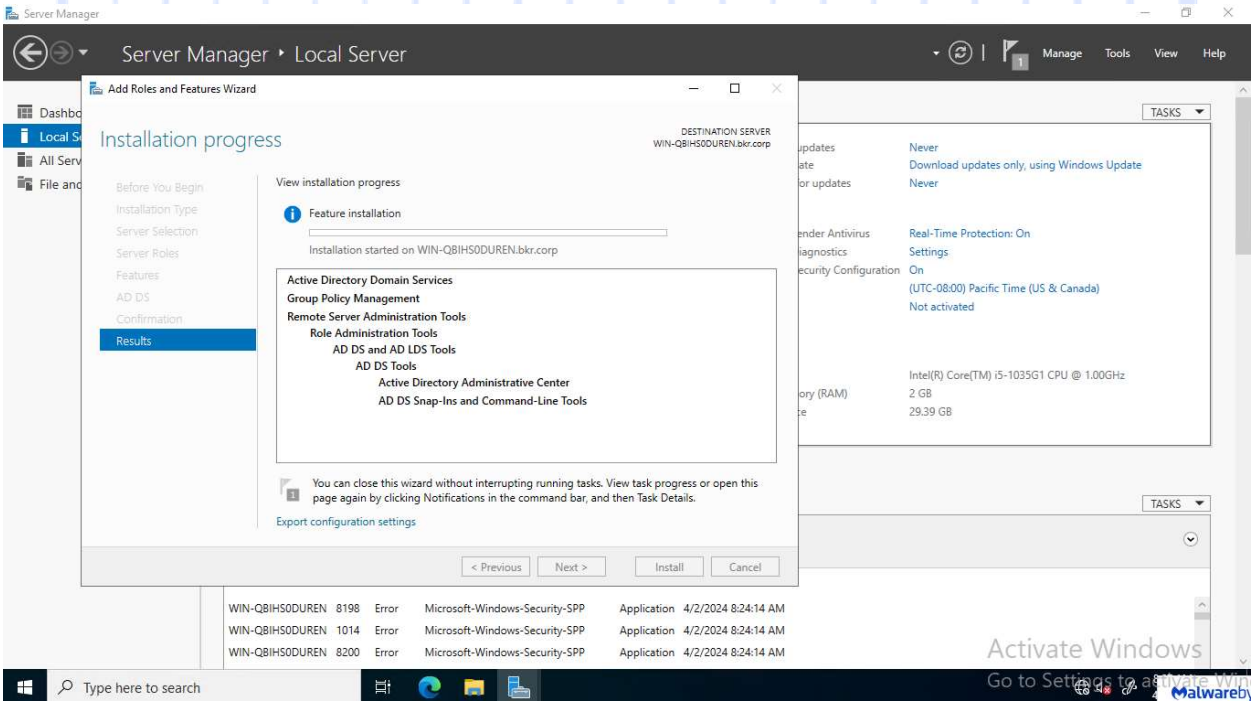
Choose the server you want to install the Active Directory Domain Services role on. If it's the local server, it should be selected by default. Click "Next" to continue.



In the Roles section, select "Active Directory Domain Services." A window will pop up, prompting you to add features required for Active Directory Domain Services. Click "Add Features" and then click "Next."

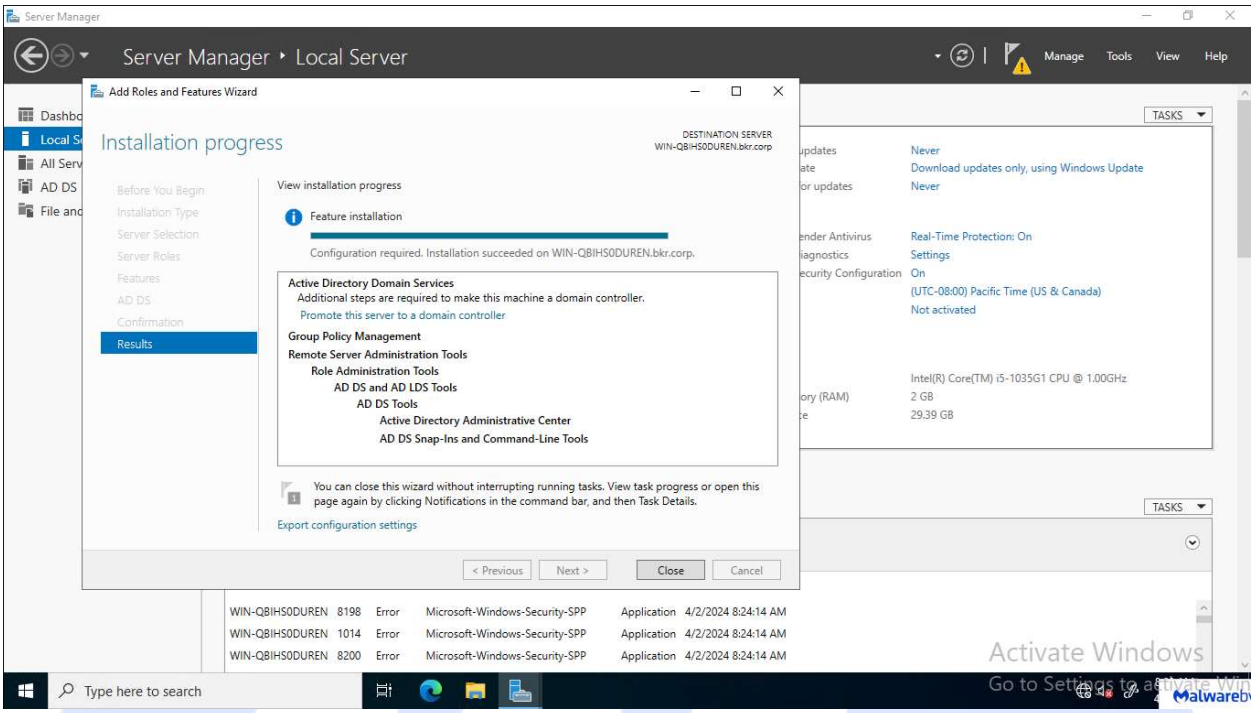
Review the information provided about Active Directory Domain Services, and then click "Next."

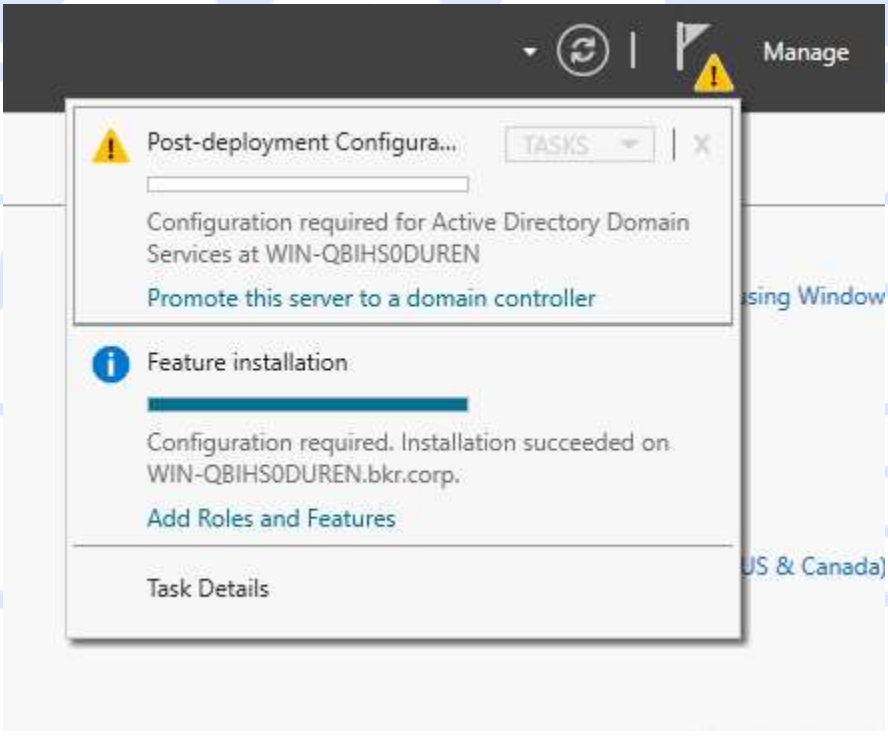
On the Features page, you can skip this step as no additional features are required. Click "Next."



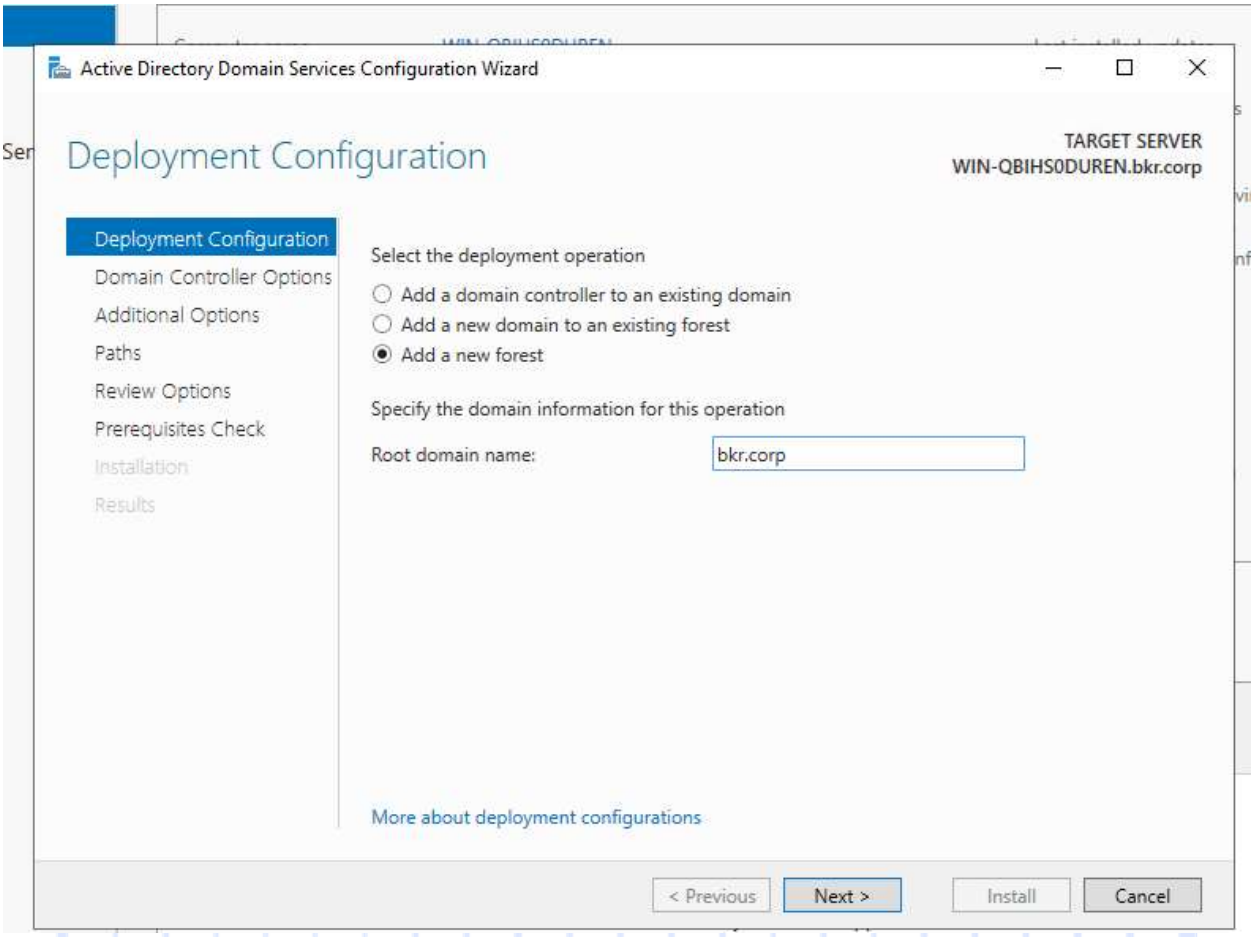
Click "Next" through the "AD DS" sections until you reach the "Confirmation" page.

Review the selections you've made, and then click "Install" to begin the installation process.



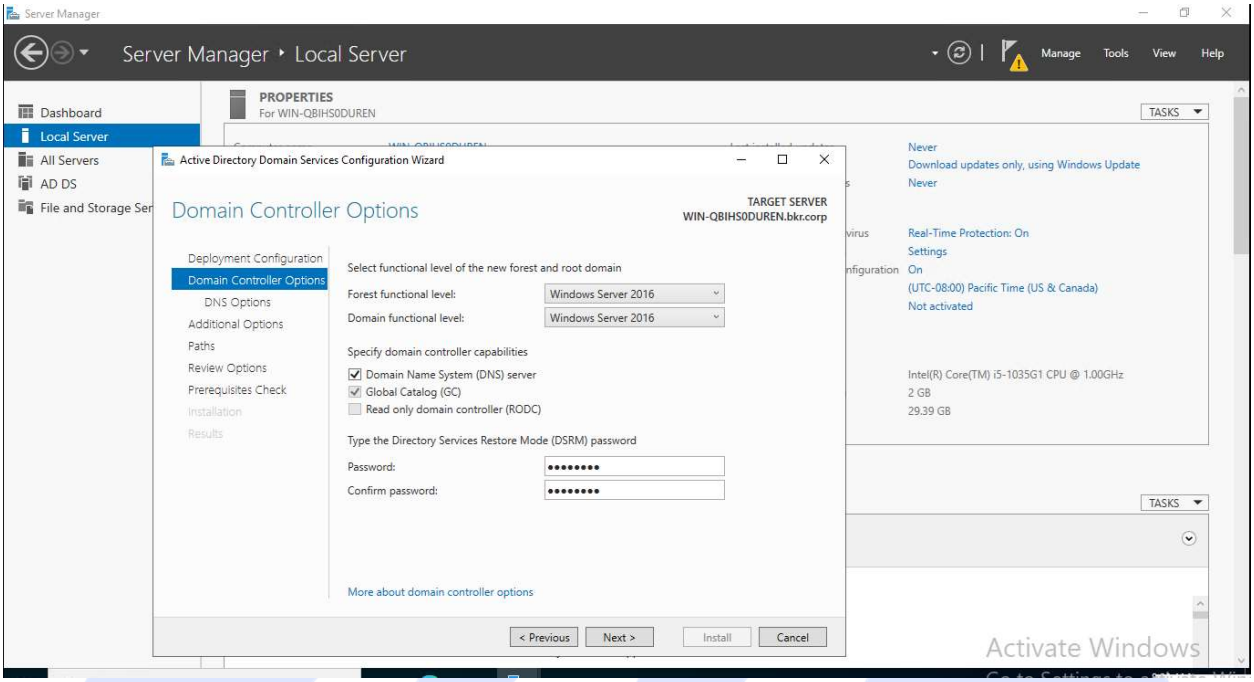


Once the installation is complete, click on the "Promote this server to a domain controller" link in the "Notifications" section of the Server Manager.

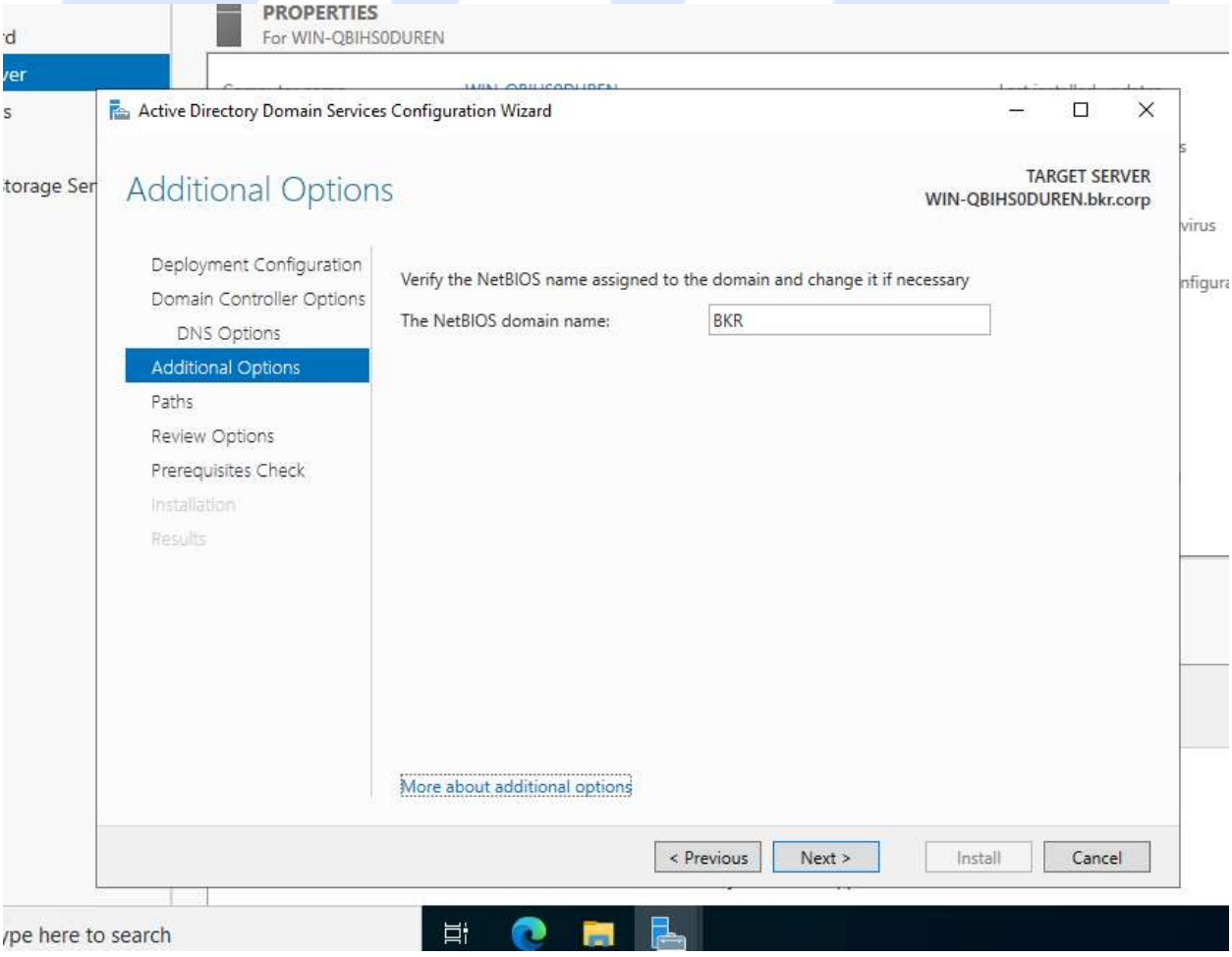


The Active Directory Domain Services Configuration Wizard will appear. Select "Add a new forest" if you're creating a new domain. Enter the root domain name for your Active Directory forest in the "Root domain name" field. Click "Next" to continue.

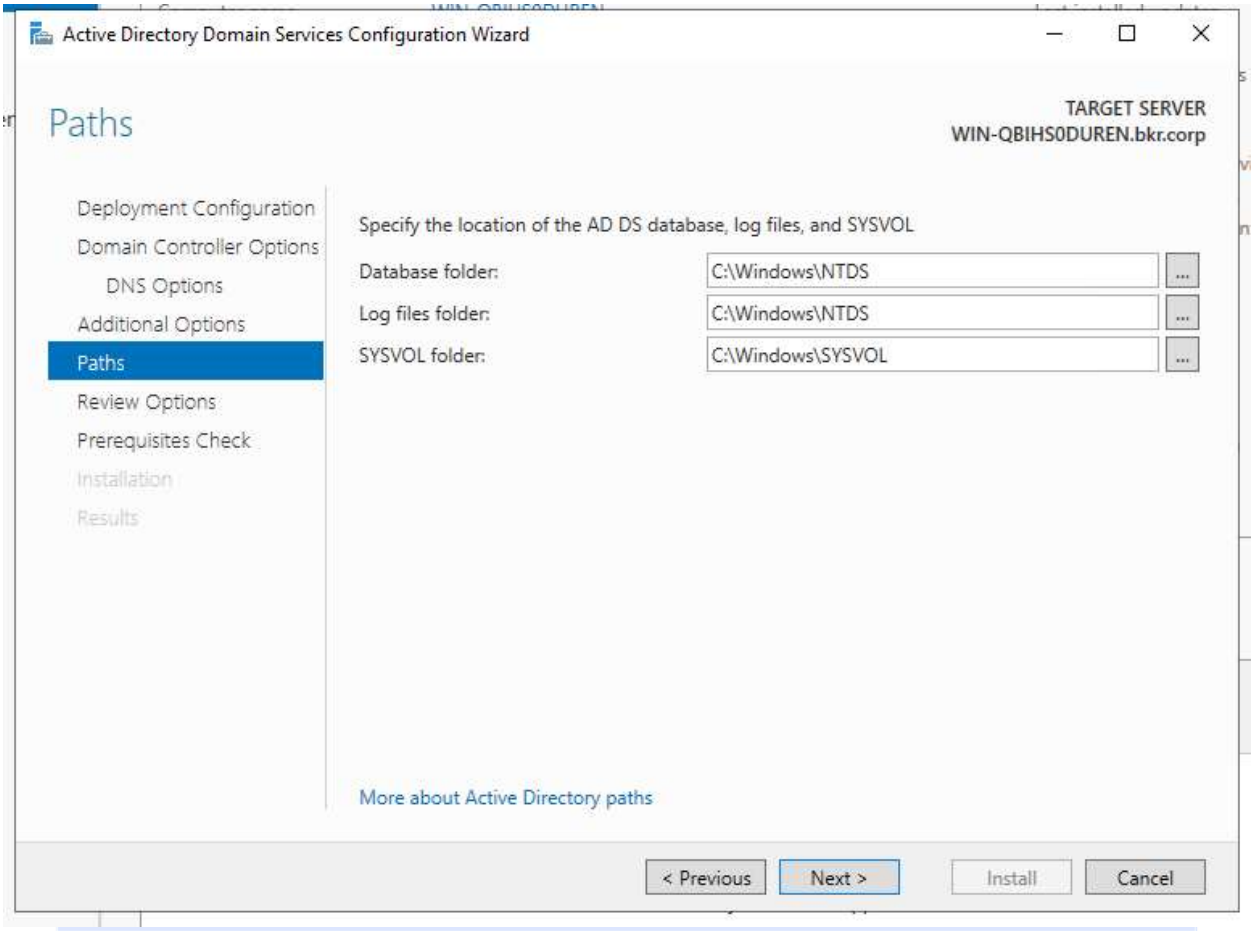
Choose the Forest Functional Level and Domain Functional Level according to your requirements. Click "Next."



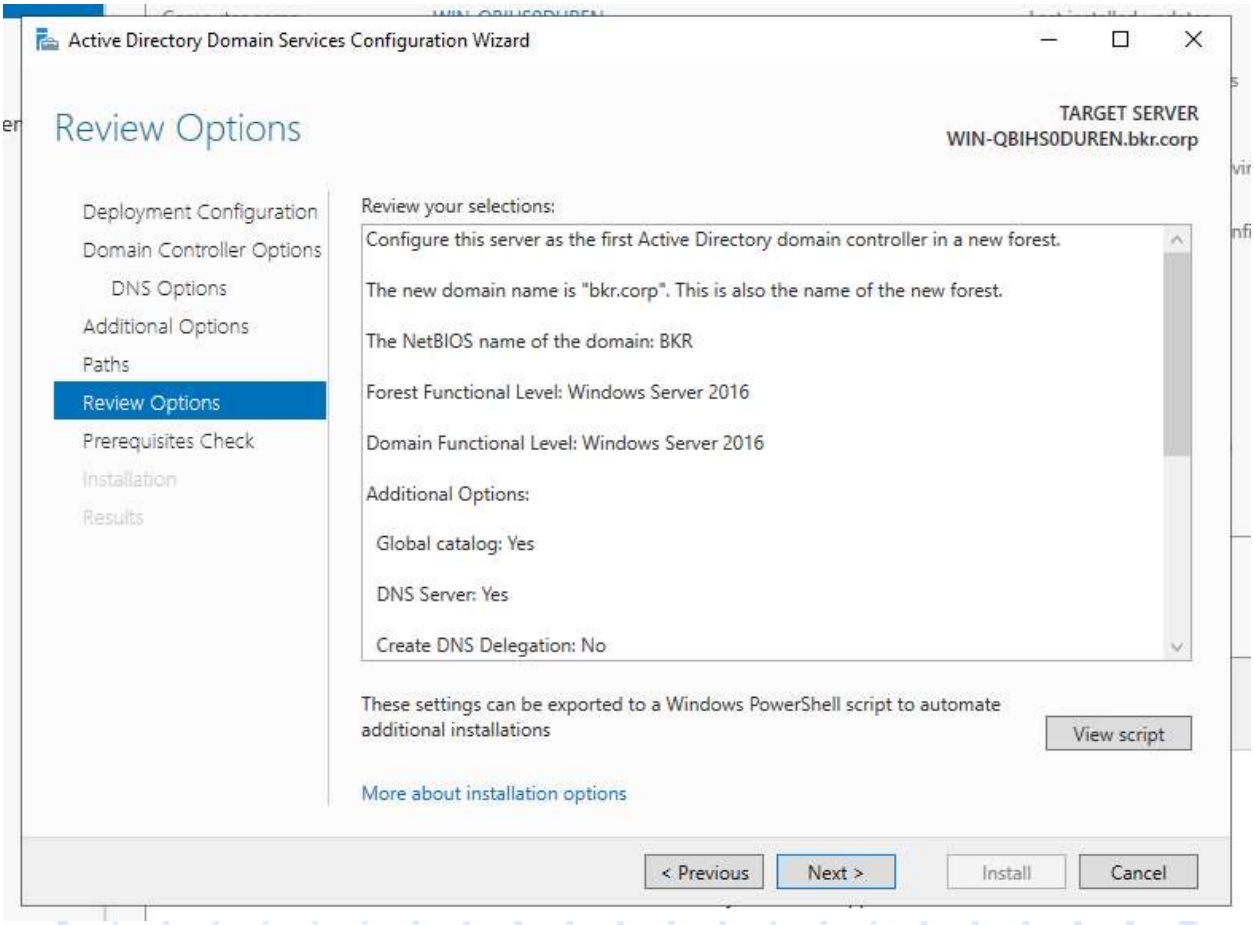
Specify a Directory Services Restore Mode (DSRM) password and click "Next."



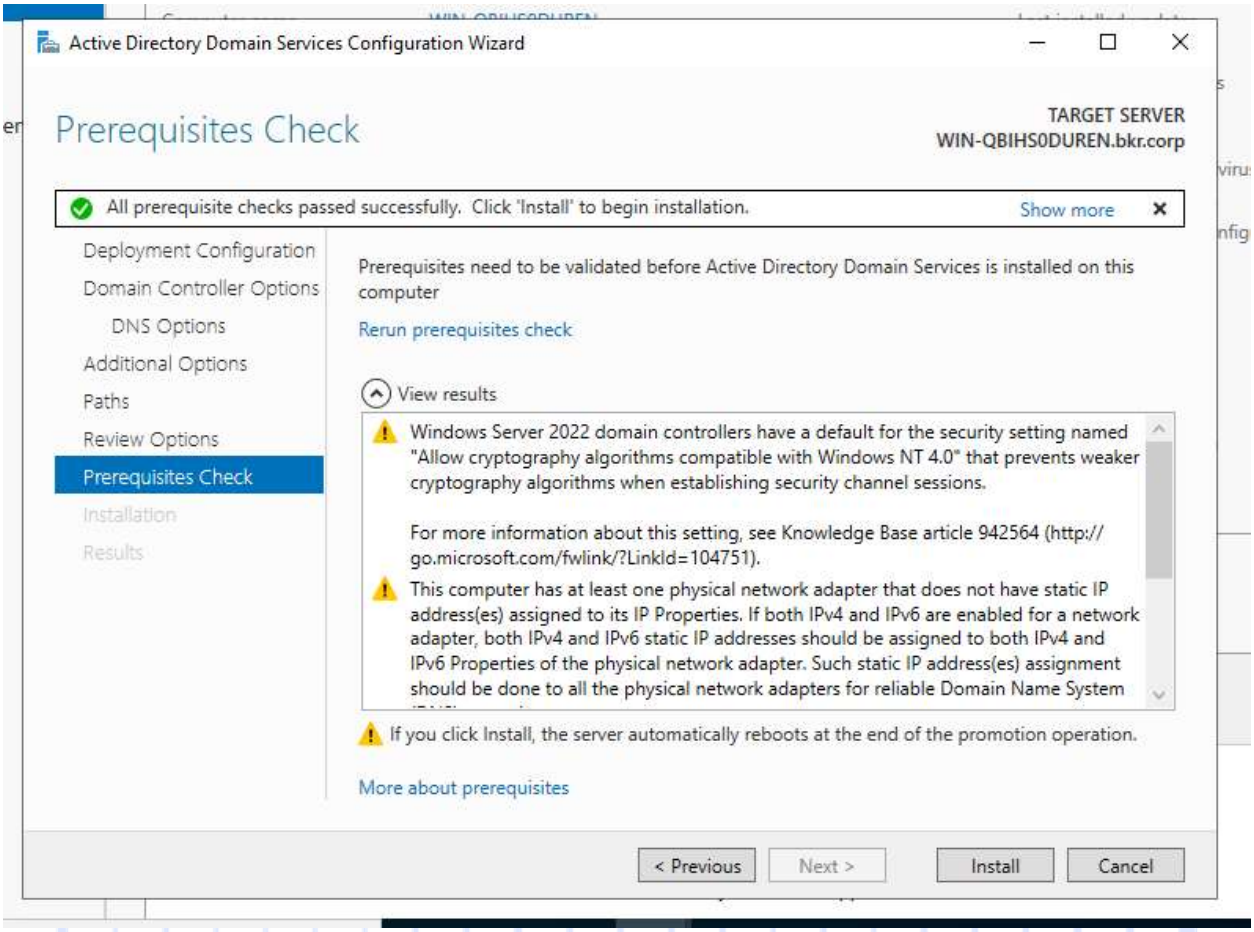
Review the NetBIOS domain name, and then click "Next."



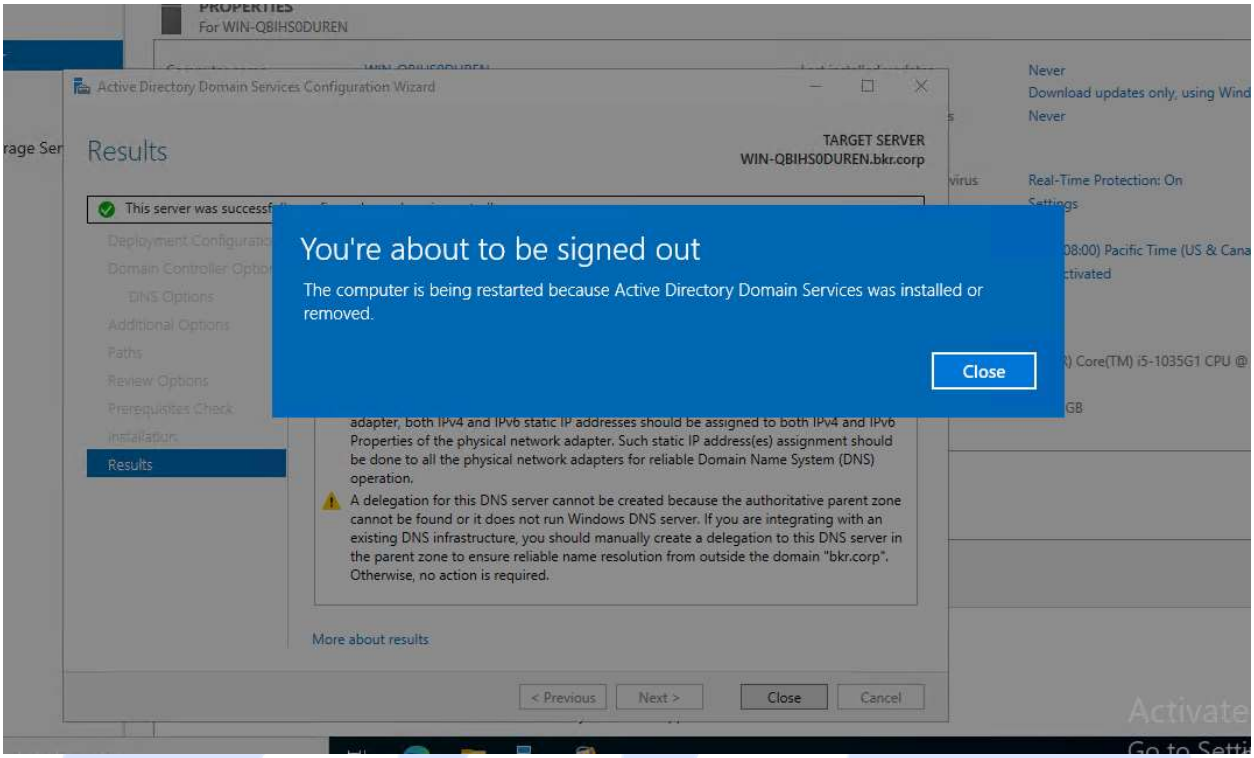
On the Paths page, you can leave the default paths as they are. Click "Next."



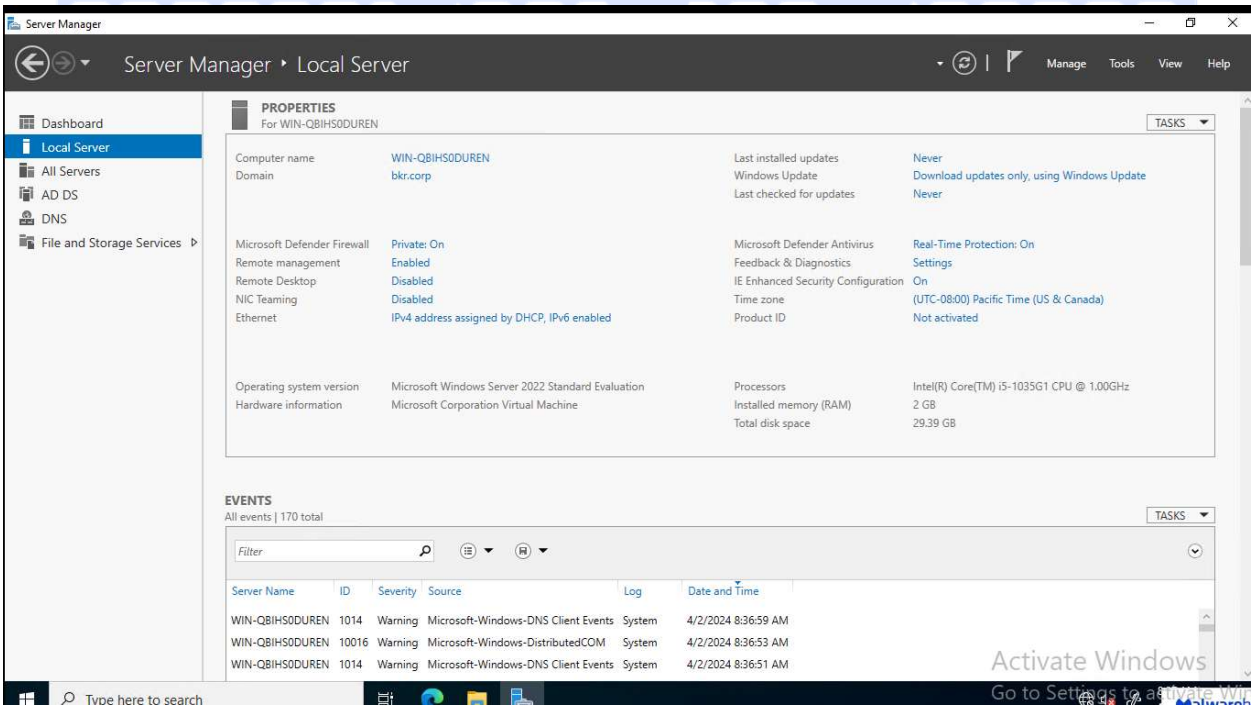
Review your selections on the Review Options page, and then click "Next" to proceed.



The prerequisite checks will be performed. If everything is successful, click "Install" to begin the installation process.



Once the installation is complete, your server will restart automatically. After the restart, your machine will be transformed into a domain controller, and you'll have successfully created a new domain.



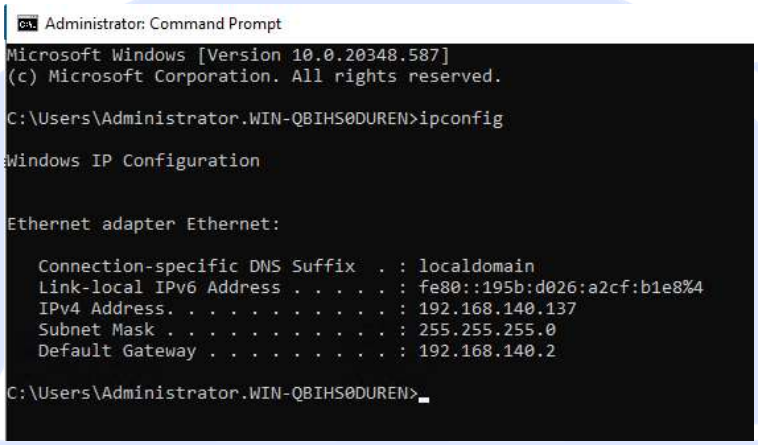
You can now log in using the domain credentials you specified during the promotion process.

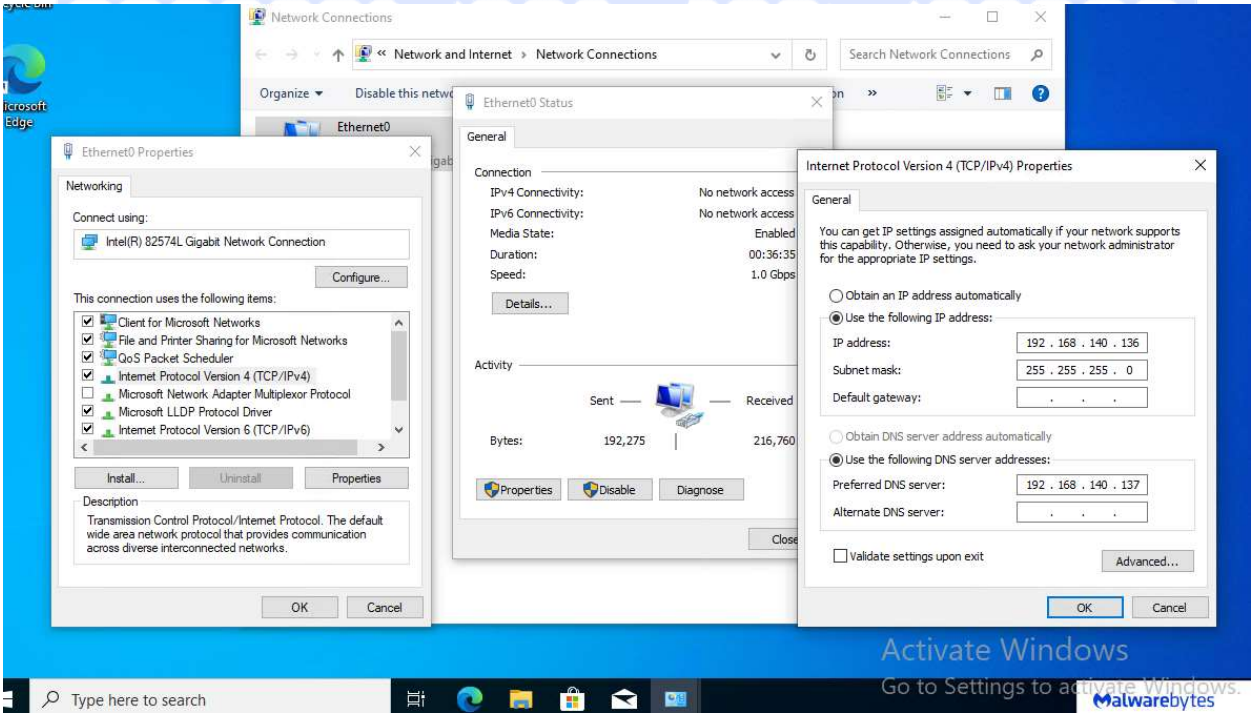
- ## Step 2: Adding the Client to the Domain:

We need to add a client to the domain to verify that our configuration is working as expected. On the client machine, before proceeding with joining the client to the domain, it's essential to ensure proper connectivity between the machines and configure the DNS settings on the client machine to point to the domain controller's IP address. Follow these steps to join the domain we created earlier:

Note: Ensure VMs are in the same network

On the client machine, open the network adapter settings by typing **"ncpa.cpl"** in the search bar and pressing Enter. This will open the Network Connections window directly.



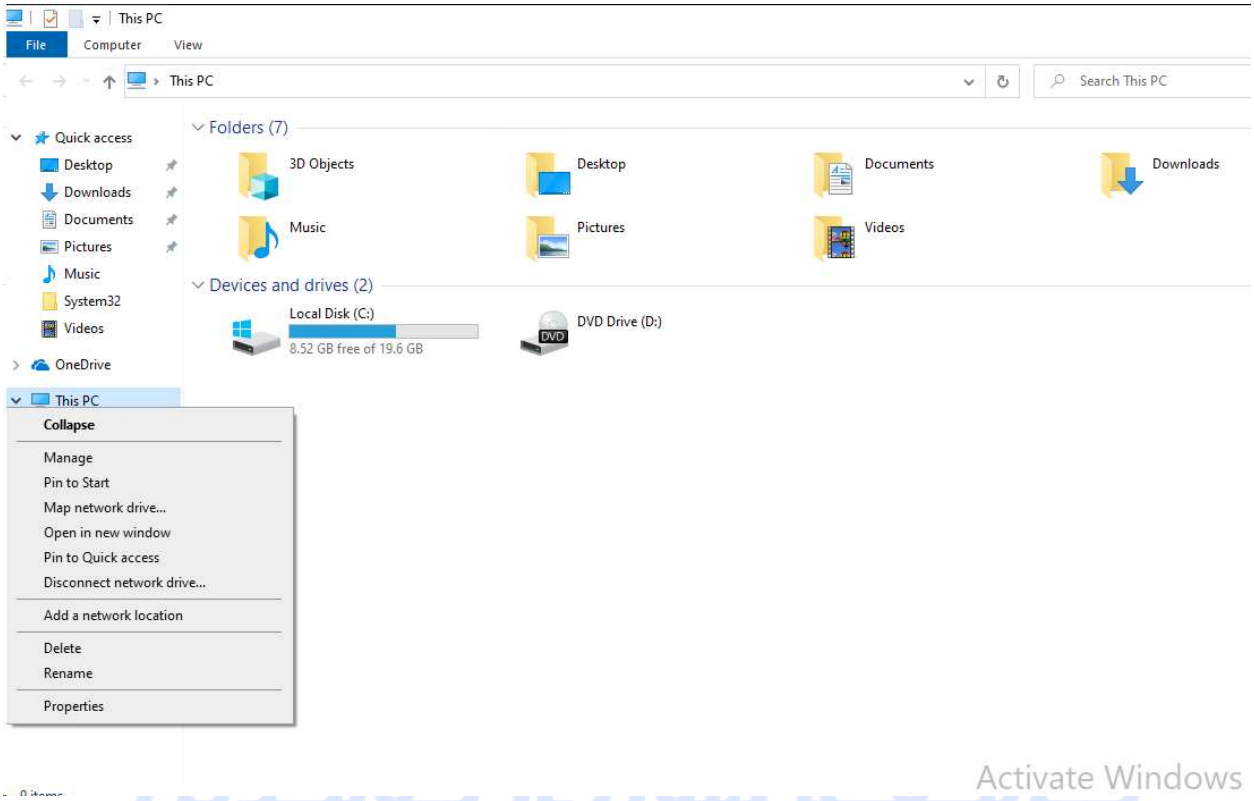


Right-click on the network adapter that is currently active and select "Properties".

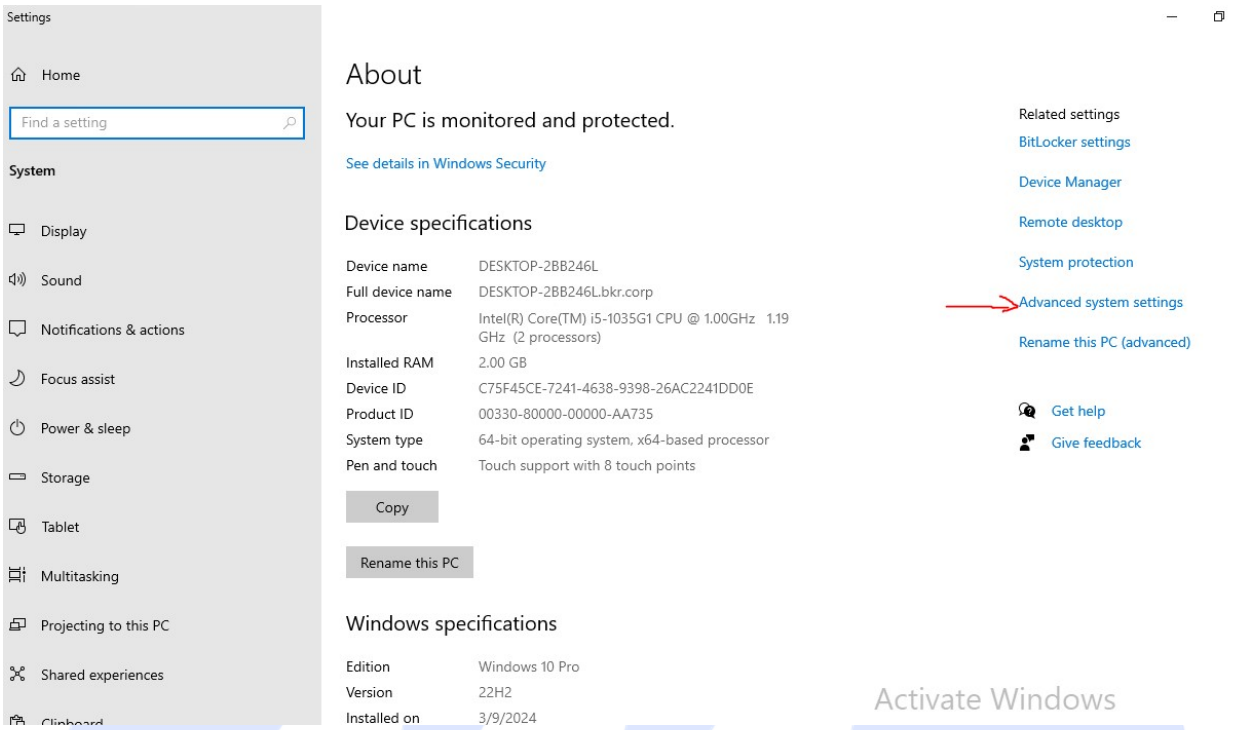
In the Properties window, scroll down and select "Internet Protocol Version 4 (TCP/IPv4)" and then click on the "Properties" button.

In the IPv4 properties window, select the option "Use the following DNS server addresses".

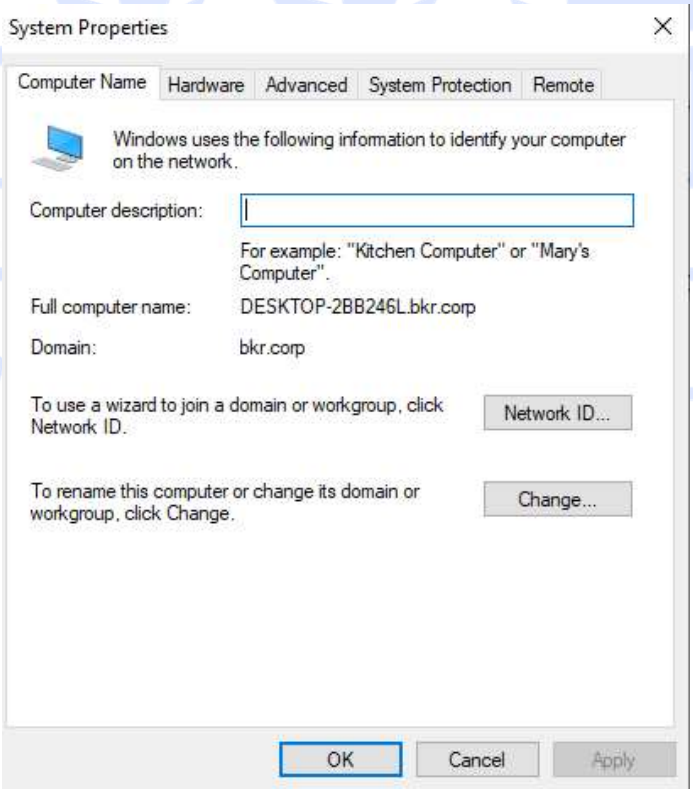
Enter the IP address of the domain controller in the "Preferred DNS server" field.



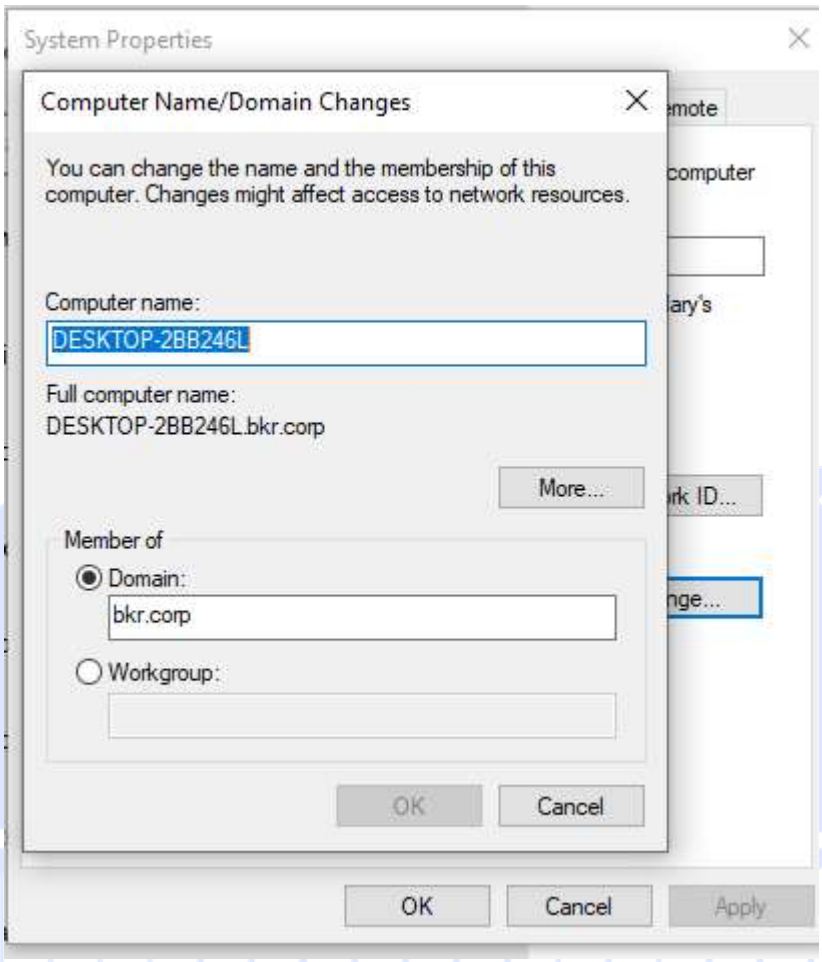
Open File Explorer on the client machine and right-click on "This PC" and select "Properties." This will take you to the System window.



In the System window, click on "Advanced system settings" on the left side.



In the System Properties window, click on the "Computer Name" tab, and then click the "Change" button.



In the Computer Name/Domain Changes window, select the "Domain" option and enter the domain name that you created in Step 1 into the "Domain" field.

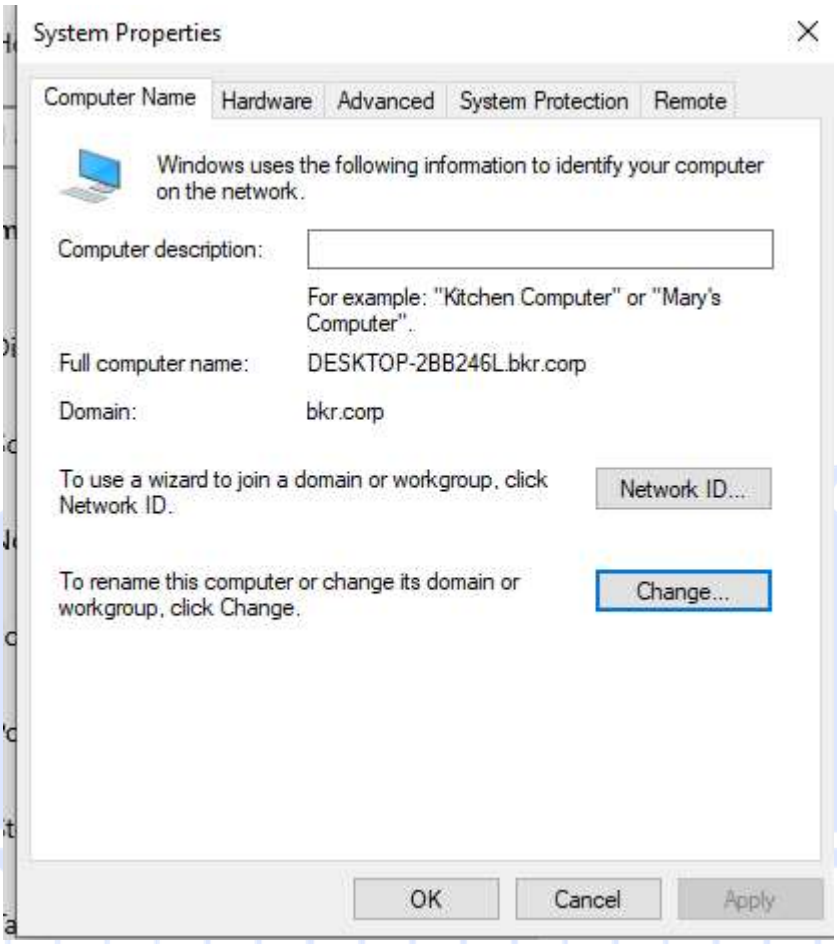
Click "OK" and then enter the credentials of a user account that has permission to join computers to the domain. This is typically an administrator account on the domain.

After entering the credentials, click "OK" again.

You will receive a message indicating that you have successfully joined the domain. Click "OK" to close the message.

You will then be prompted to restart the computer. Click "OK" to restart the computer and complete the process.

After the computer restarts, log in using the domain credentials of a user account that has access to the domain resources.



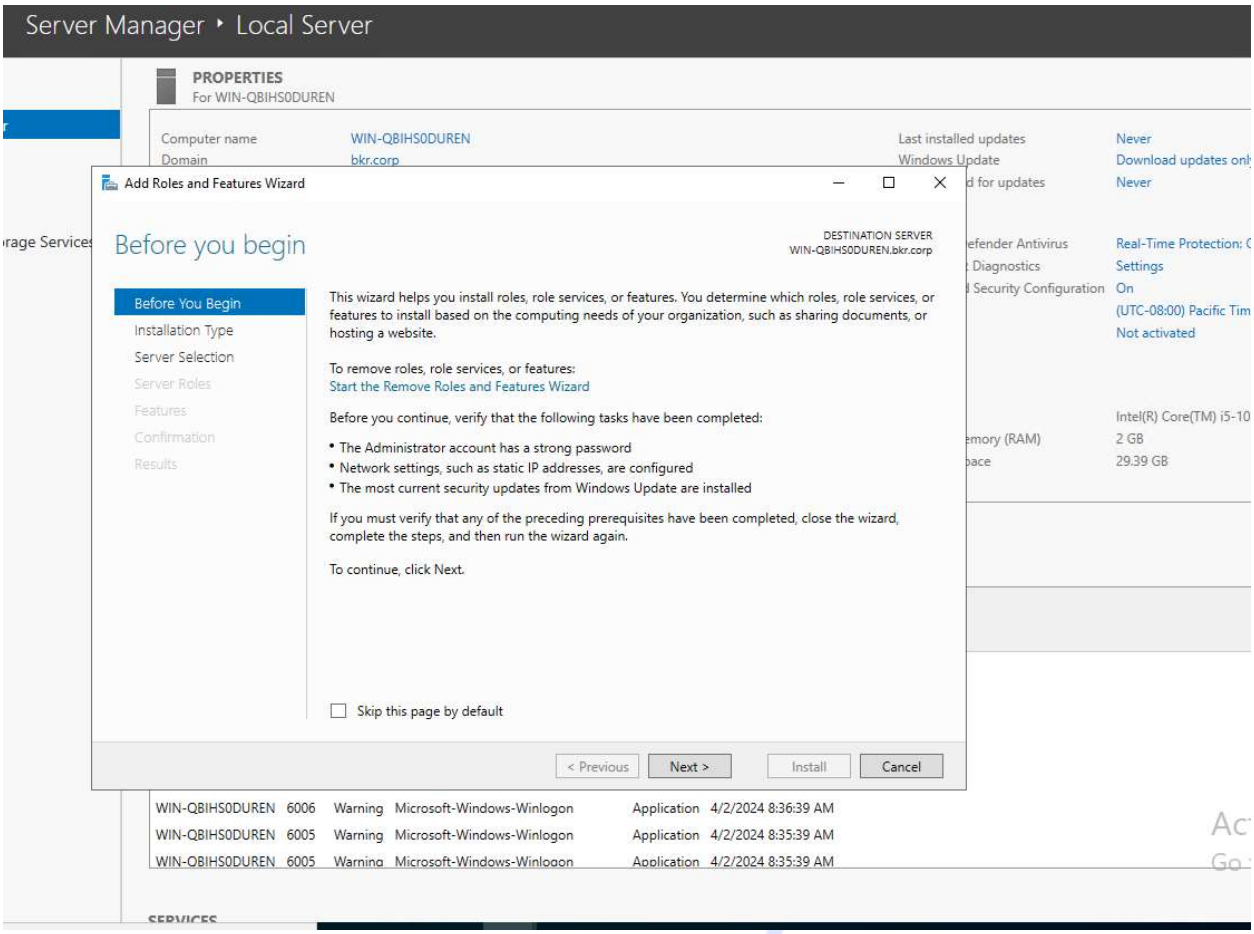
Once logged in, you can verify that the client machine has successfully joined the domain by checking the domain name in the System Properties or by attempting to access domain resources.

- **Step 3: Installing the Web Server (IIS):**

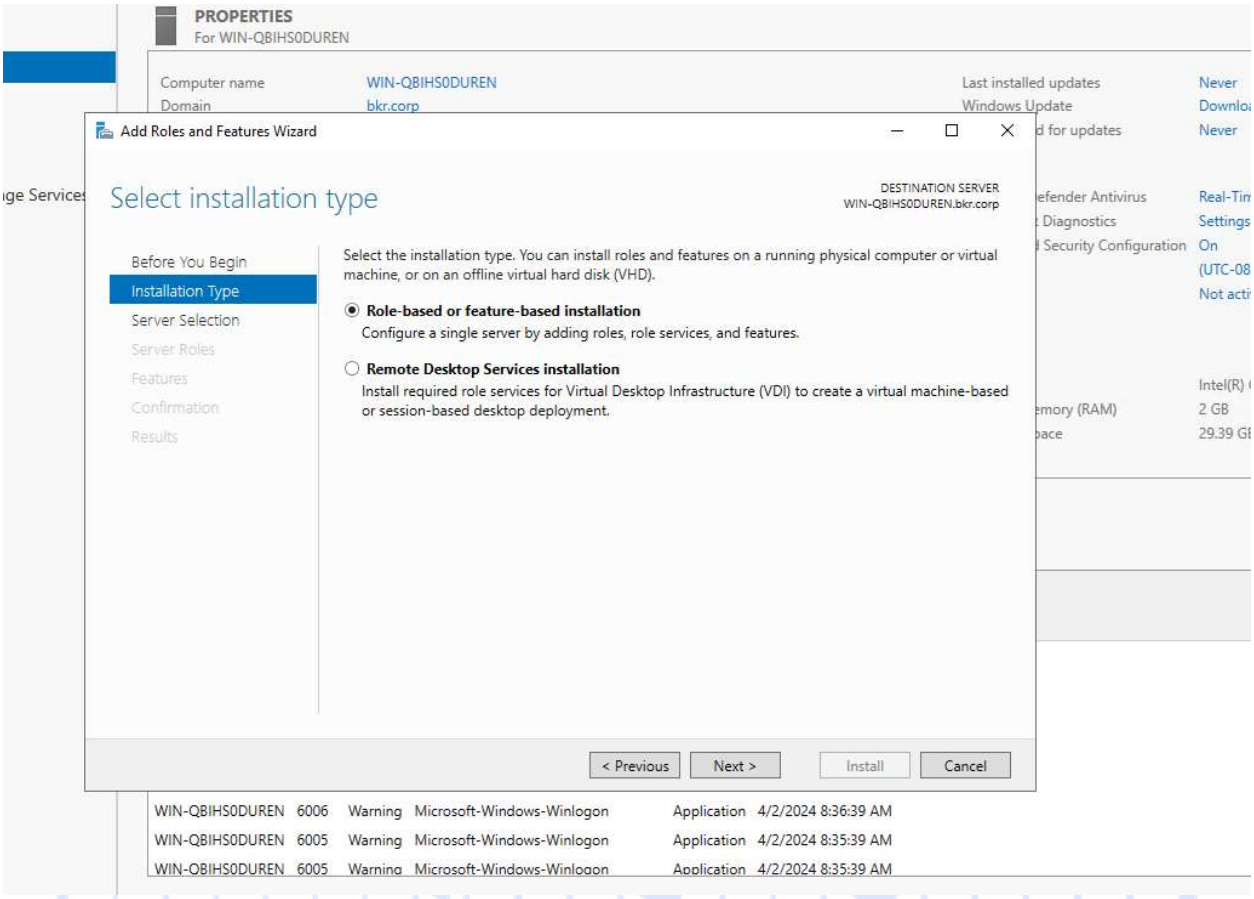
We will install the web server (IIS) on the client machine. By default, this will use the HTTP protocol, which is not secure. We will secure this later.

To install IIS on the client machine, follow these steps:

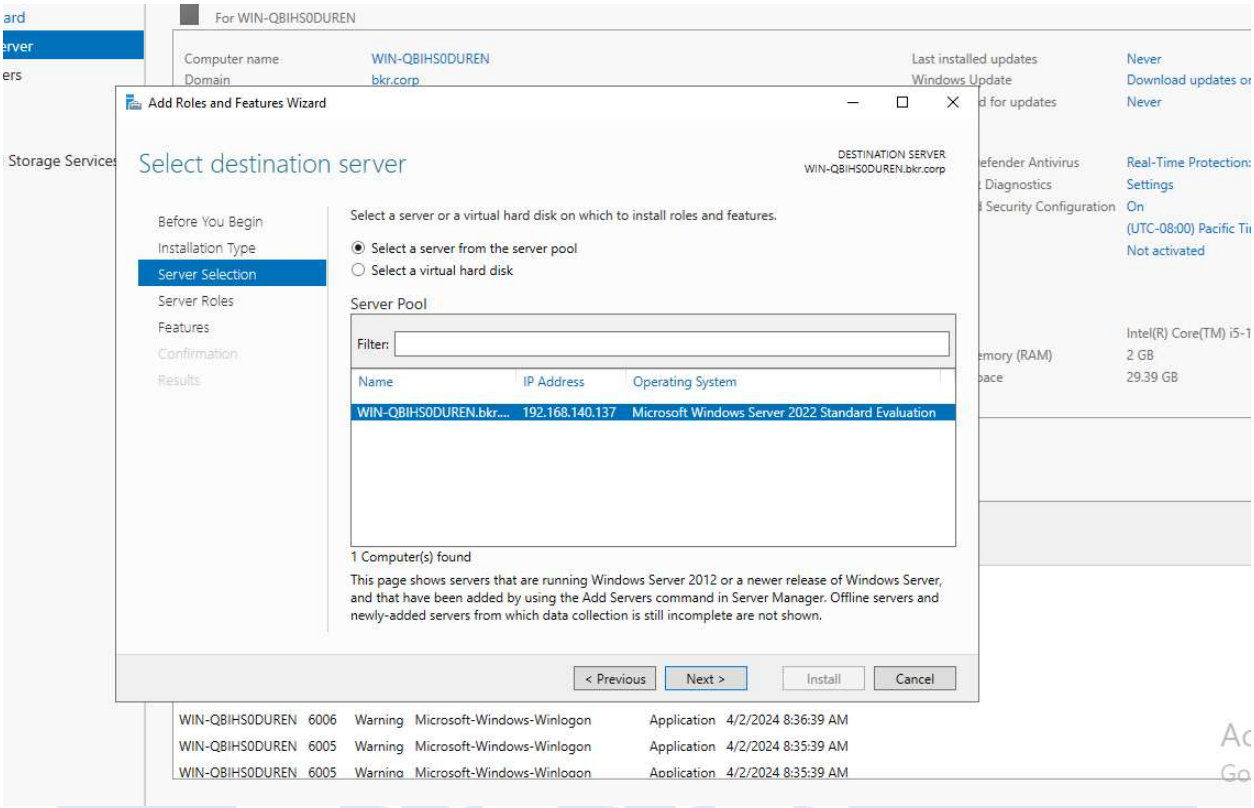
open the Server Manager then click on "Manage" at the top-right corner and select "Add Roles and Features".



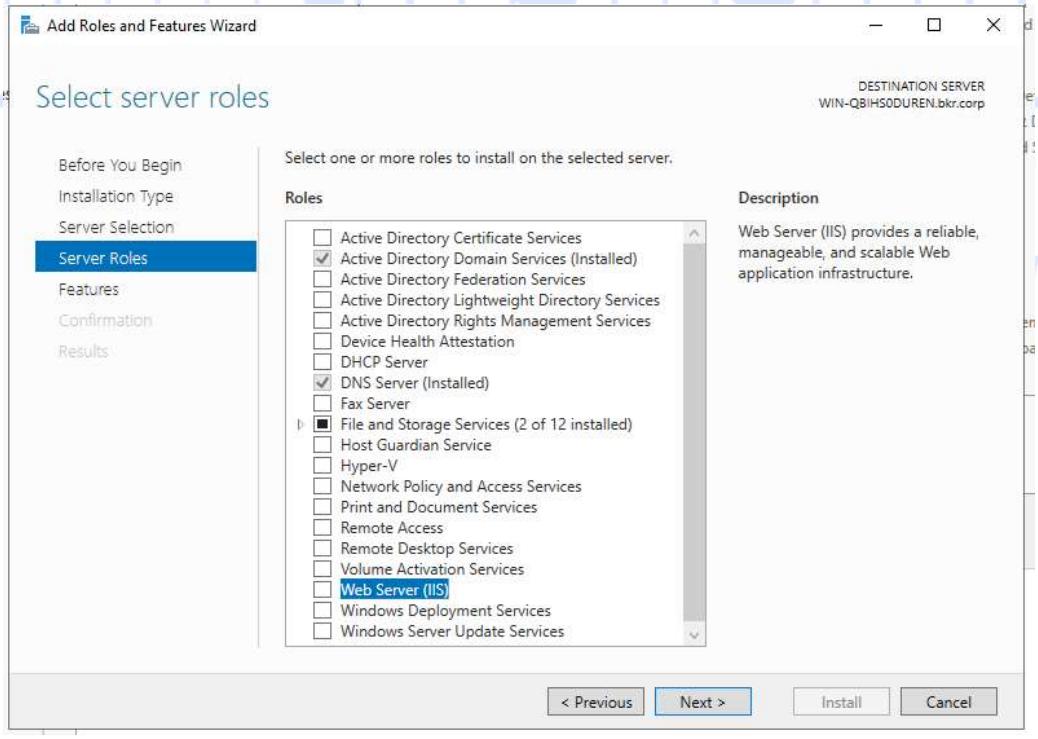
The Add Roles and Features Wizard will open. Click "Next" on the Before you begin page.



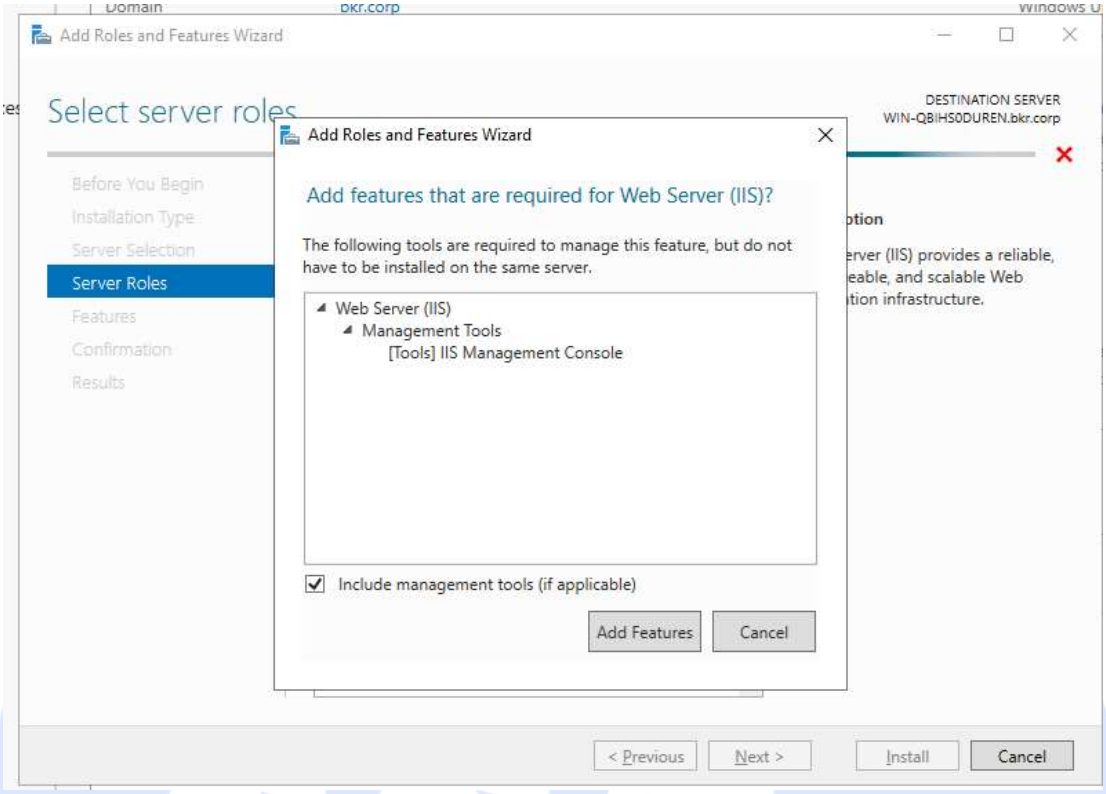
Select "Role-based or feature-based installation" and click "Next".



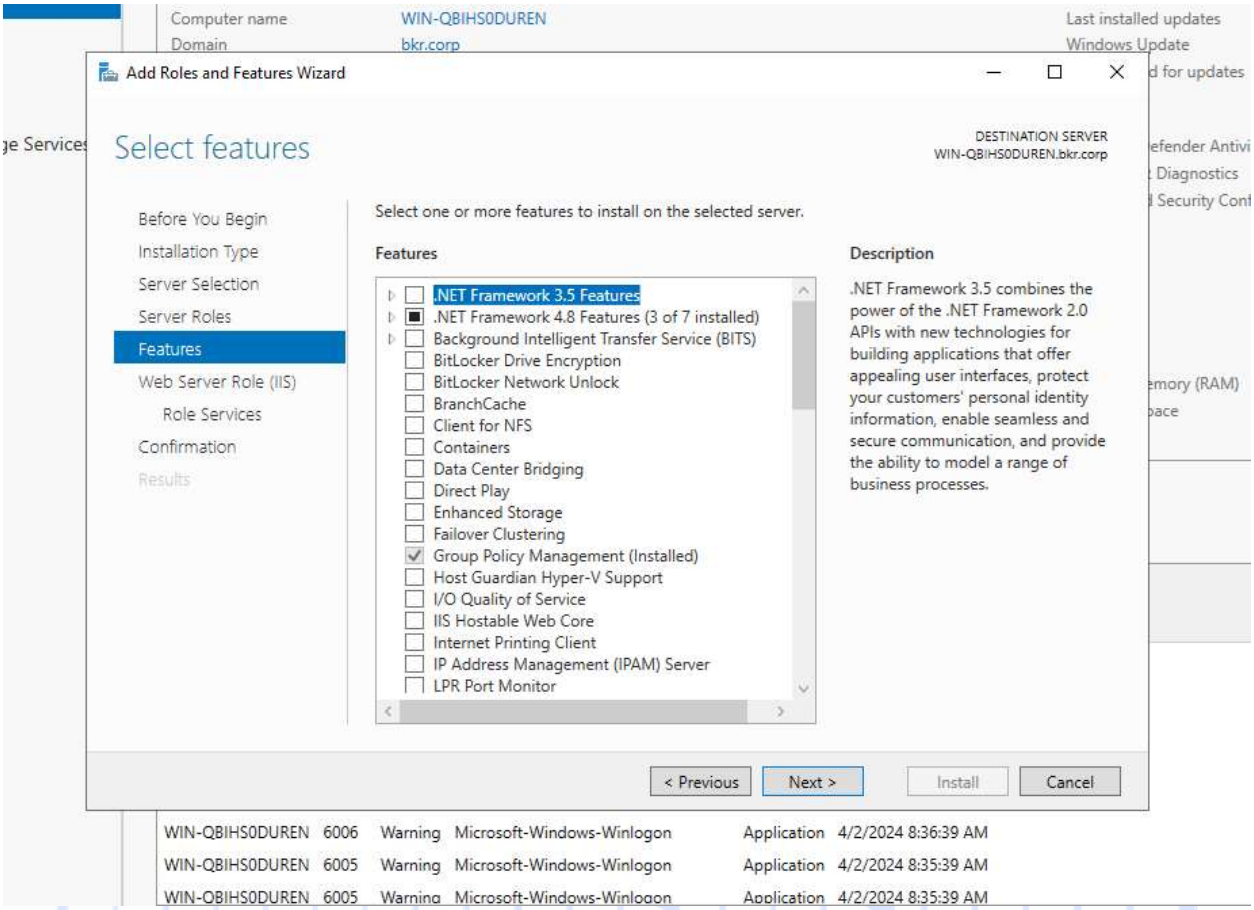
Choose the server you want to install IIS on and click "Next".



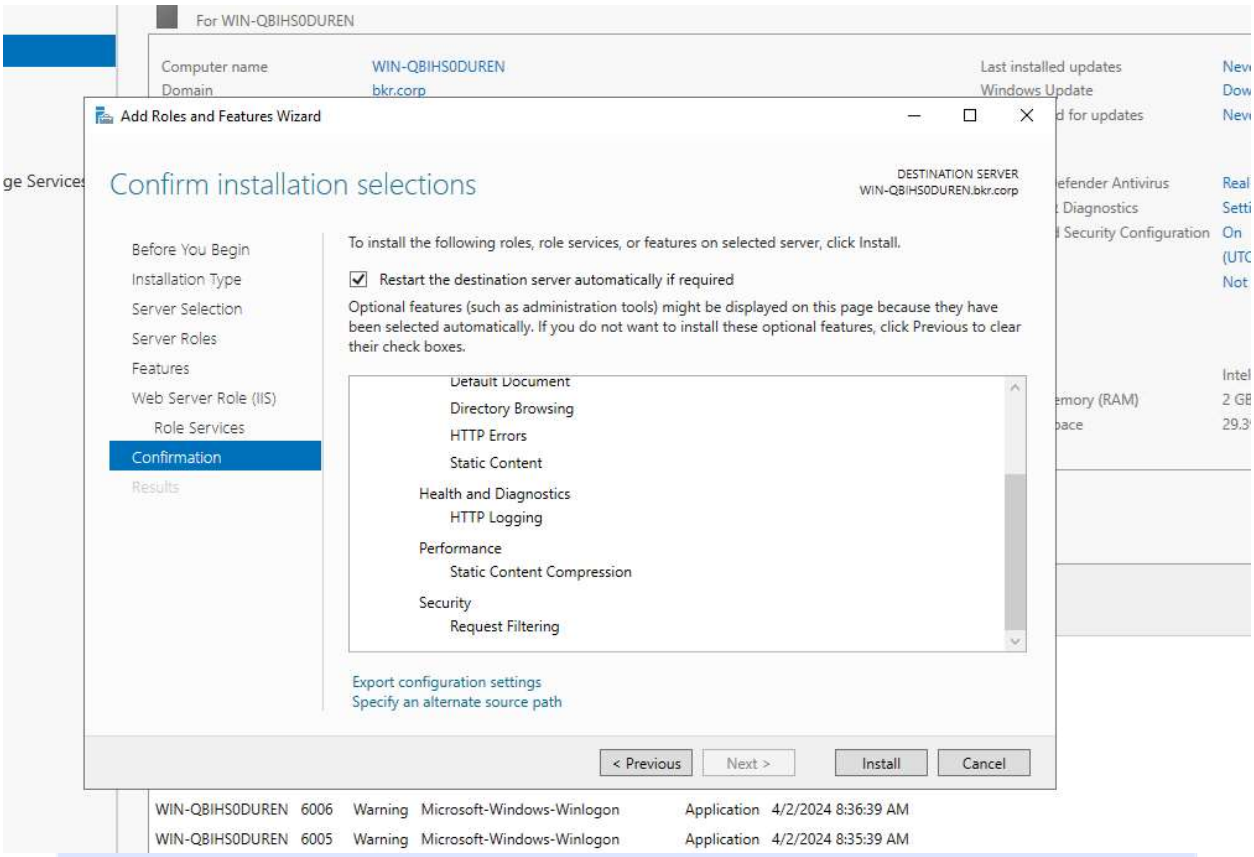
In the Roles list, select "Web Server (IIS)".



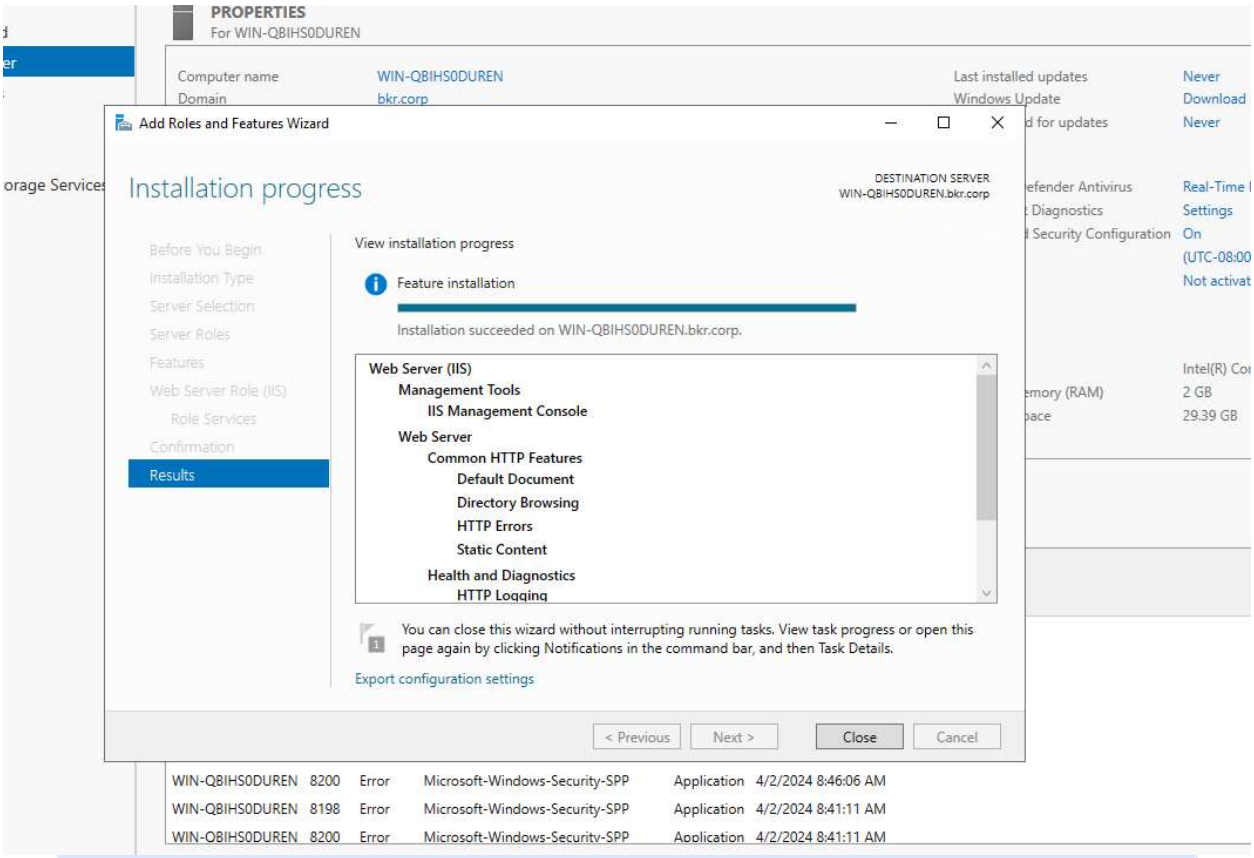
A dialog box will appear, prompting you to add features that are required for Web Server (IIS) to function properly. Click "Add Features".



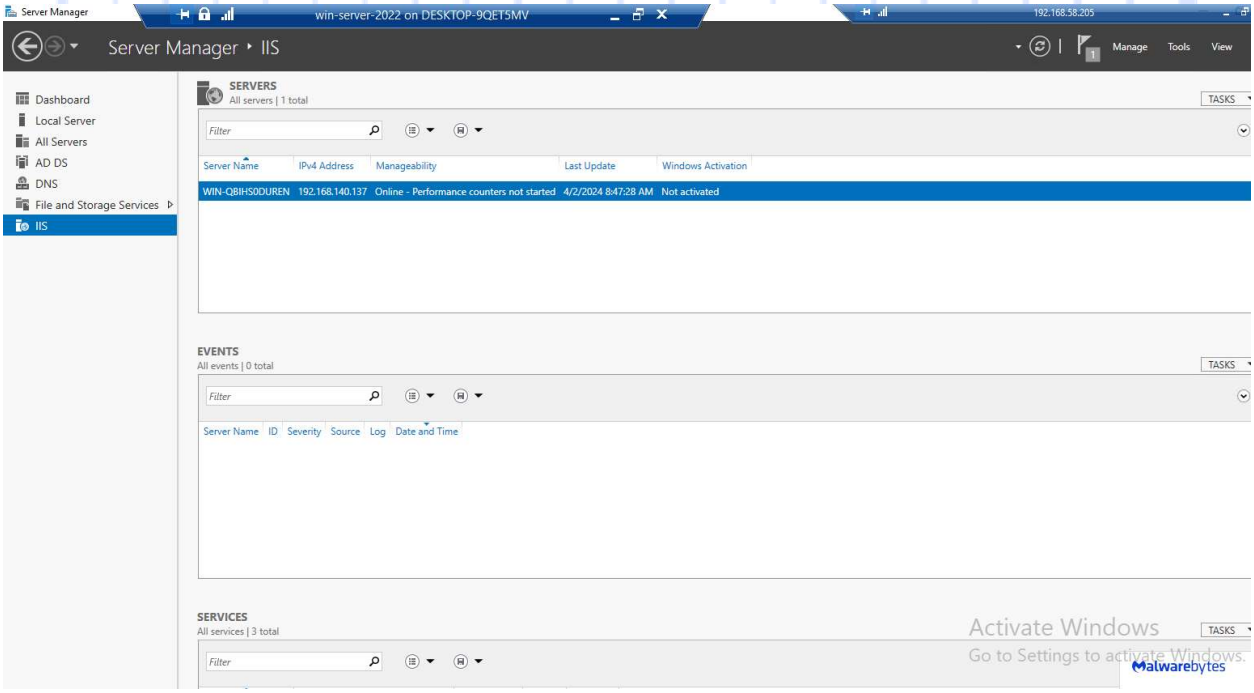
Click "Next" through the Features, Web Server Role (IIS), and Role Services pages without making any changes.



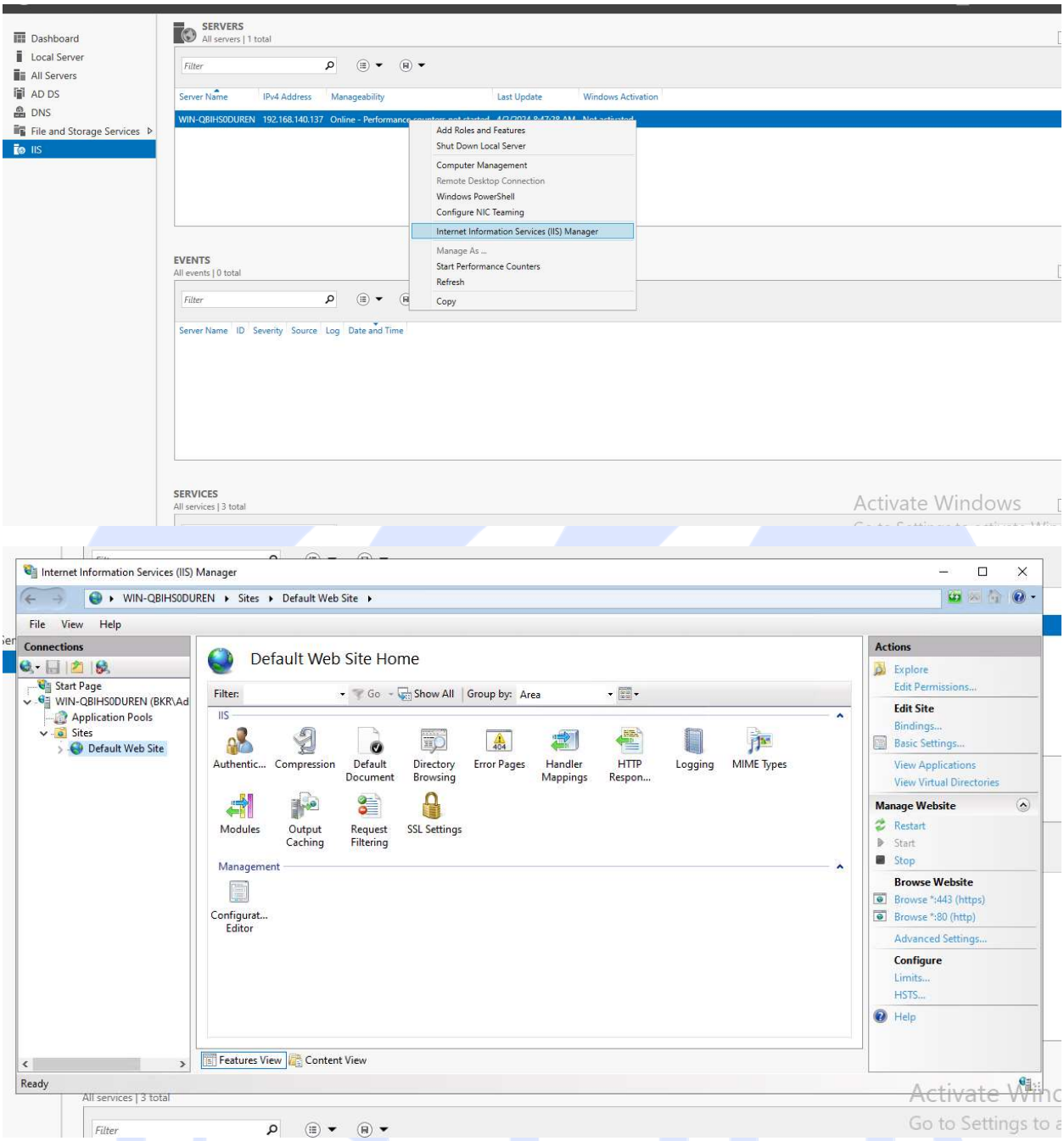
On the Confirmation page, review your selections and click "Install" to begin the installation process.



Once the installation is complete, click "Close" to exit the wizard.



Now, IIS is installed on your Windows Server. You can verify the installation by opening the Internet Information Services (IIS) Manager from the Tools menu in Server Manager.



To verify that the web server is functioning as expected, you can follow these steps:

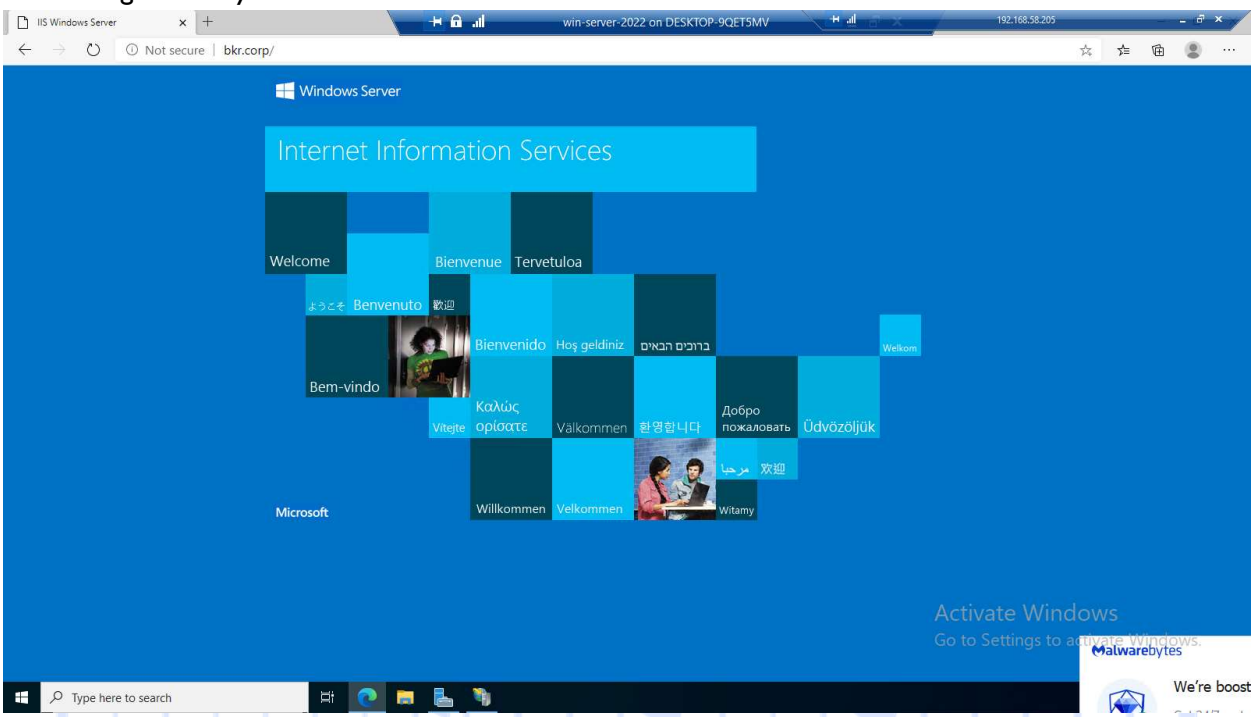
Open a web browser on the client or on another machine connected to the same network as the web server.

In the browser's address bar, enter the IP address or domain name of the web server. For example, if the web server's IP address is 192.168.1.100, enter **"http://192.168.1.100"** or **"http://domain-name"**.

Press Enter to access the website hosted on the IIS server.

You should see the default homepage or any other web page you have configured on the server.

If you are able to access the website without encountering errors, it means that the web server is functioning correctly.

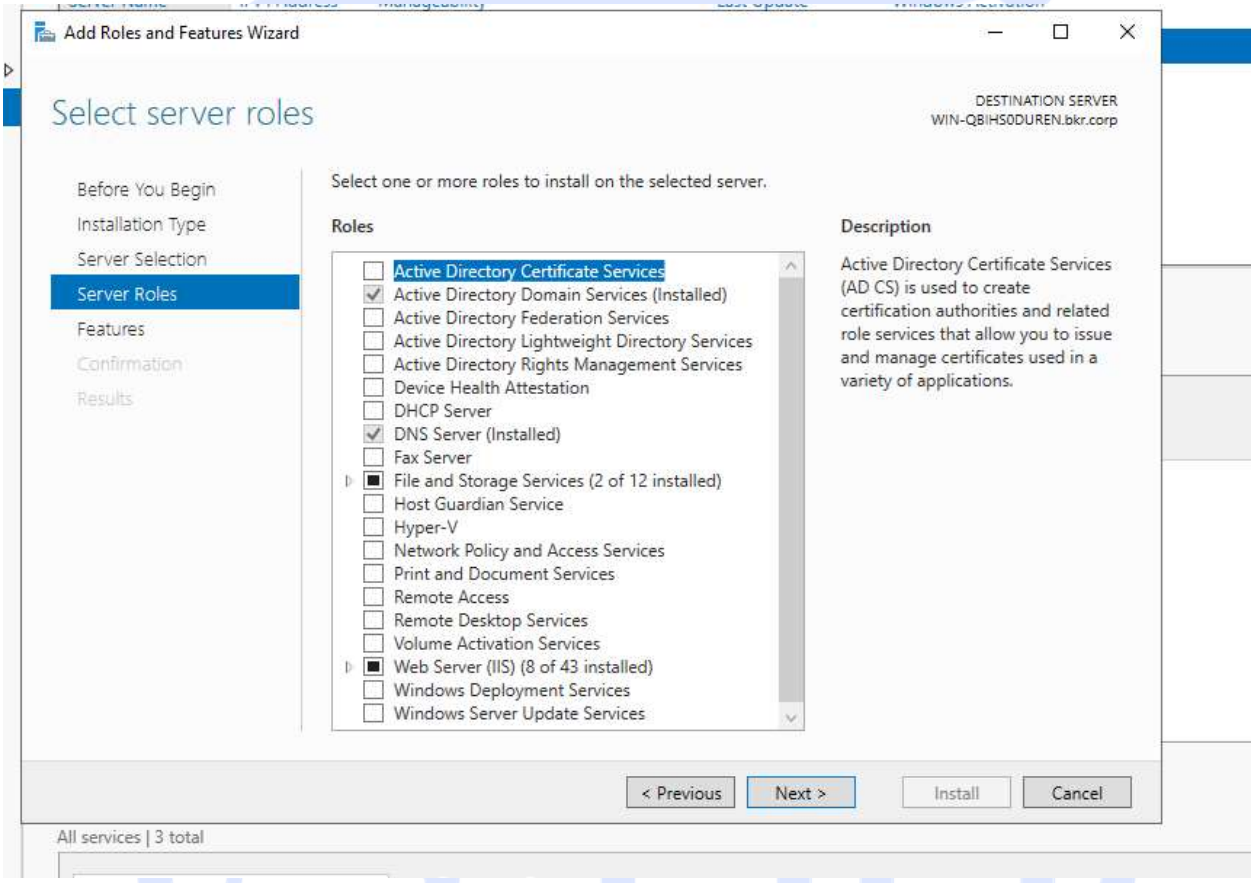


- ## Step 4: Installing and configuring Active Directory Certificate Services:

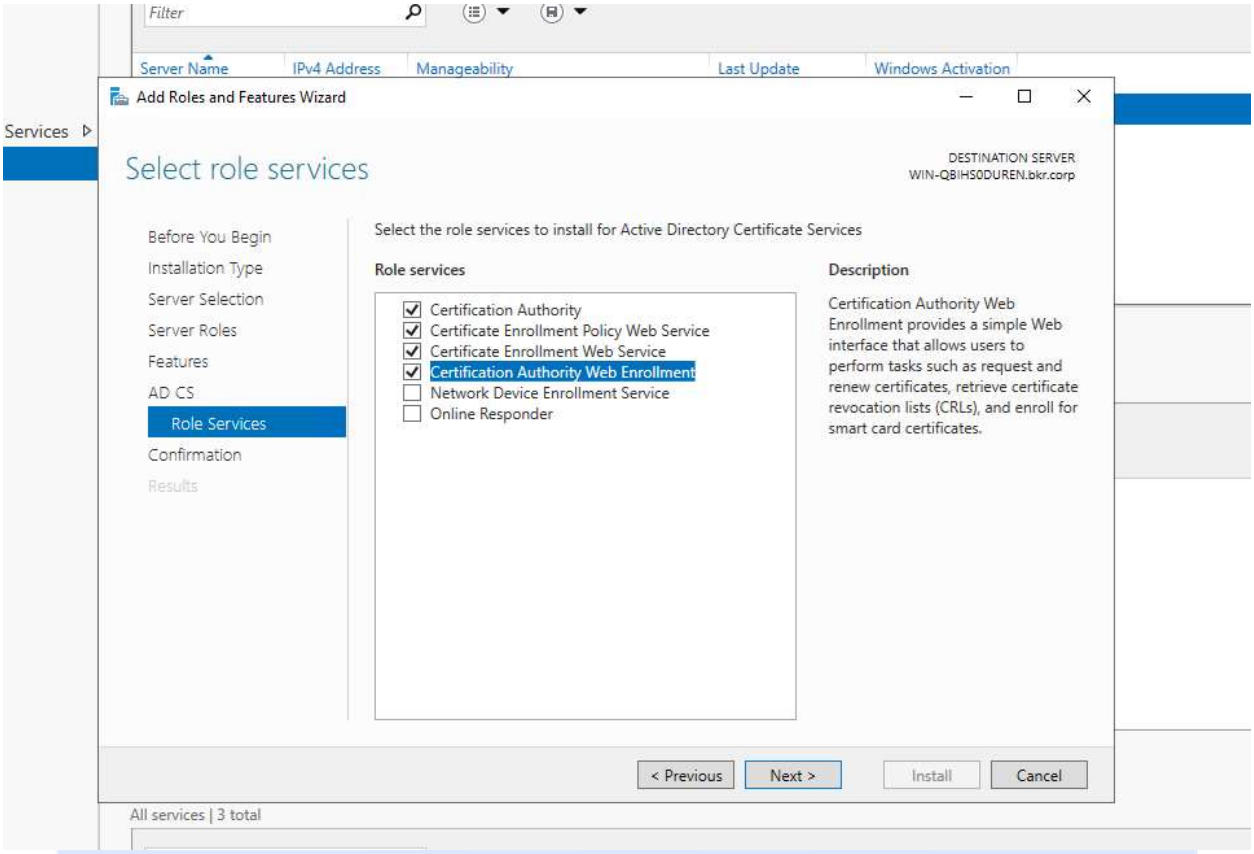
We will install Active Directory Certificate Services (AD CS) on our server to secure communications via SSL/TLS. We will select SHA512, the most secure version of the SHA hashing algorithm.

To install Active Directory Certificate Services on a Windows Server, follow these steps:

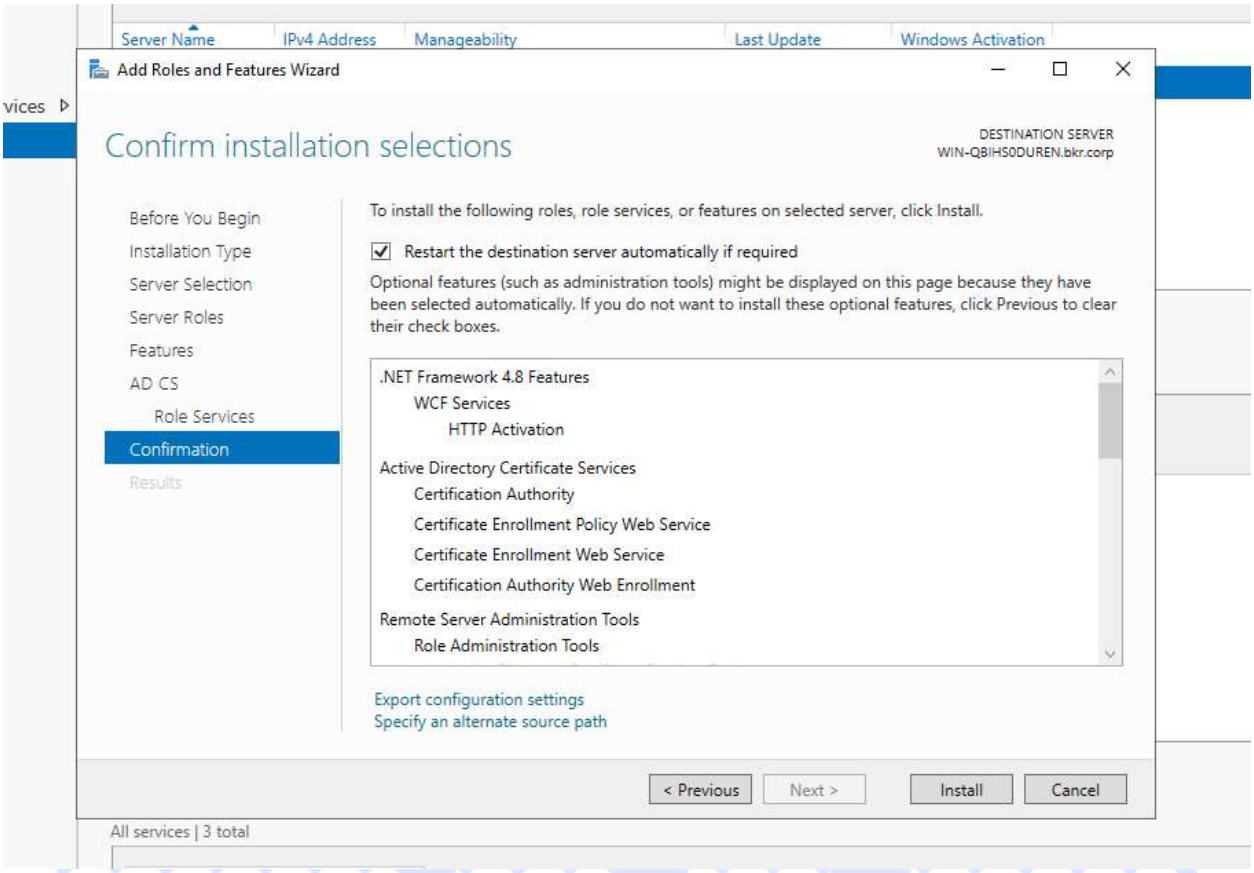
Open Server Manager then click on "Manage" at the top-right corner and select "Add Roles and Features", Click "Next" on the Before you begin page, select "Role-based or feature-based installation" and click "Next", choose the server you want to install Active Directory Certificate Services on and click "Next".



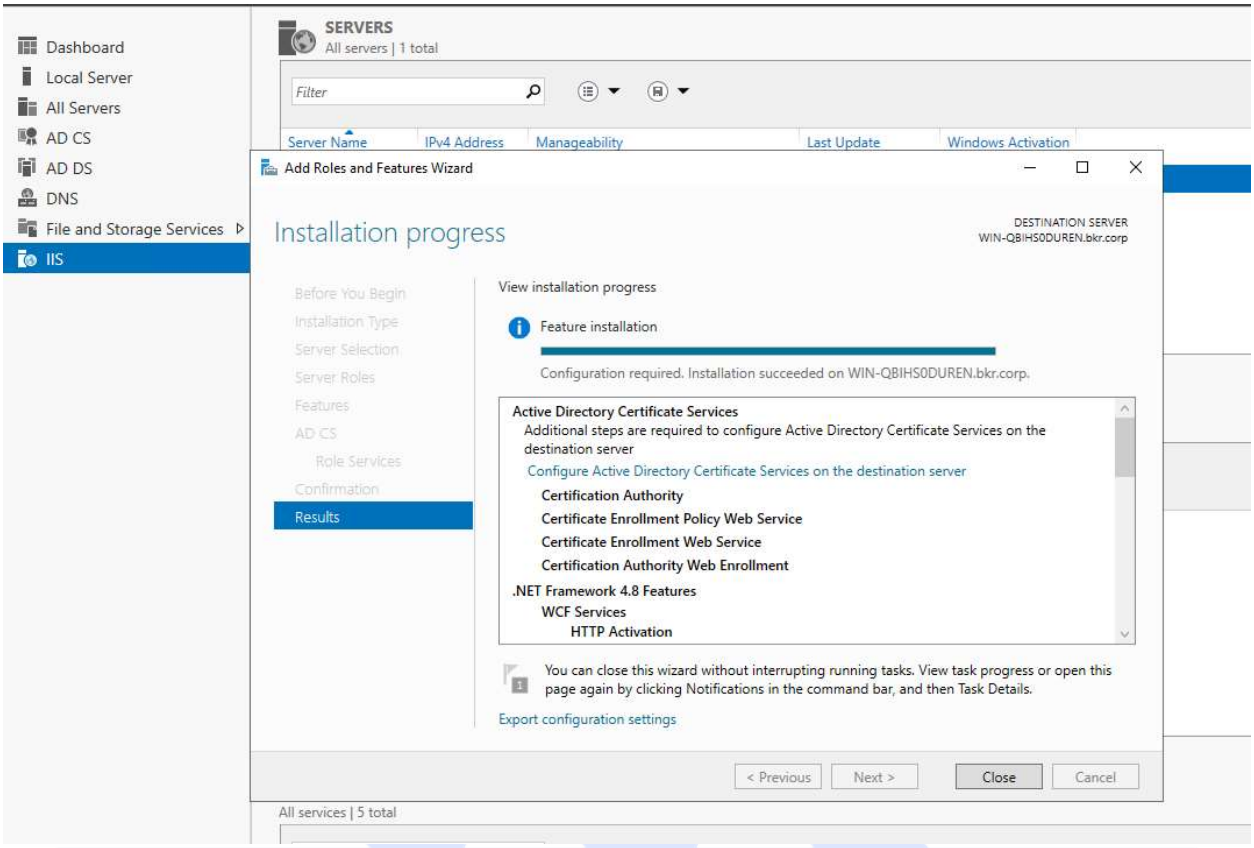
In the Roles list, select "Active Directory Certificate Services".



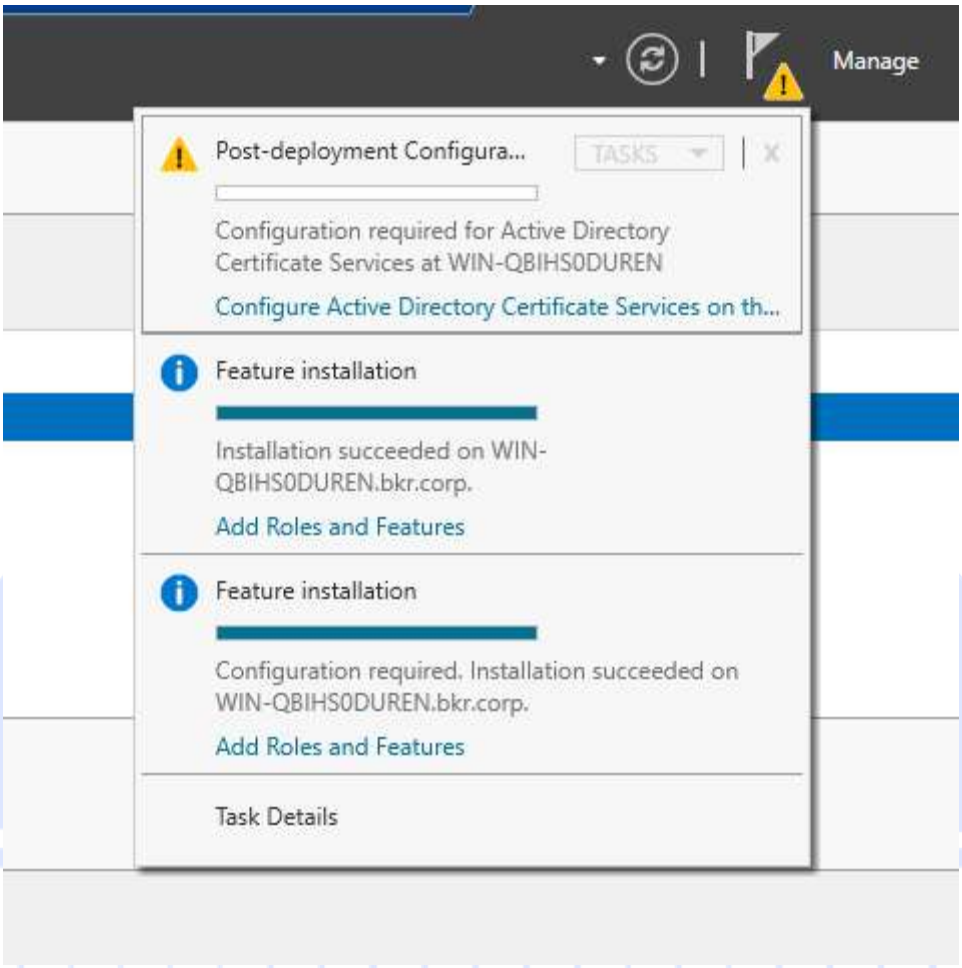
A dialog box will appear, please select the same options as shown in the screenshot above and Click "Next".



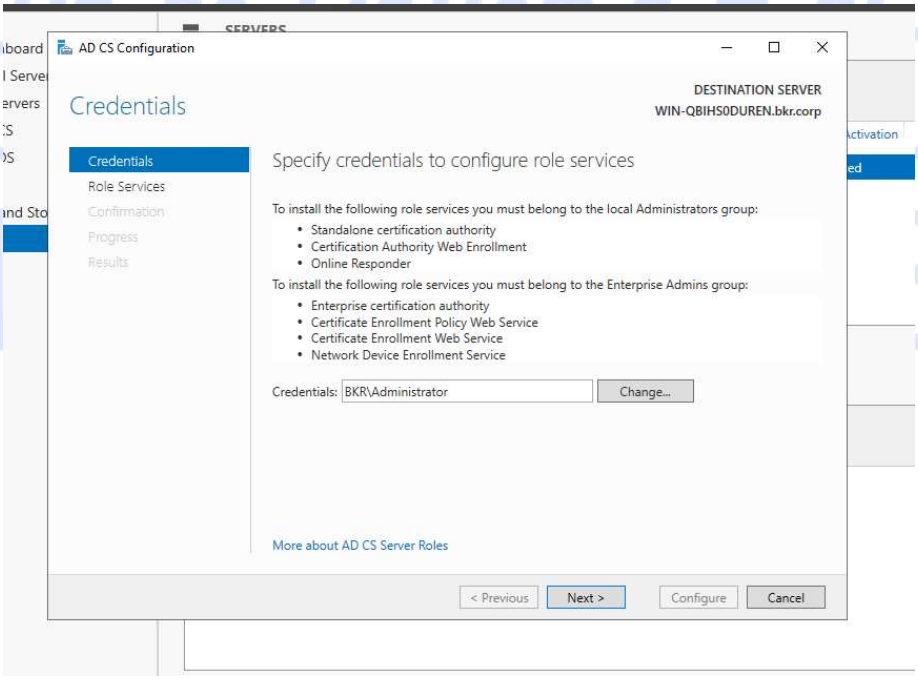
On the Confirmation page, review your selections and click "Install" to begin the installation process.



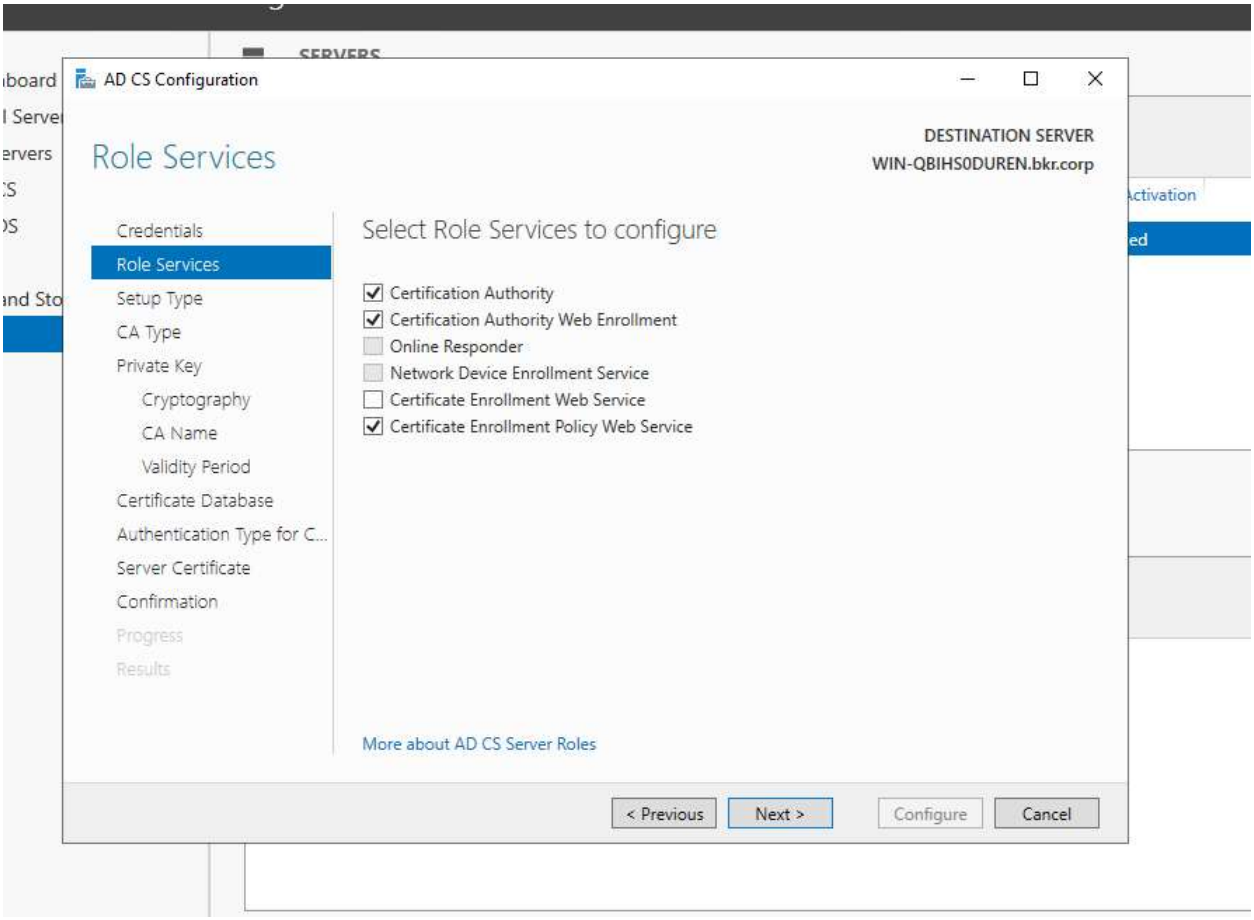
Once the installation is complete, After the installation is complete, you will receive a notification flag in Server Manager indicating that additional configuration is required for Active Directory Certificate Services.



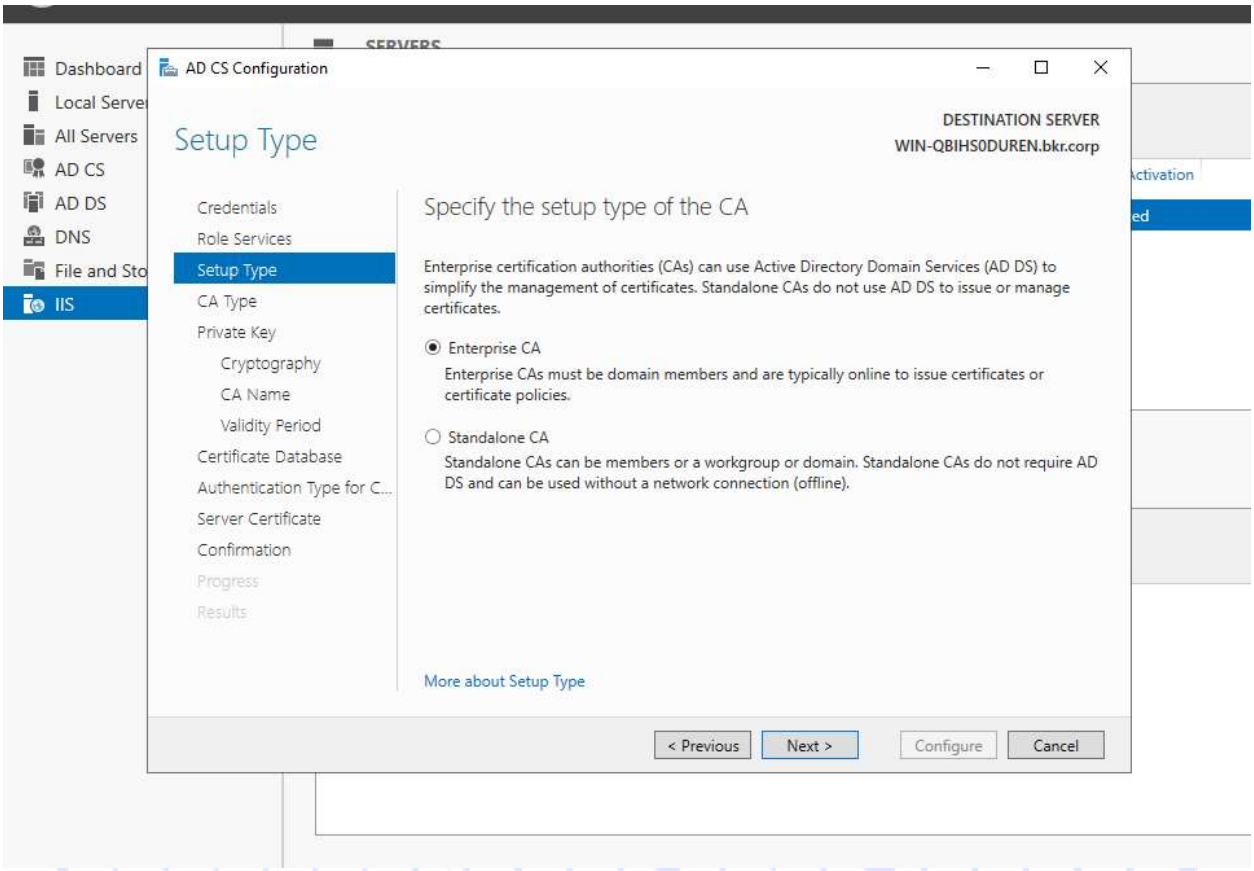
Click on the notification flag to open the Active Directory Certificate Services Configuration Wizard.



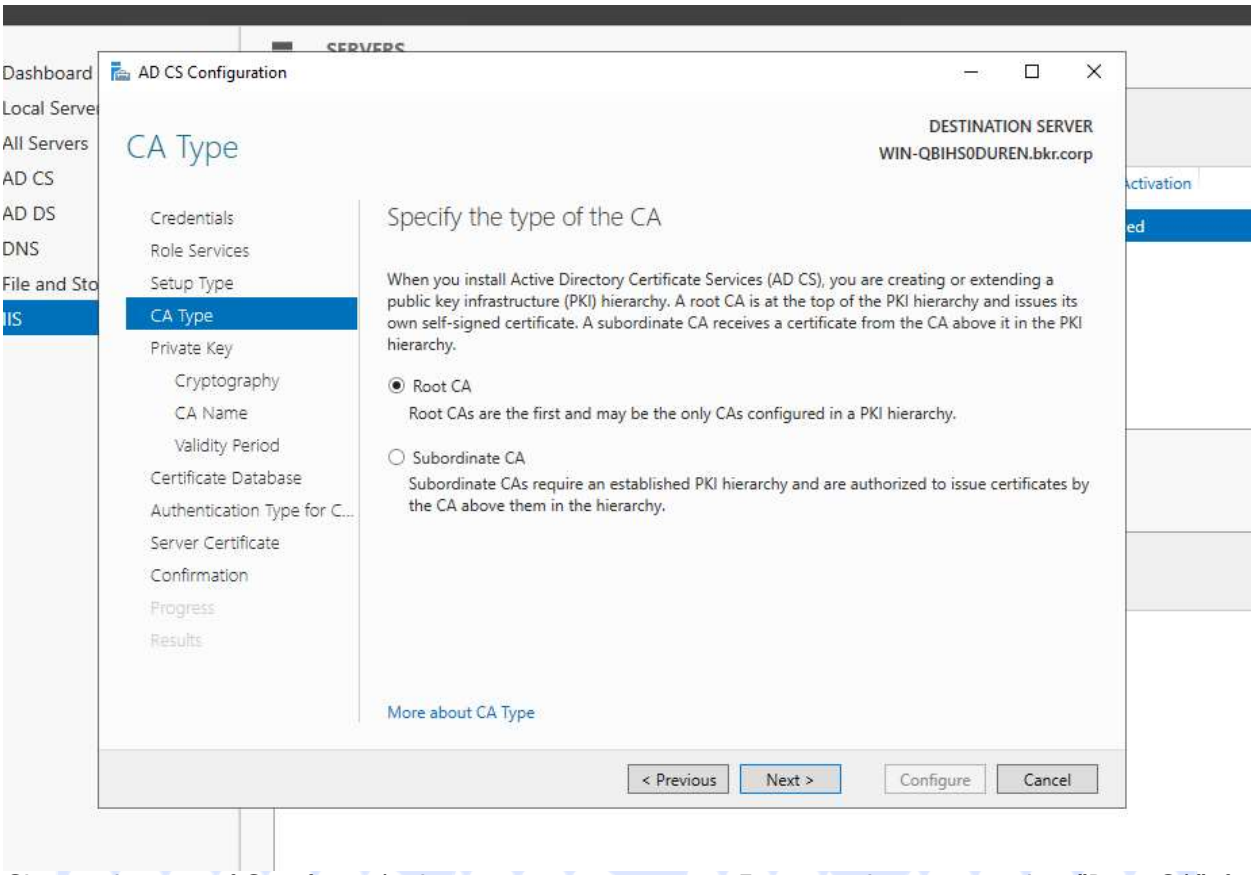
In the Configuration Wizard, you'll be prompted to specify credentials to configure role services. You can leave this at the default settings and click "Next" to proceed.



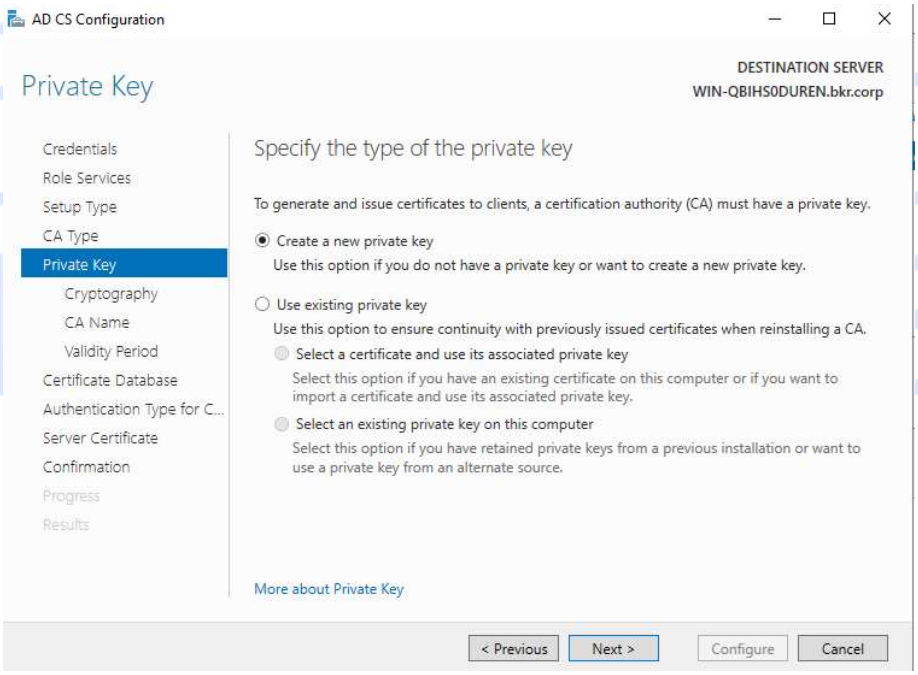
Next, you'll need to select the role services to configure. please select the same role services as shown in the screenshot above. Once selected, click "Next" to continue with the configuration process.

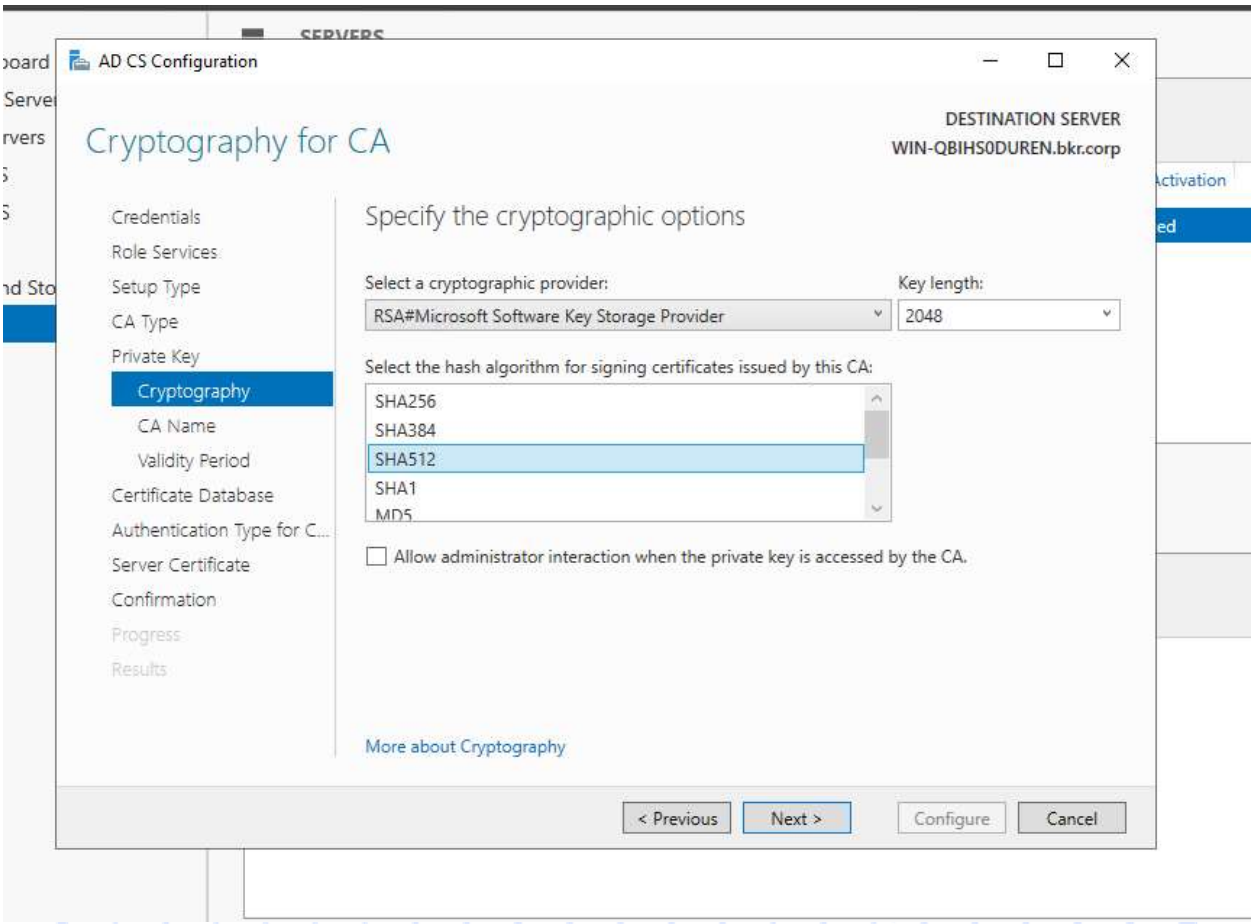


In the Configuration Wizard, select the deployment configuration for Active Directory Certificate Services. This could be "Enterprise CA" or "Standalone CA", depending on your organization's requirements. Click "Next" to proceed.

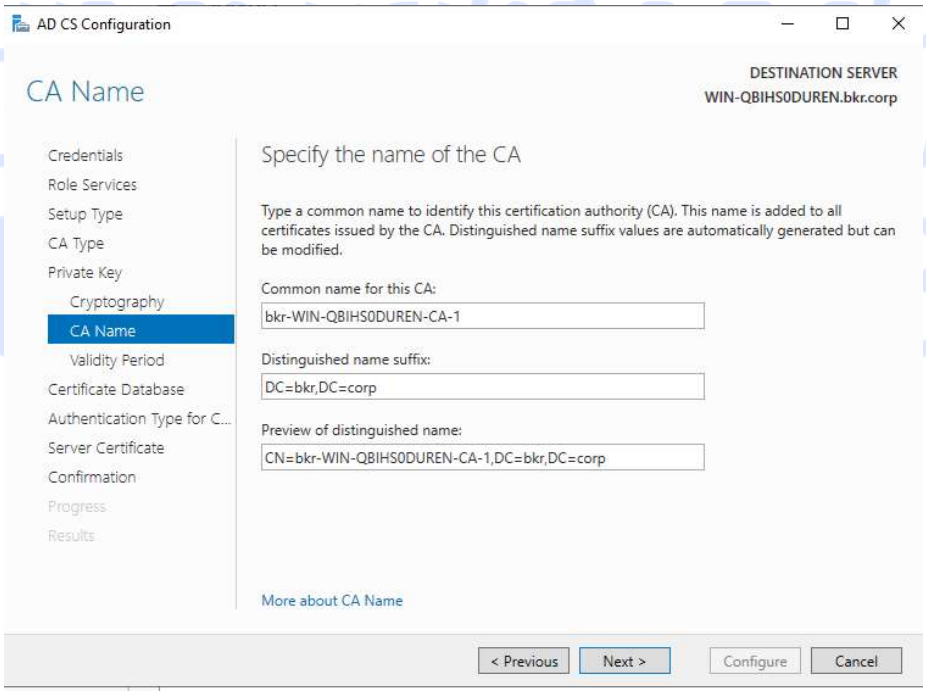


Choose the type of Certificate Authority you want to set up. For example, you can select "Root CA" if this is the first CA in your organization's hierarchy. Click "Next".

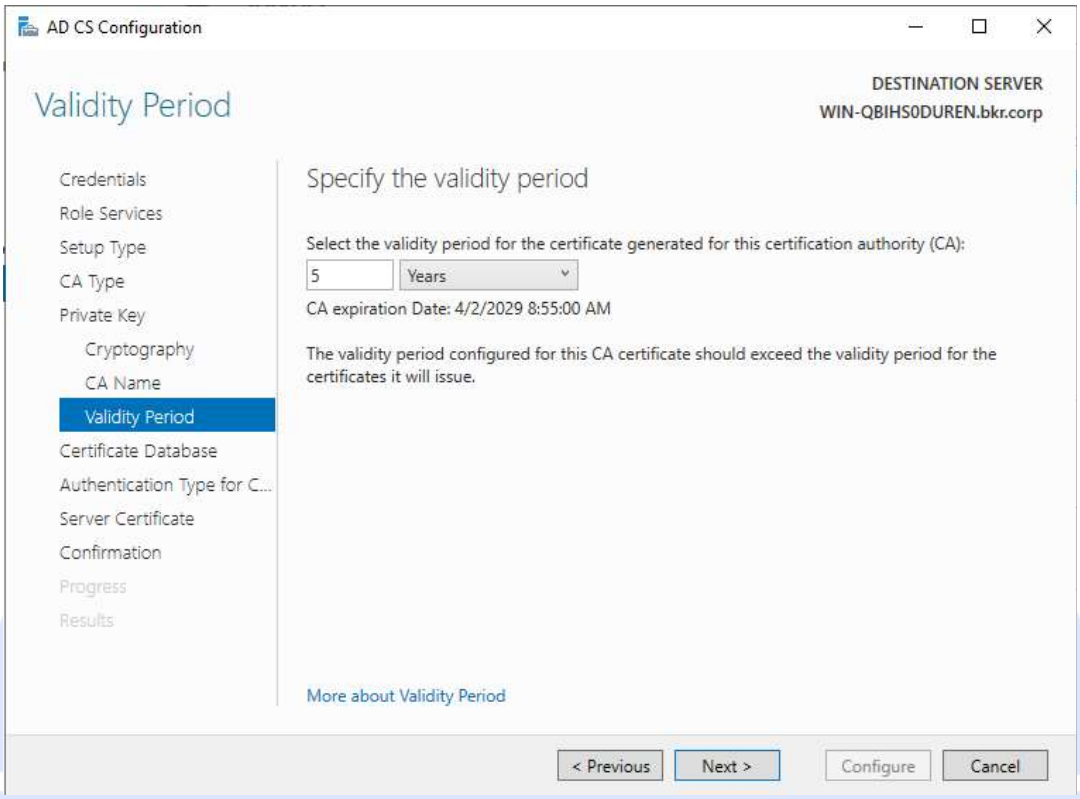


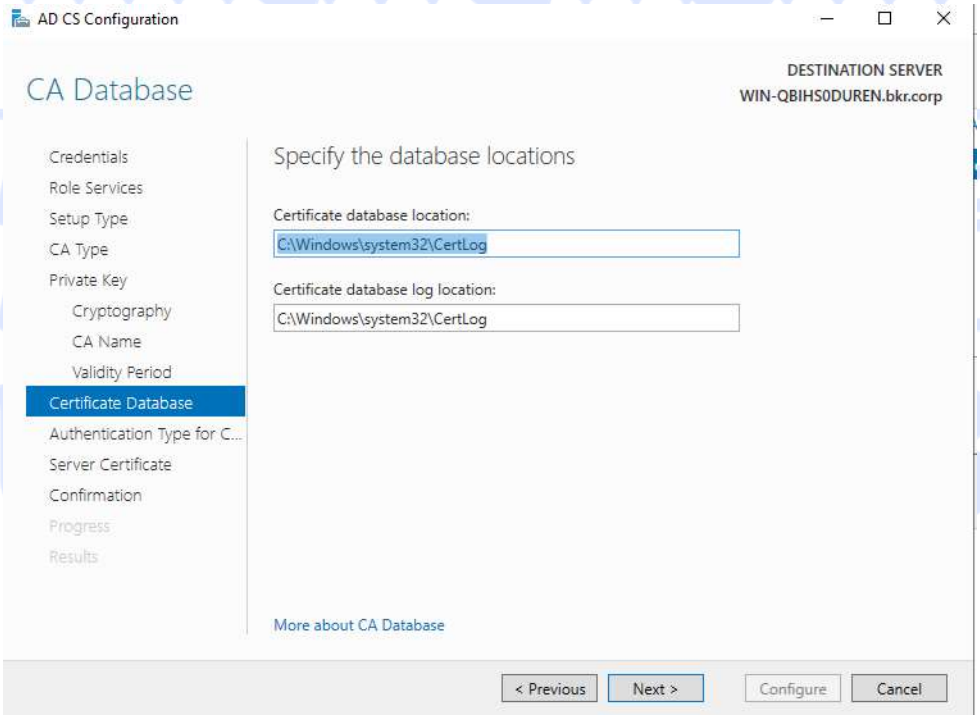


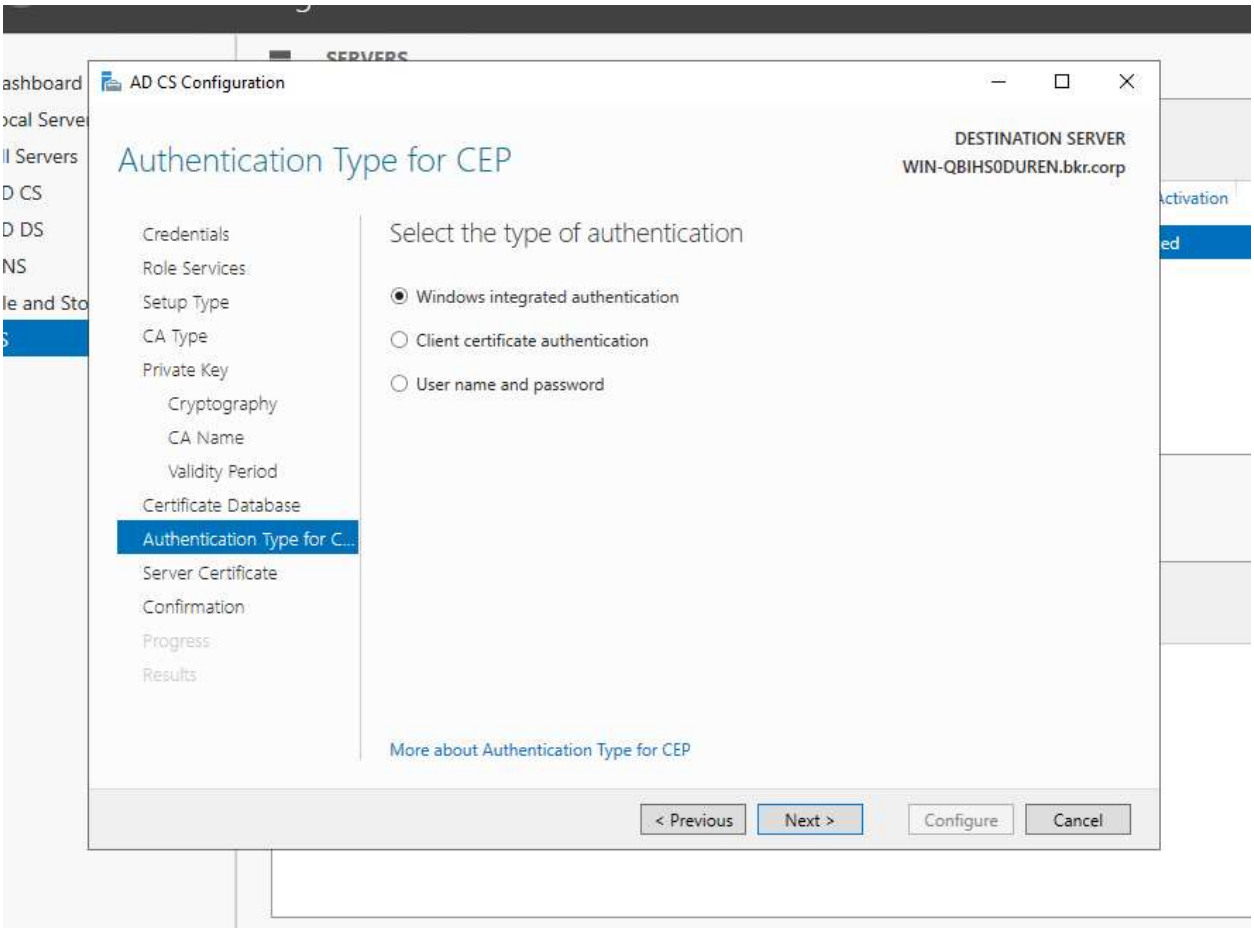
Select the cryptographic options for the CA. You can choose SHA512 as the hash algorithm for enhanced security. Click "Next".

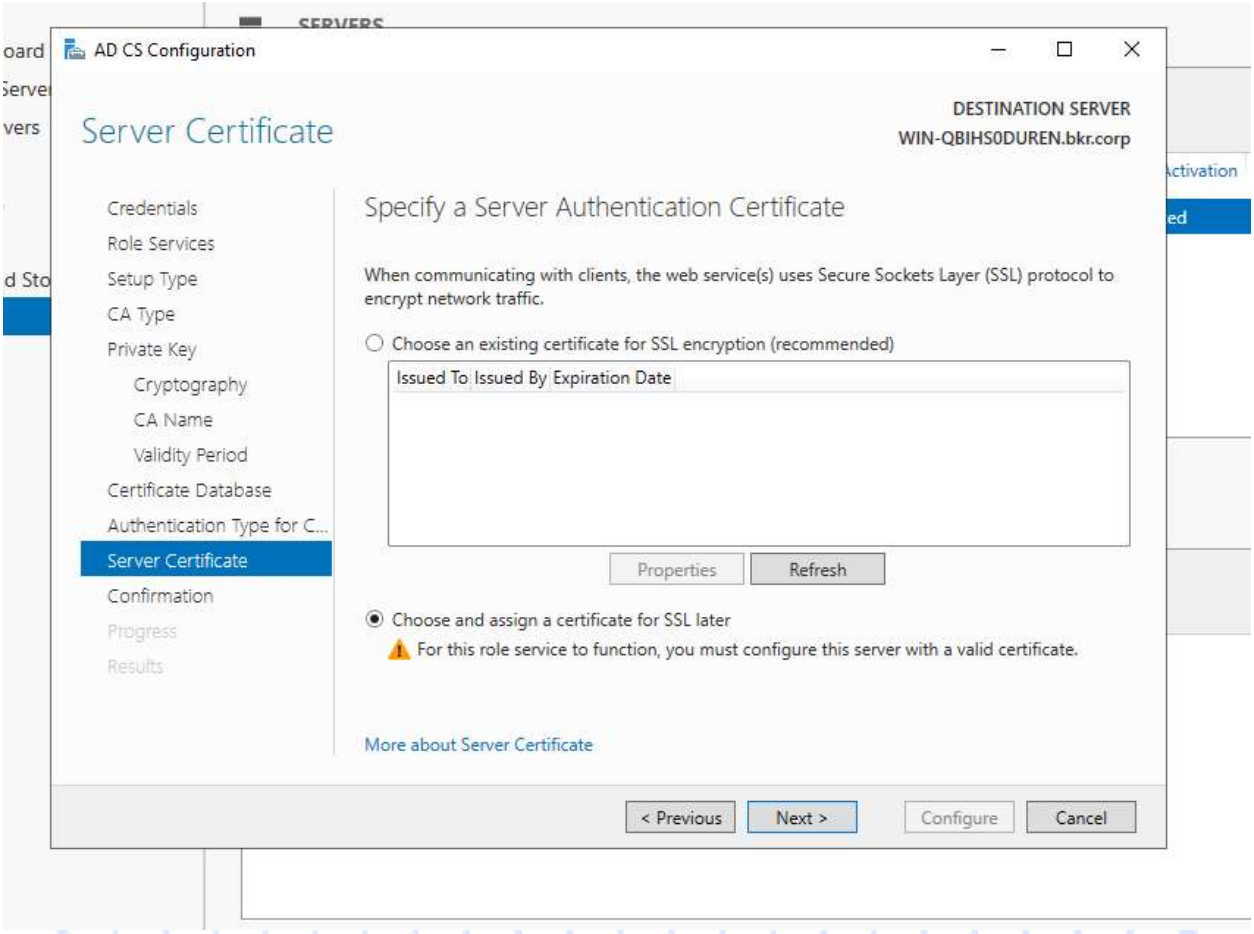


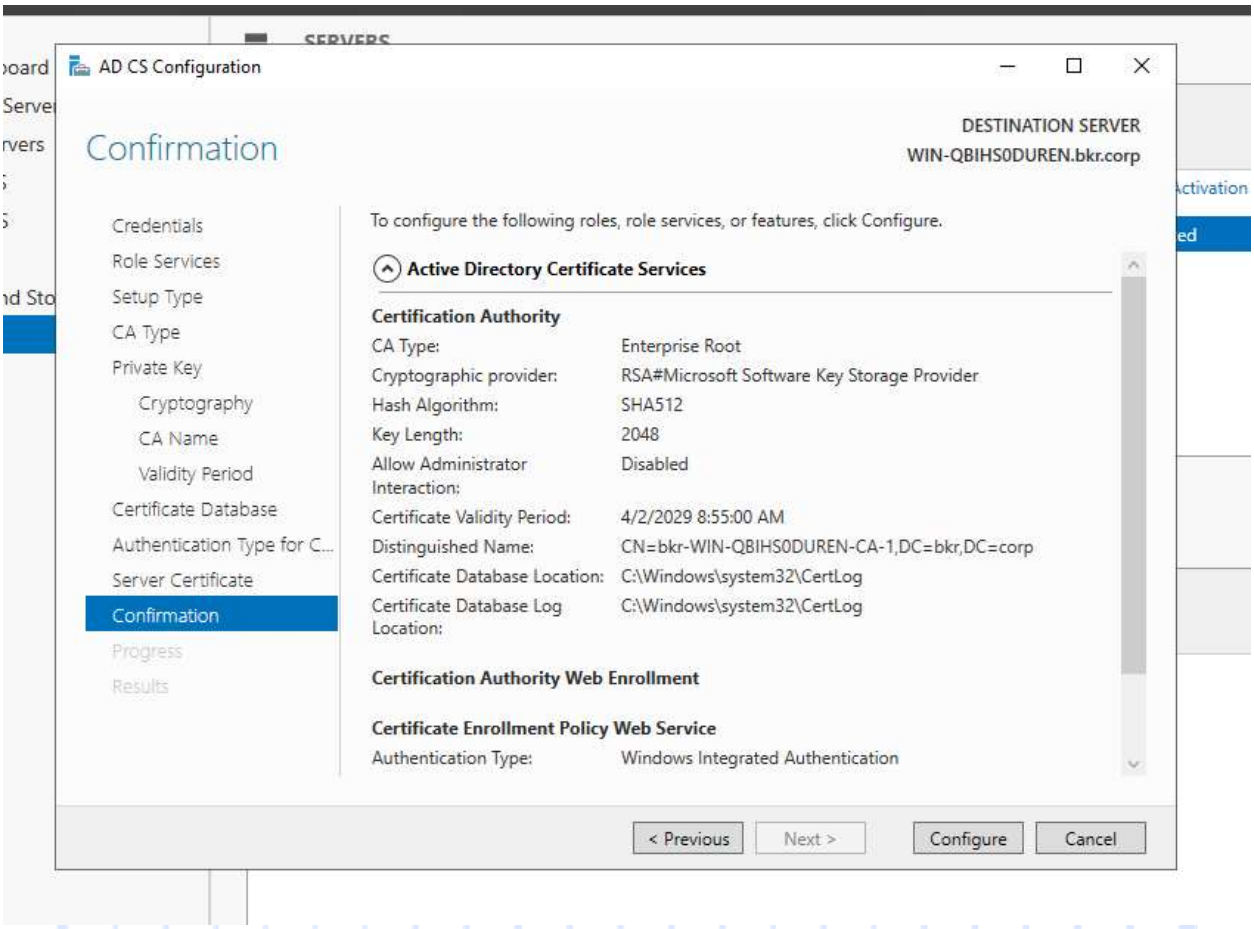
From here, you simply need to replicate the screenshots, as it's pretty straightforward.

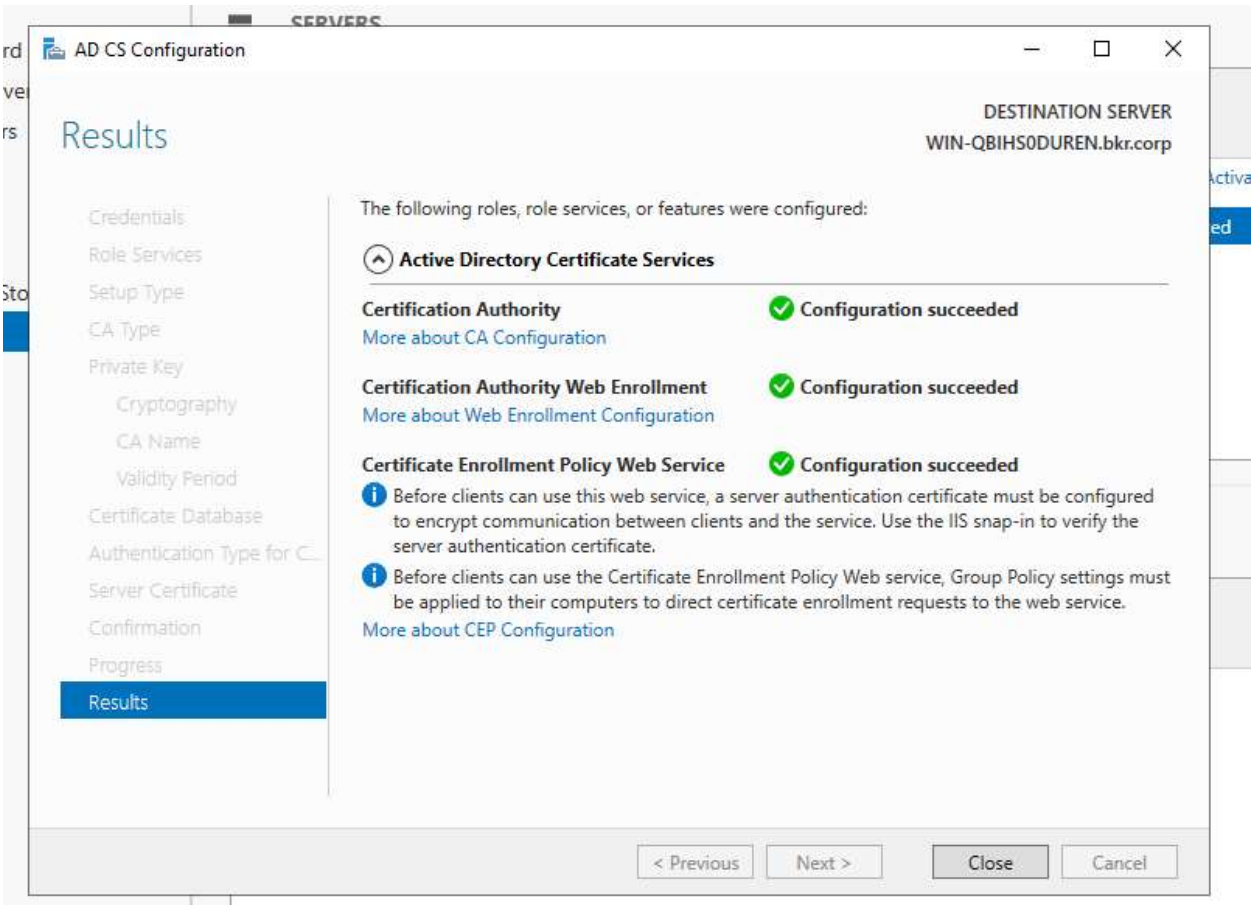


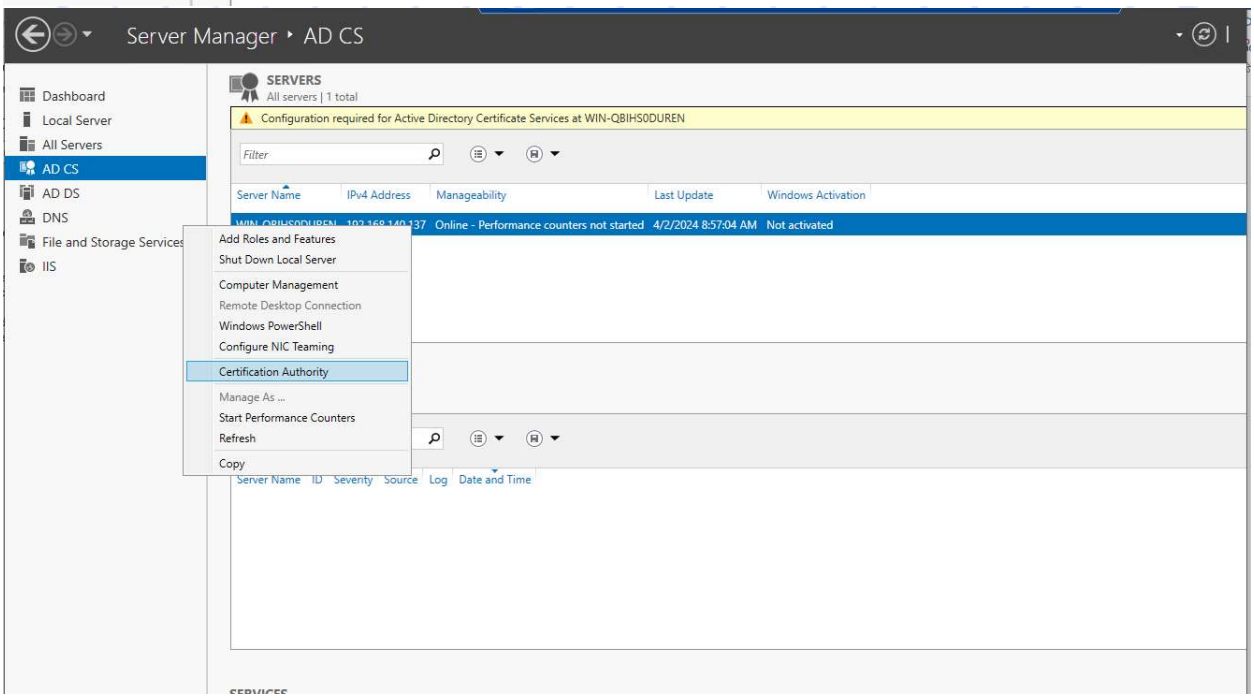


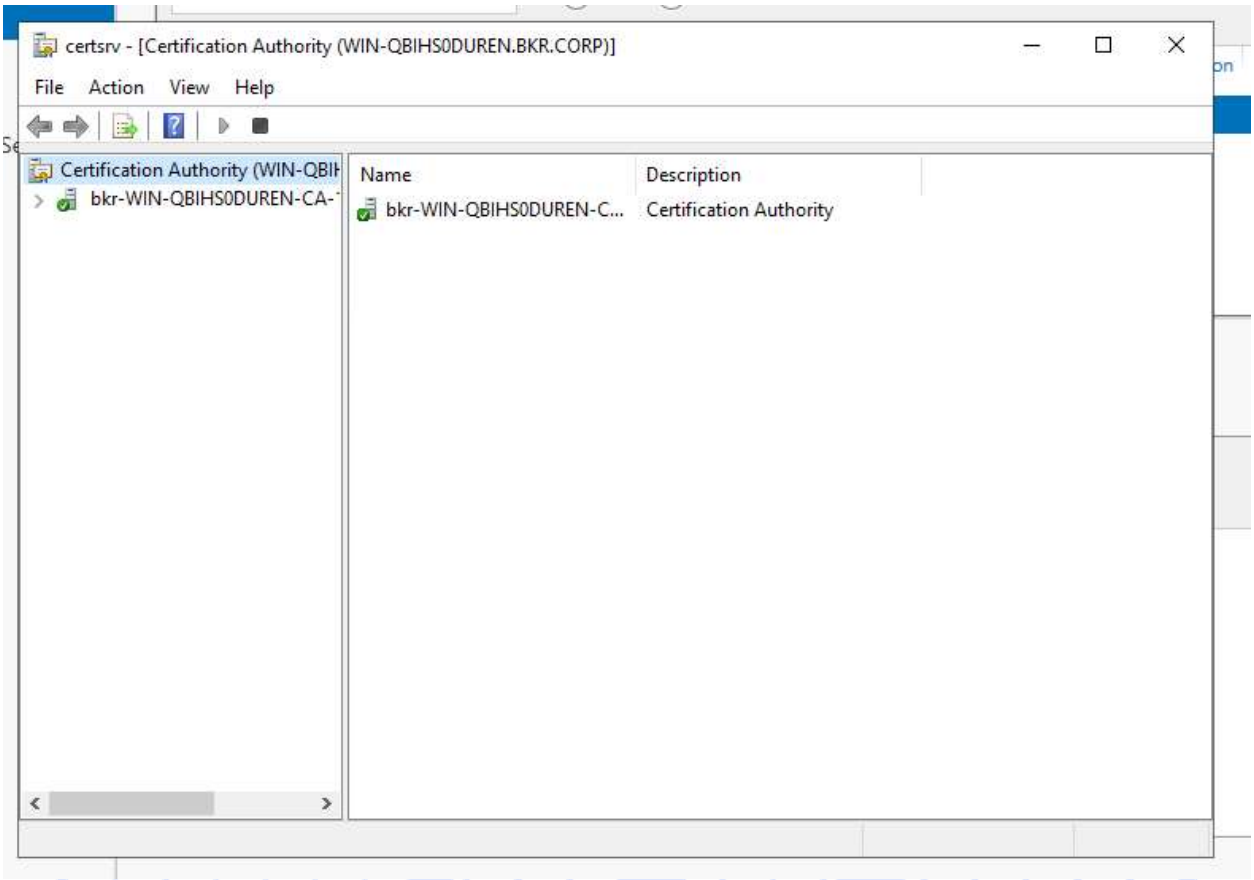


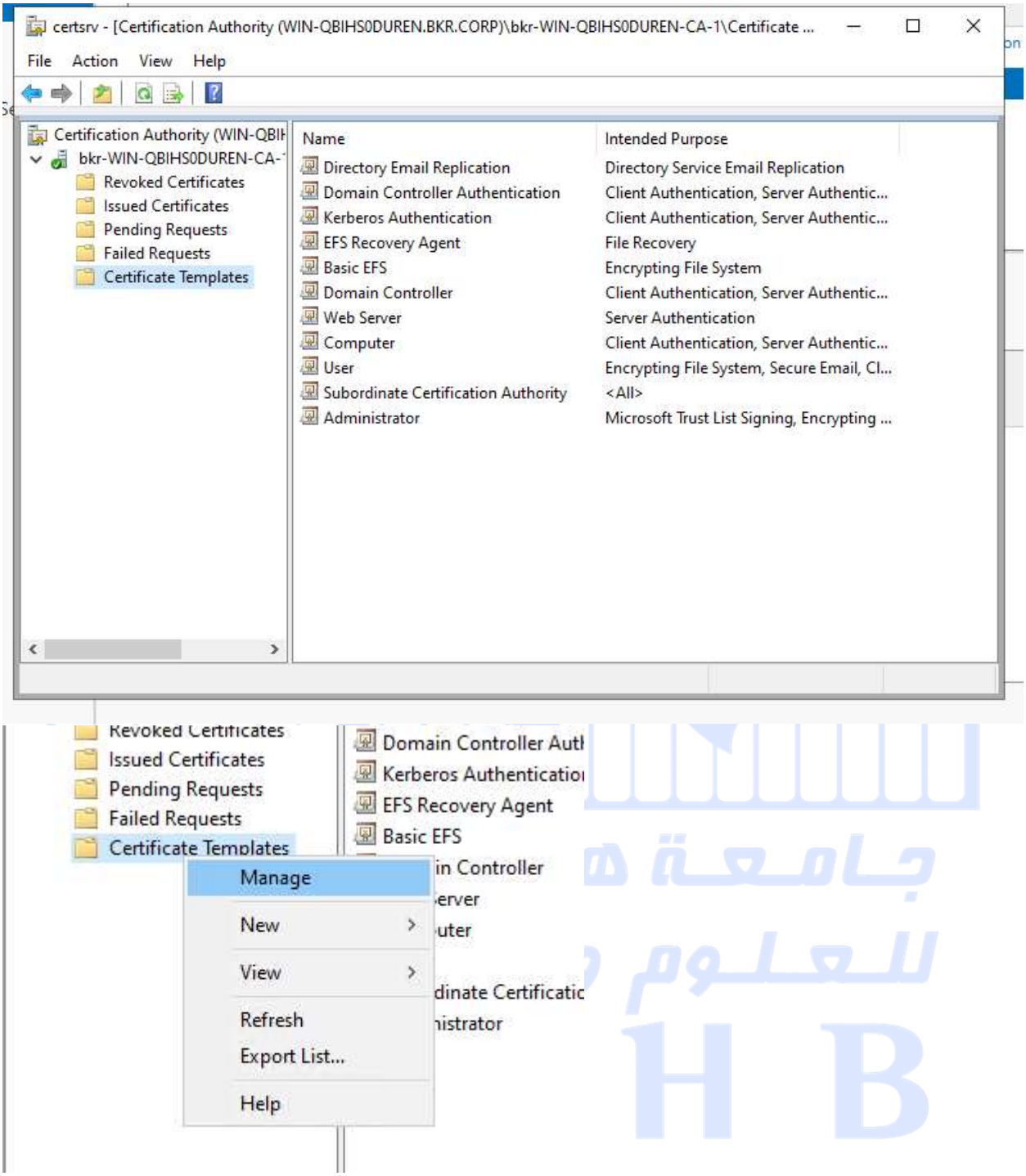


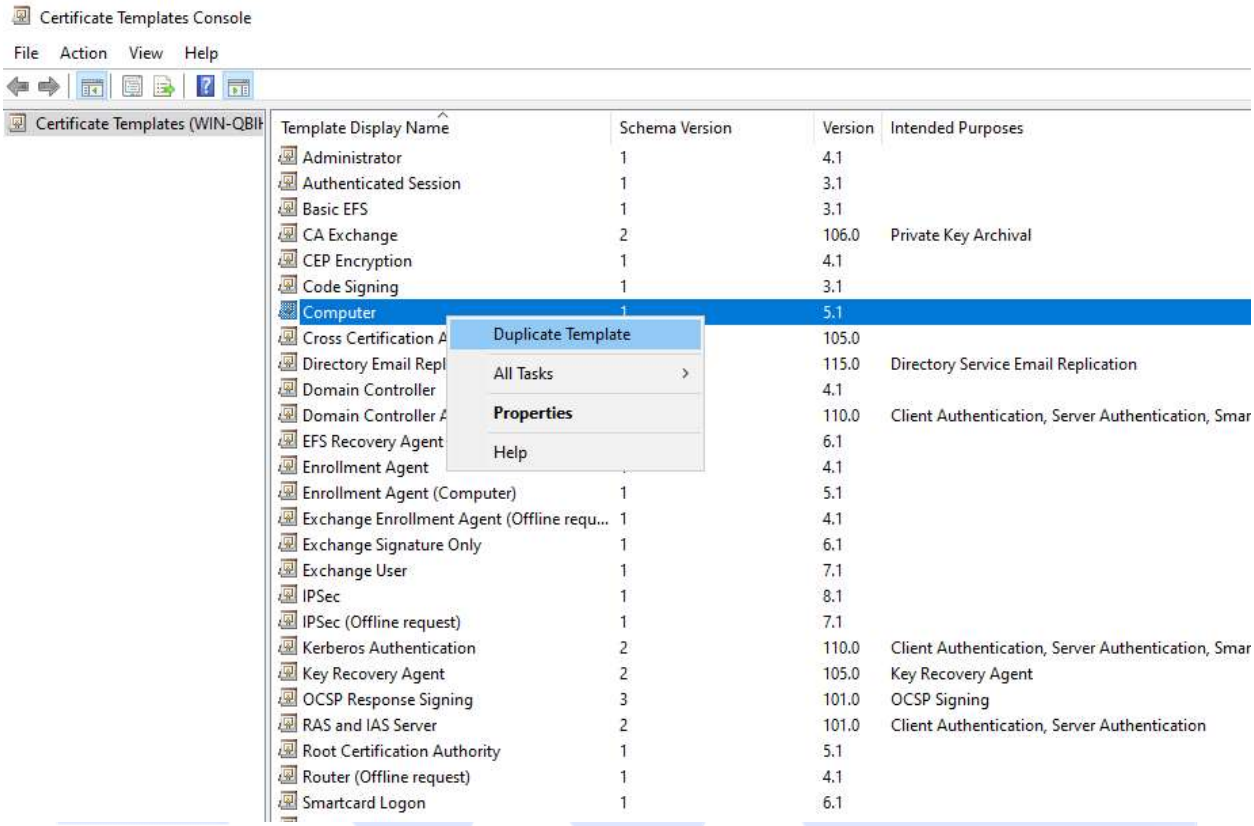


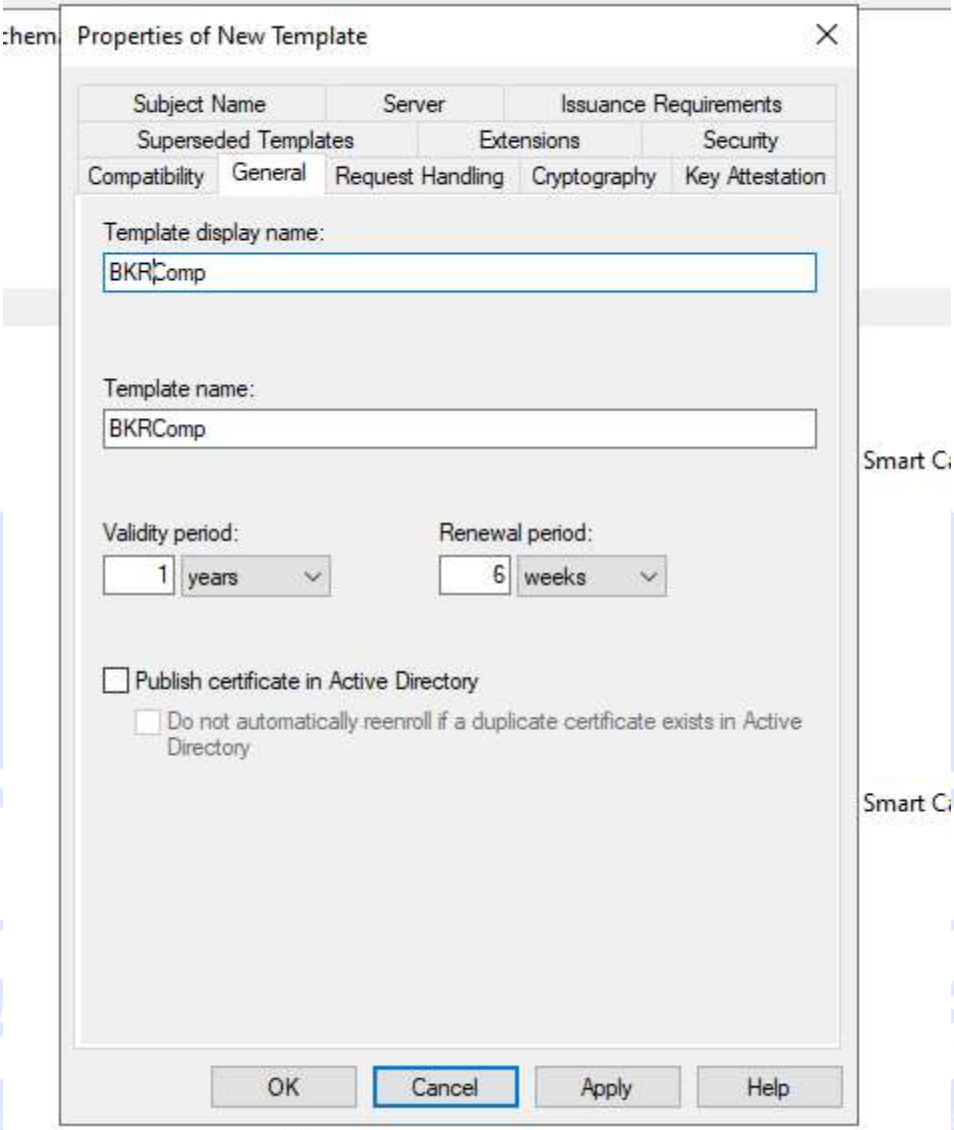

AD CS Configuration
Results
DESTINATION SERVER
WIN-QBIHS0DUREN.bkr.corp
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
The following roles, role services, or features were configured:
Active Directory Certificate Services
Certification Authority
Configuration succeeded
More about CA Configuration
Certification Authority Web Enrollment
Configuration succeeded
More about Web Enrollment Configuration
Certificate Enrollment Policy Web Service
Configuration succeeded
Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.
Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.
More about CEP Configuration
< Previous
Next >
Close
Cancel

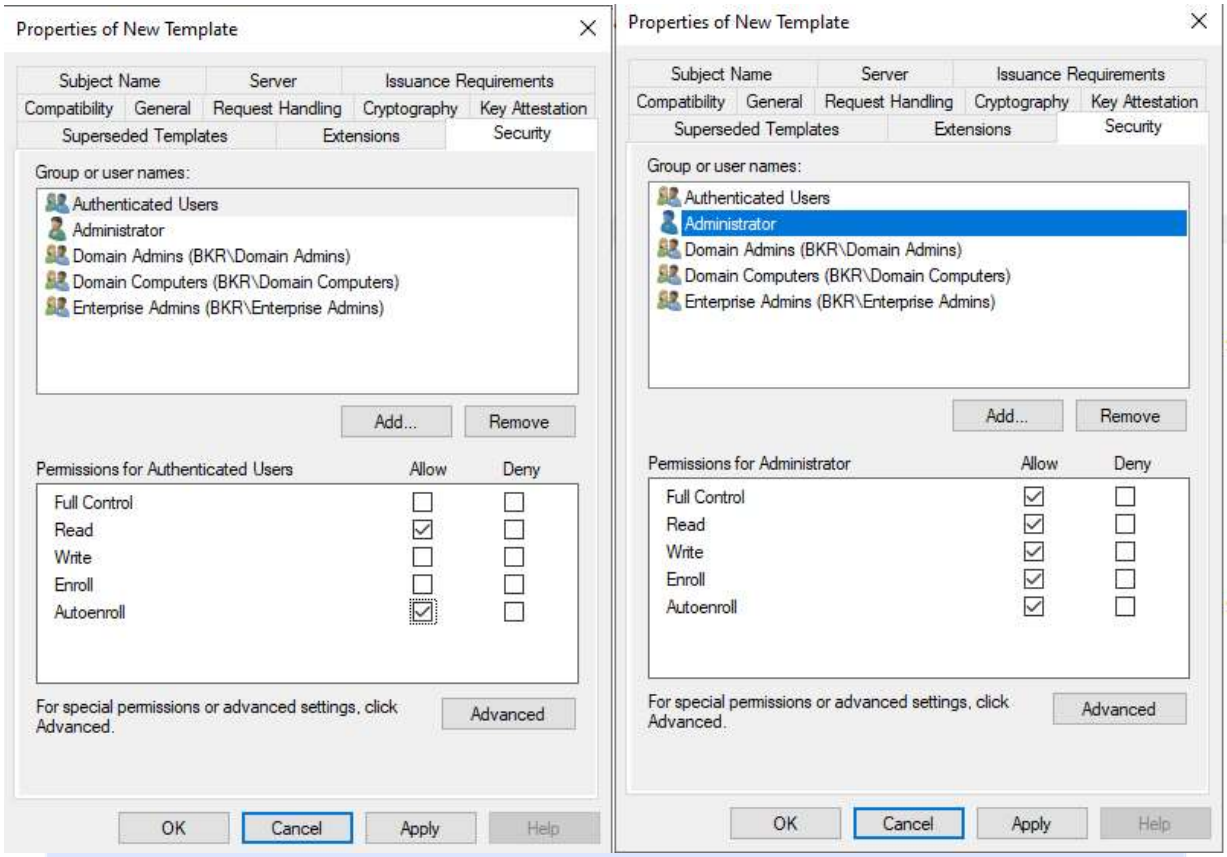

Server Manager • AD CS
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
SERVERS
All servers | 1 total
Configuration required for Active Directory Certificate Services at WIN-QBIHS0DUREN
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
Online - Performance counters not started
4/2/2024 8:57:04 AM
Not activated
Add Roles and Features
Shut Down Local Server
Computer Management
Remote Desktop Connection
Windows PowerShell
Configure NIC Teaming
Certification Authority
Manage As ...
Start Performance Counters
Refresh
Copy
Server Name
ID
Severity
Source
Log
Date and Time



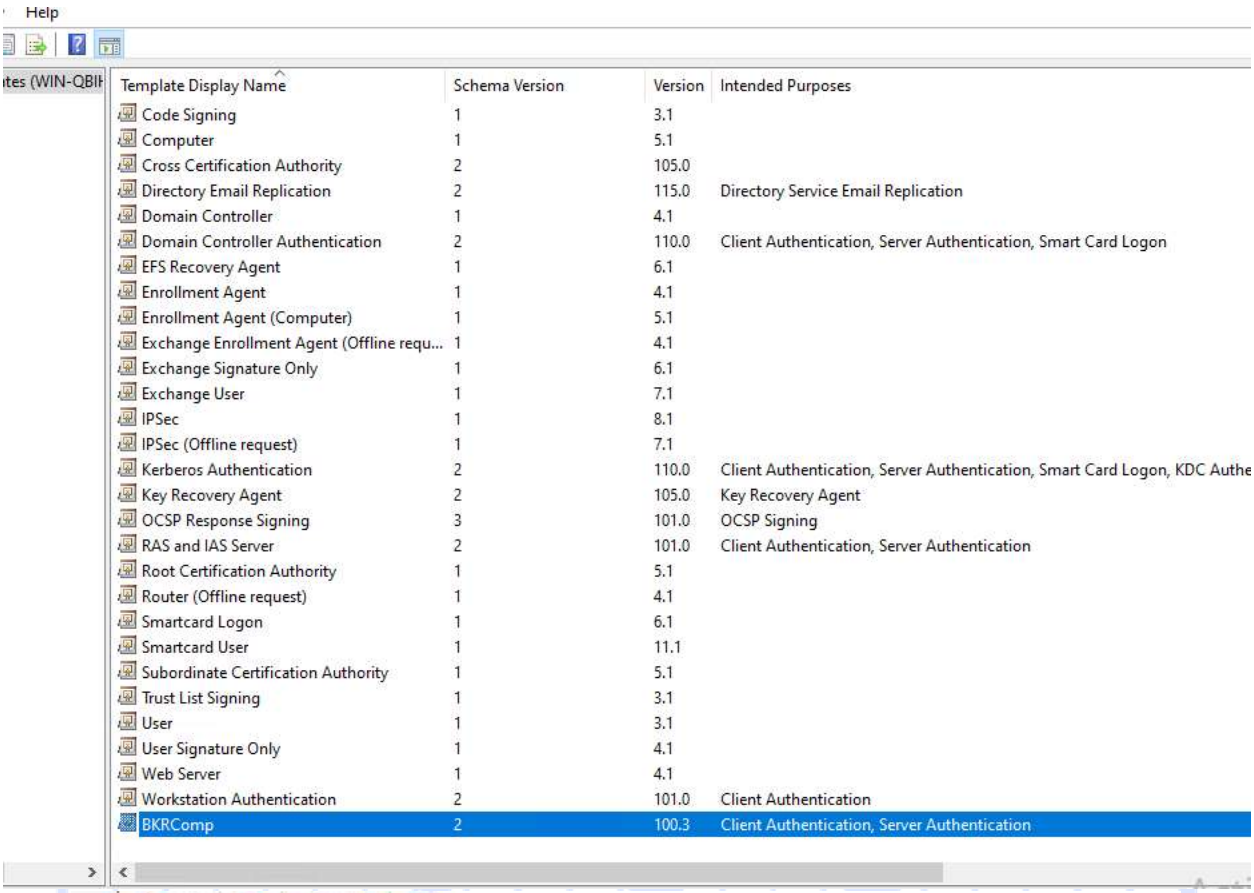

certsrv - [Certification Authority (WIN-QBIHS0DUREN.BKR.CORP)\bkr-WIN-QBIHS0DUREN-CA-1\Certificate ...
File
Action
View
Help
Certification Authority (WIN-QBIH
bkr-WIN-QBIHS0DUREN-CA-
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Domain Controller
Client Authentication, Server Authentic...
Web Server
Server Authentication
Computer
Client Authentication, Server Authentic...
User
Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority
<All>
Administrator
Microsoft Trust List Signing, Encrypting ...
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Domain Controller Auth
Kerberos Authentication
EFS Recovery Agent
Basic EFS
Manage
New
View
Refresh
Export List...
Help

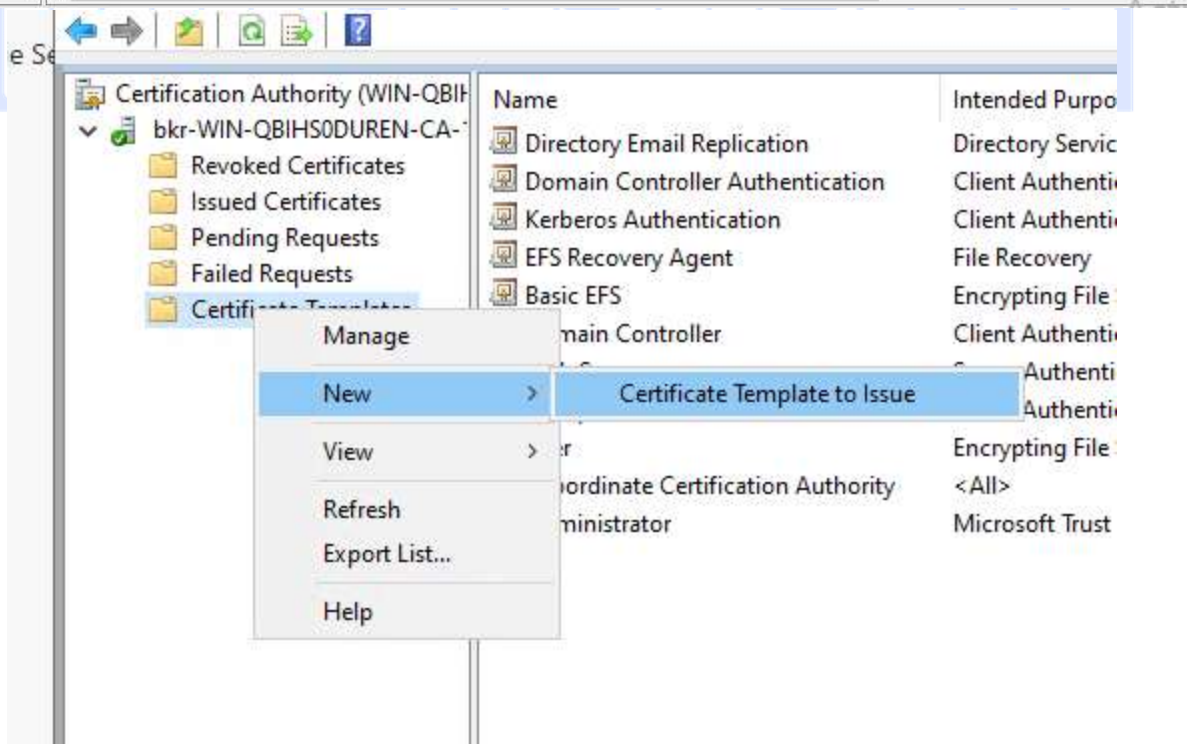


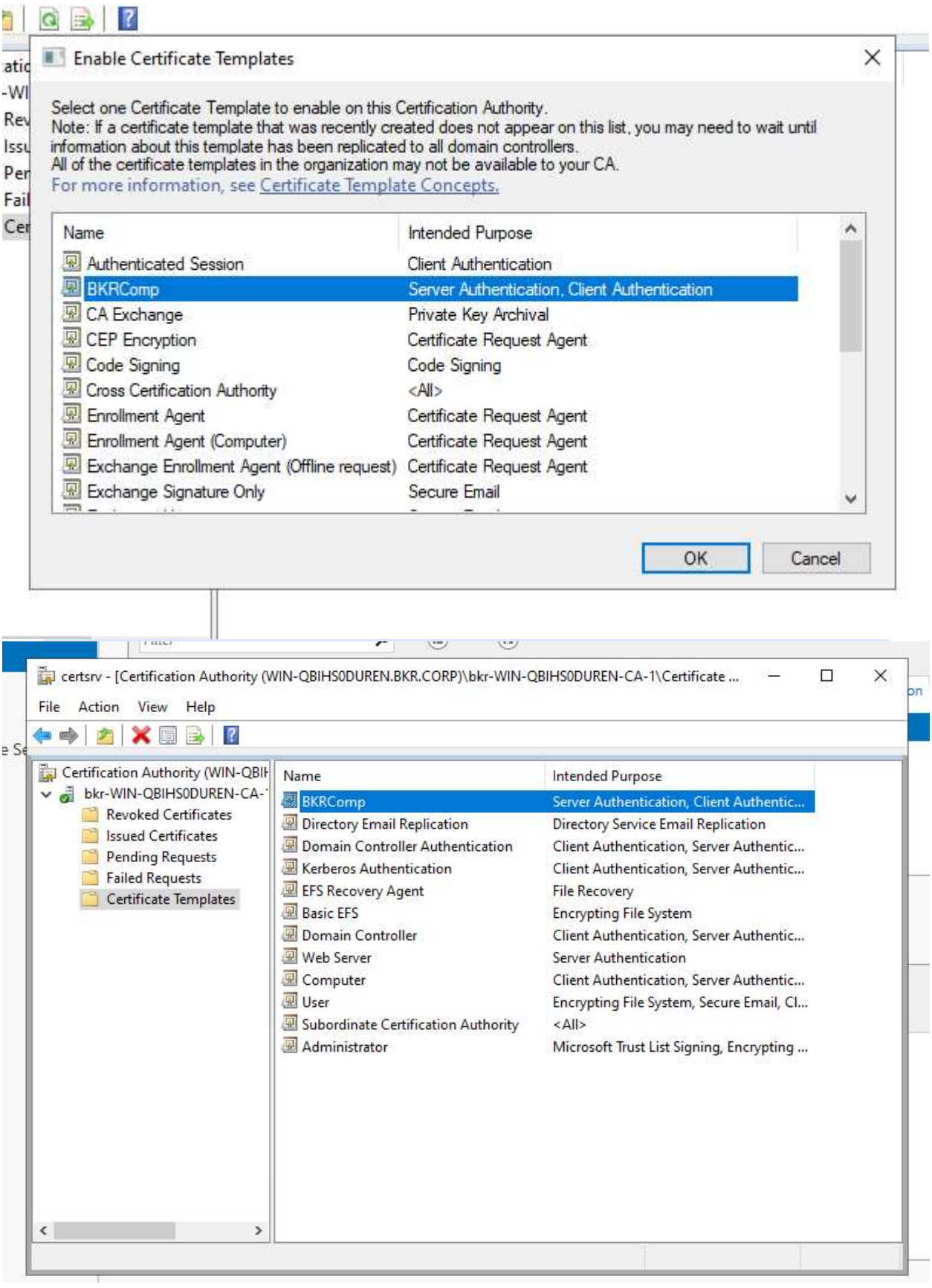

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
BKRComp
Template name:
BKRComp
Validity period:
1
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

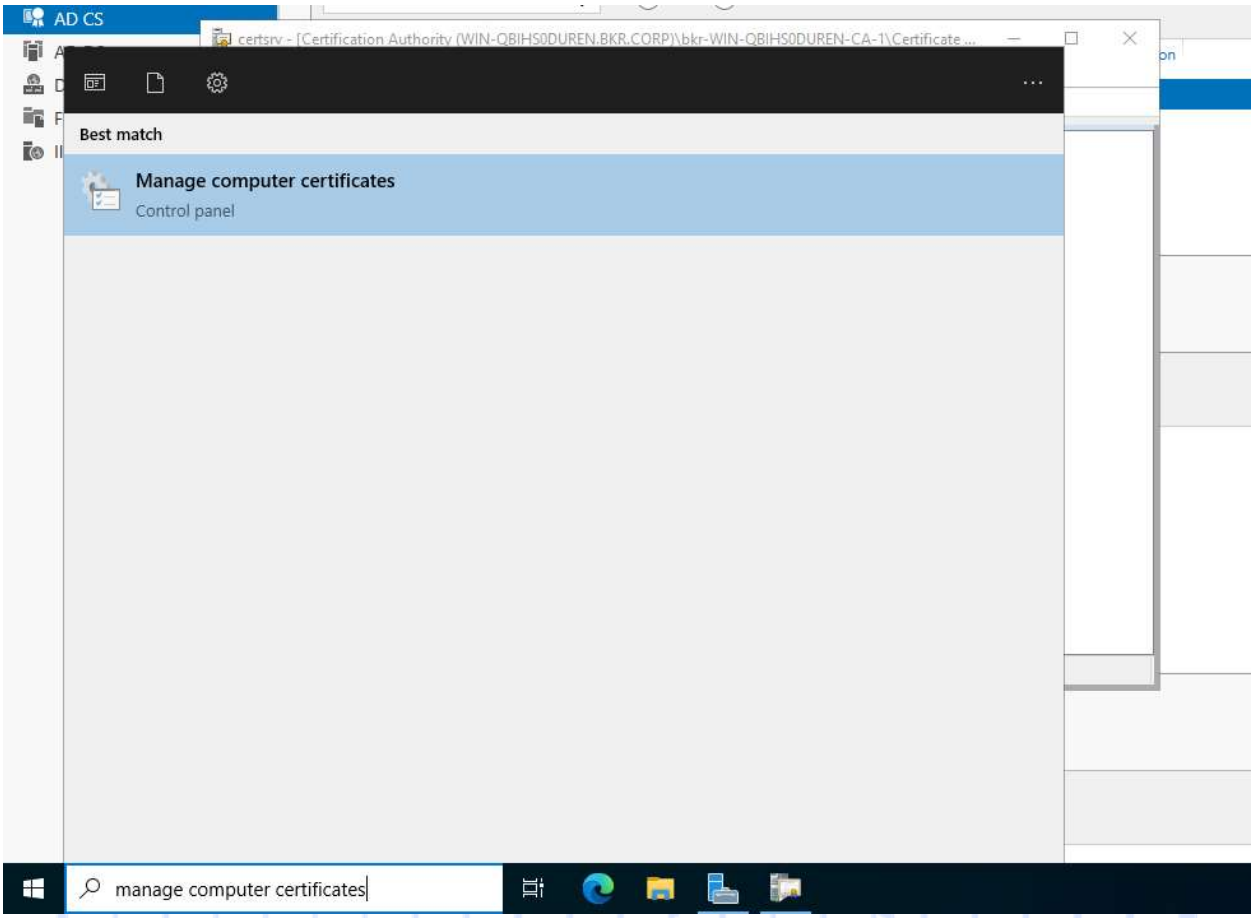


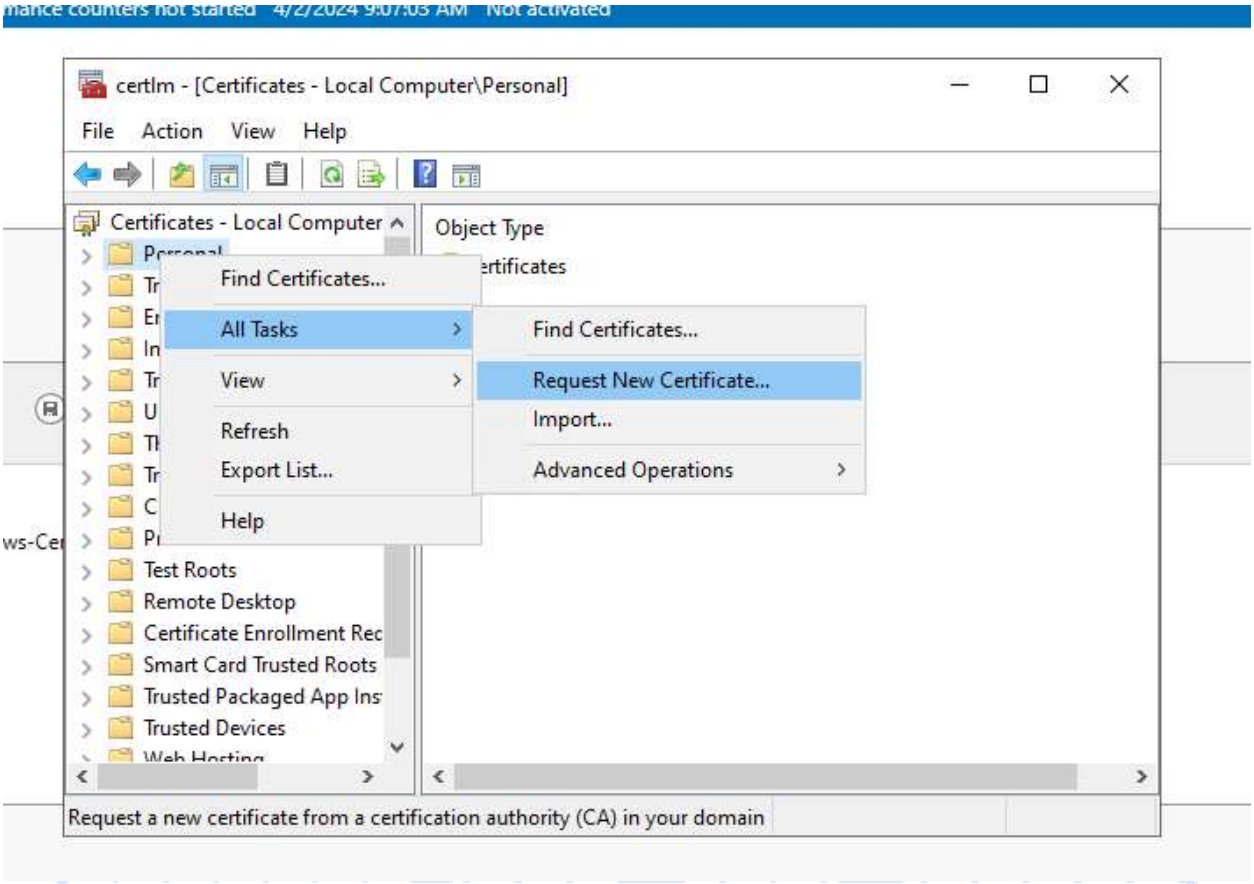
Note: Ensure that "Autoenroll" is selected for all users.

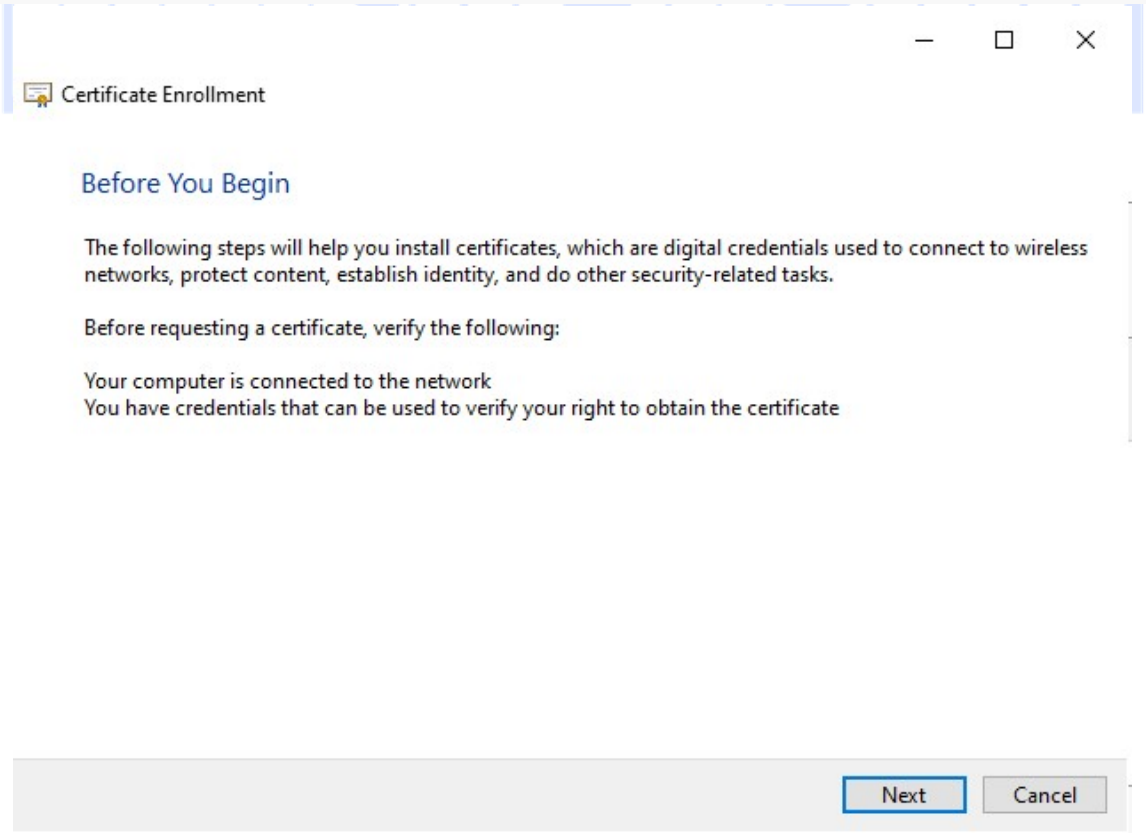

Help
Template Display Name
Schema Version
Version
Intended Purposes
Code Signing 1 3.1
Computer 1 5.1
Cross Certification Authority 2 105.0
Directory Email Replication 2 115.0 Directory Service Email Replication
Domain Controller 1 4.1
Domain Controller Authentication 2 110.0 Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent 1 6.1
Enrollment Agent 1 4.1
Enrollment Agent (Computer) 1 5.1
Exchange Enrollment Agent (Offline requ... 1 4.1
Exchange Signature Only 1 6.1
Exchange User 1 7.1
IPSec 1 8.1
IPSec (Offline request) 1 7.1
Kerberos Authentication 2 110.0 Client Authentication, Server Authentication, Smart Card Logon, KDC Authe
Key Recovery Agent 2 105.0 Key Recovery Agent
OCSP Response Signing 3 101.0 OCSP Signing
RAS and IAS Server 2 101.0 Client Authentication, Server Authentication
Root Certification Authority 1 5.1
Router (Offline request) 1 4.1
Smartcard Logon 1 6.1
Smartcard User 1 11.1
Subordinate Certification Authority 1 5.1
Trust List Signing 1 3.1
User 1 3.1
User Signature Only 1 4.1
Web Server 1 4.1
Workstation Authentication 2 101.0 Client Authentication
BKRComp 2 100.3 Client Authentication, Server Authentication

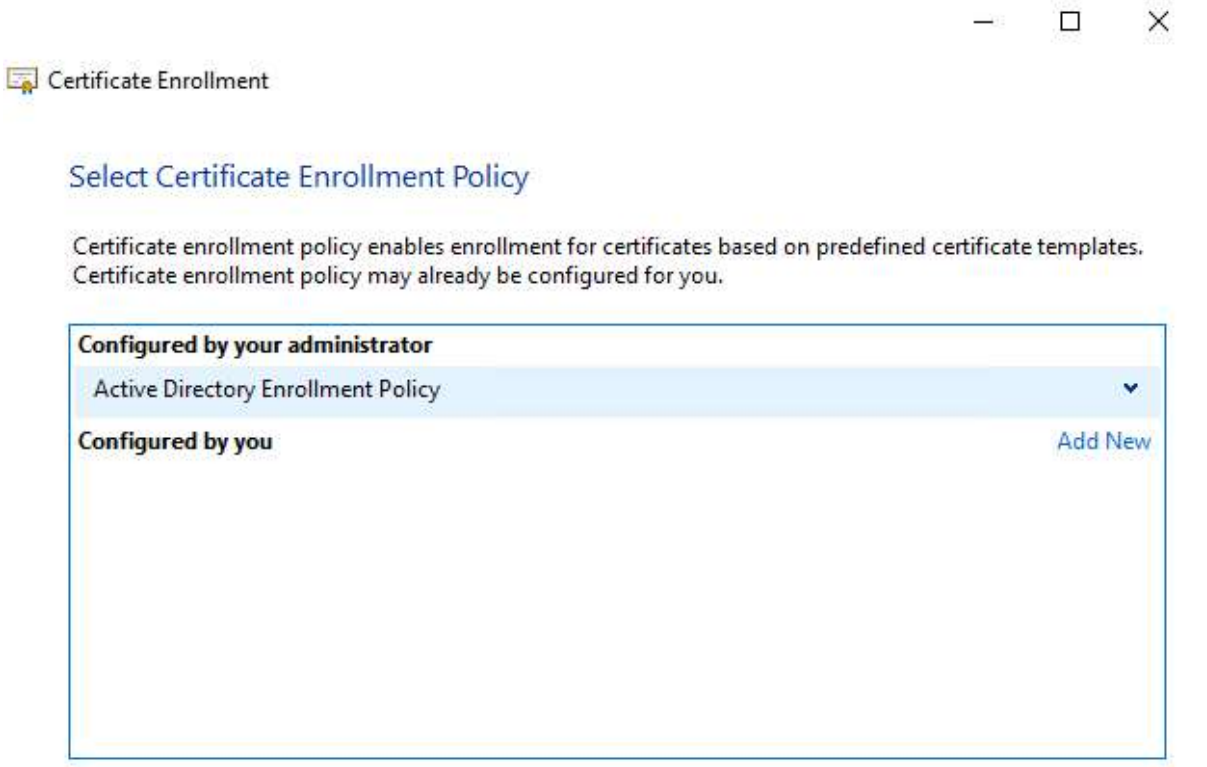

Certification Authority (WIN-QBIH
bkr-WIN-QBIHS0DUREN-CA-
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Name
Intended Purpo
Directory Email Replication
Directory Servic
Domain Controller Authentication
Client Authenti
Kerberos Authentication
Client Authenti
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File
Client Authenti
Manage
New
Certificate Template to Issue
View
Refresh
Export List...
Help
Encrypting File
<All>
Microsoft Trust

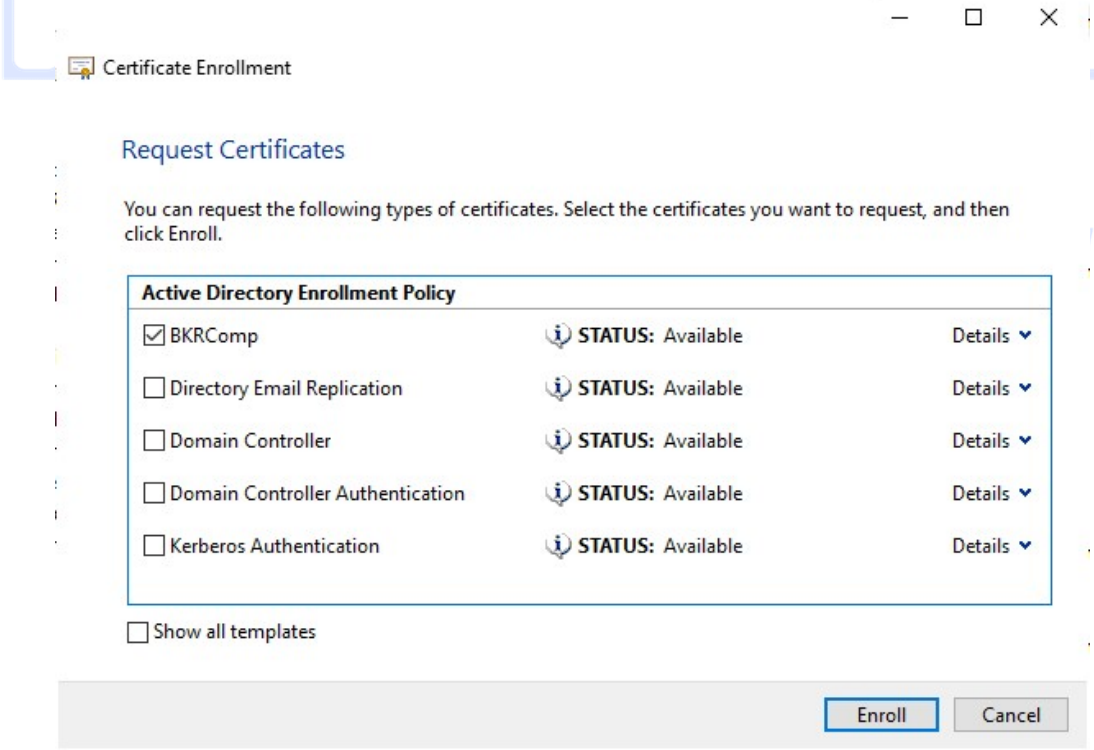

Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
Authenticated Session
Client Authentication
BKRComp
Server Authentication, Client Authentication
CA Exchange
Private Key Archival
CEP Encryption
Certificate Request Agent
Code Signing
Code Signing
Cross Certification Authority
<All>
Enrollment Agent
Certificate Request Agent
Enrollment Agent (Computer)
Certificate Request Agent
Exchange Enrollment Agent (Offline request)
Certificate Request Agent
Exchange Signature Only
Secure Email
OK
Cancel
certsrv - [Certification Authority (WIN-QBIHS0DUREN.BKR.CORP)\bkr-WIN-QBIHS0DUREN-CA-1\Certificate ...
File
Action
View
Help
Certification Authority (WIN-QBIH
bkr-WIN-QBIHS0DUREN-CA-
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
BKRComp
Server Authentication, Client Authentic...
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Domain Controller
Client Authentication, Server Authentic...
Web Server
Server Authentication
Computer
Client Authentication, Server Authentic...
User
Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority
<All>
Administrator
Microsoft Trust List Signing, Encrypting ...



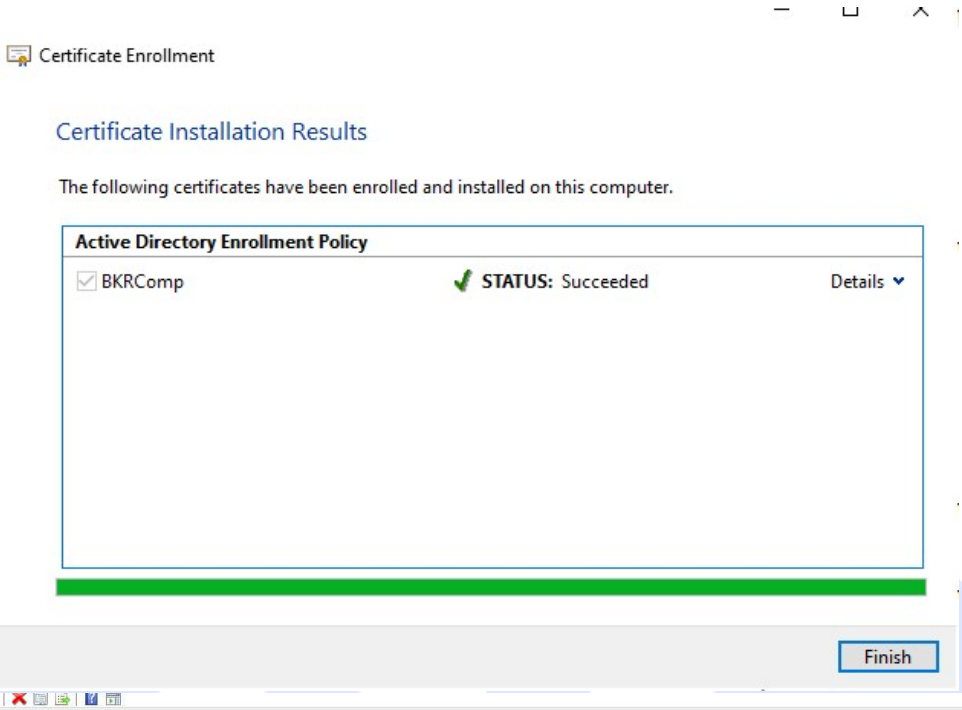

certlm - [Certificates - Local Computer\Personal]
File Action View Help
Certificates - Local Computer
Personal
Object Type
Find Certificates...
All Tasks
View
Refresh
Export List...
Help
Find Certificates...
Request New Certificate...
Import...
Advanced Operations
Test Roots
Remote Desktop
Certificate Enrollment Rec
Smart Card Trusted Roots
Trusted Packaged App Ins
Trusted Devices
Request a new certificate from a certification authority (CA) in your domain

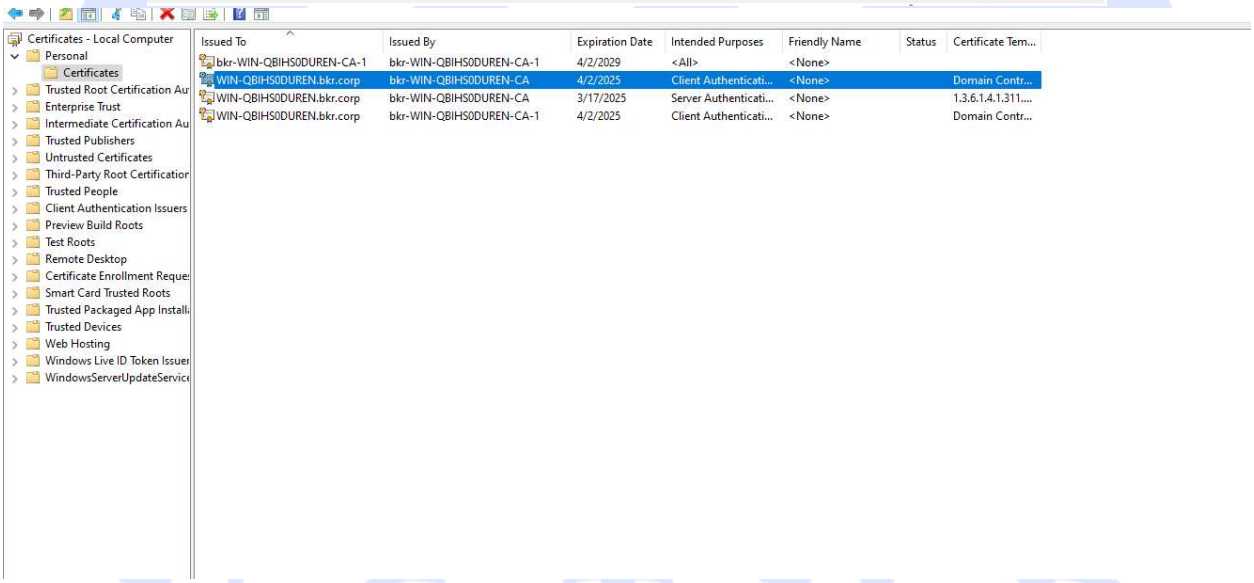

Certificate Enrollment
Before You Begin
The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
Before requesting a certificate, verify the following:
Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate
Next
Cancel





Make sure your certificate is displayed above!



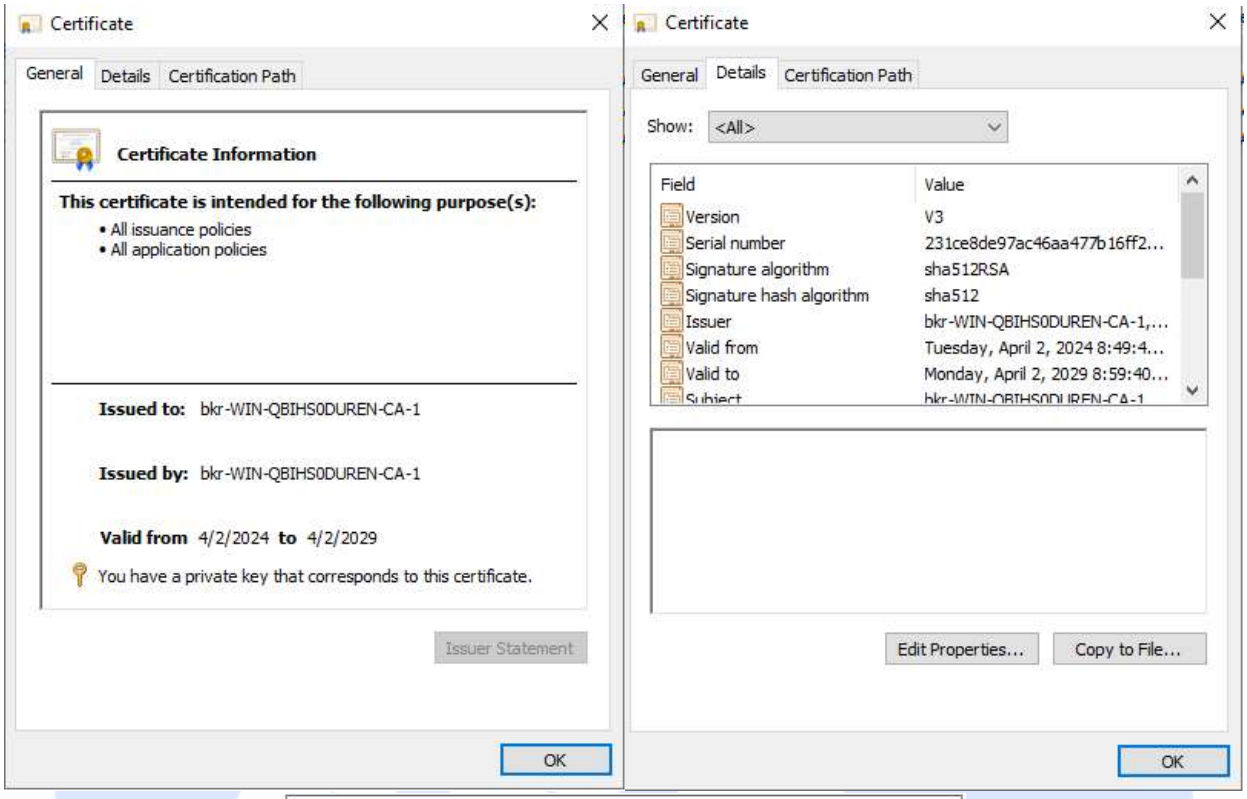


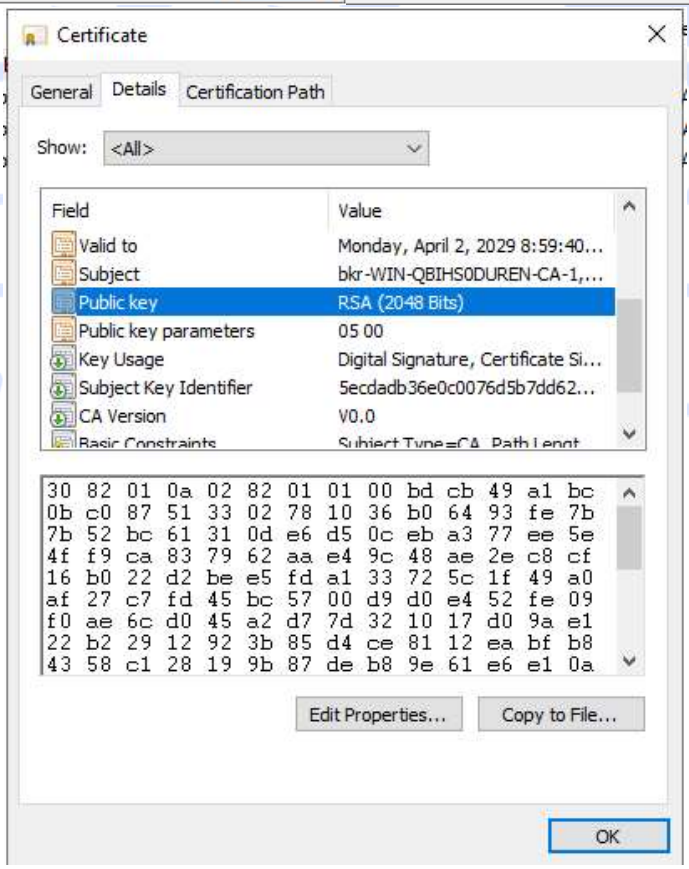
To view the certificate properties, right-click on the certificate you want to inspect then select "Properties" from the context menu.

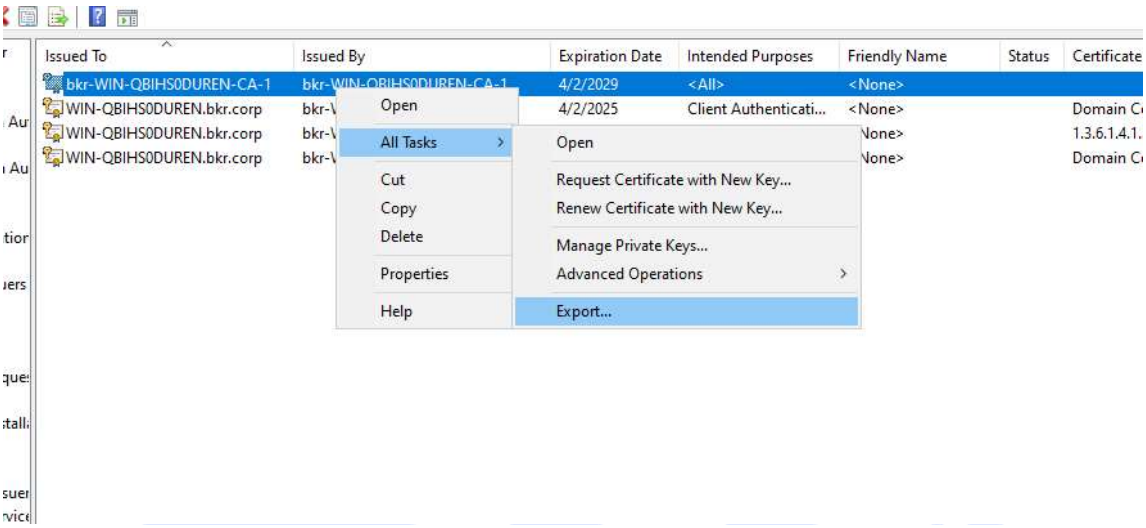
The properties of the certificate typically include details such as:

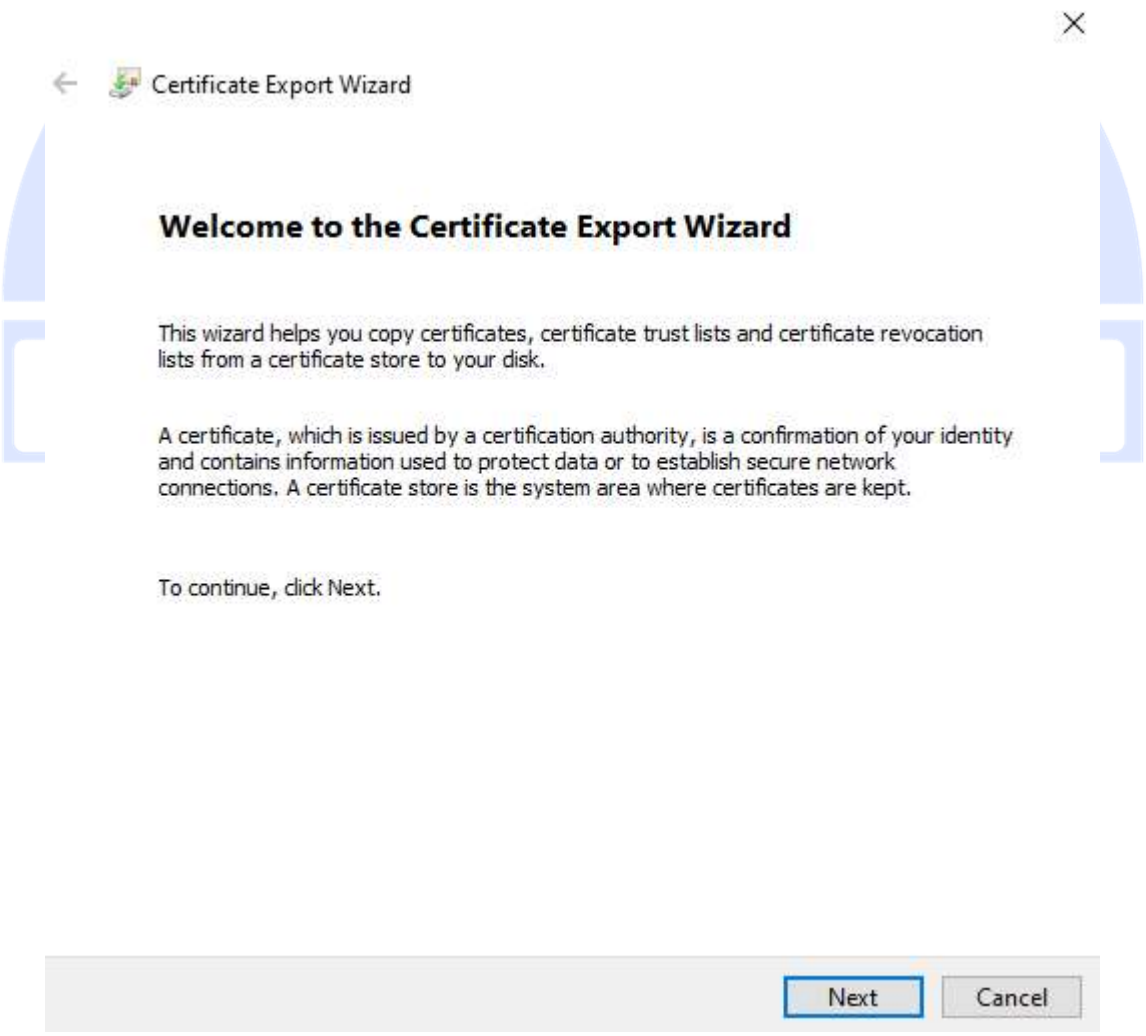
Version, Subject, Issuer, Validity period, Public key, Key usage, Extended Key Usage (EKU), Thumbprint, Serial number, Signature algorithm, Certificate chain, Certificate policies, Certificate Revocation List (CRL) distribution points, Authority Information Access (AIA) extensions, Subject Alternative Names (SANs), Basic Constraints, Enhanced Key Usage (EKU), Certificate templates used (if applicable), Revocation status.

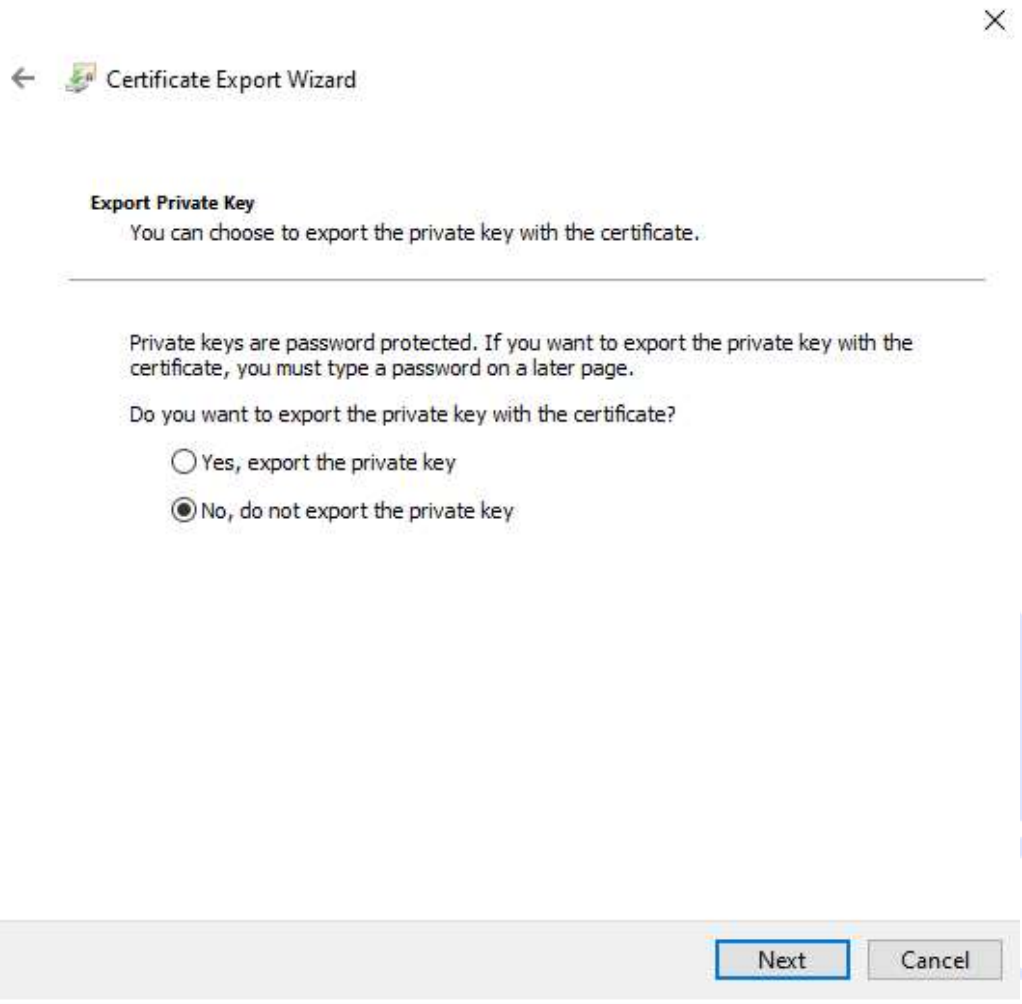
These details provide information about the certificate's identity, usage, validity, and associated cryptographic properties.

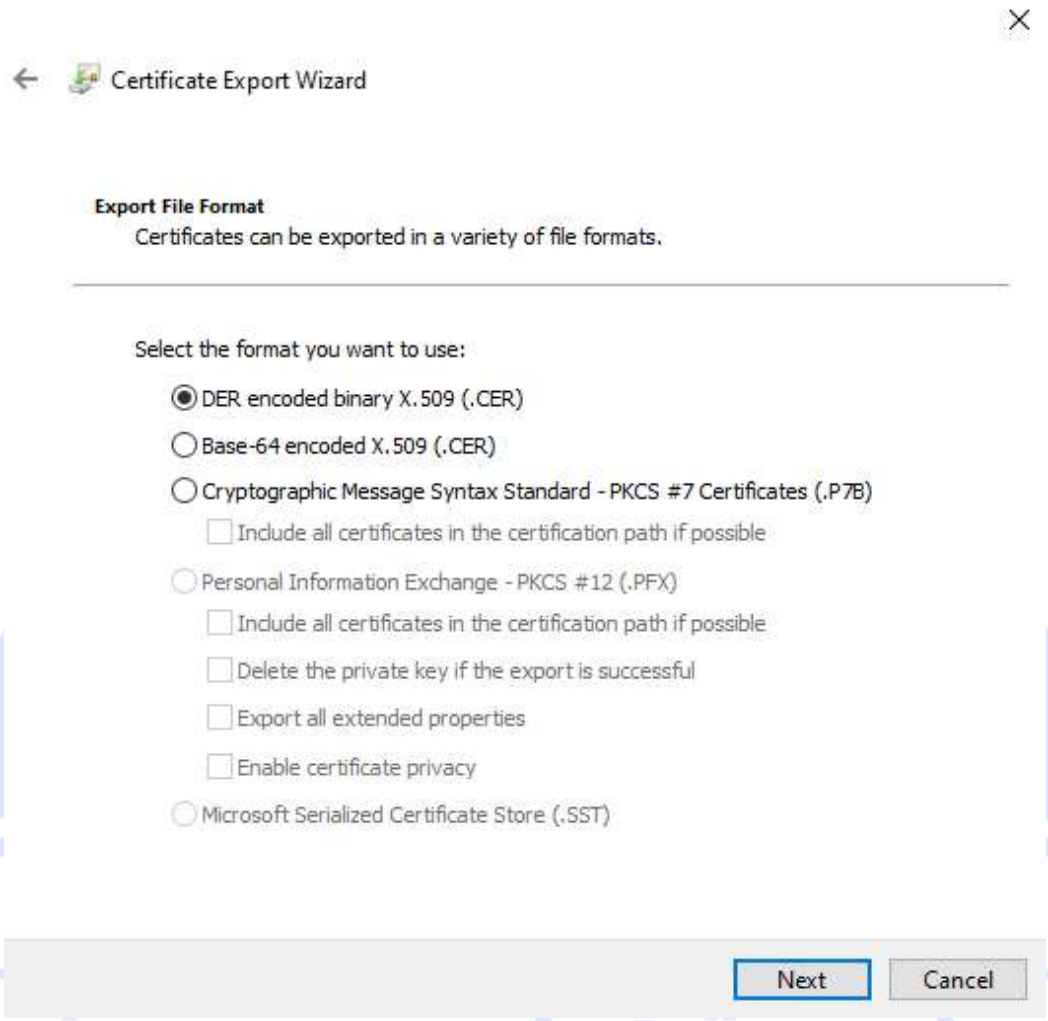

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: bkr-WIN-QBIHS0DUREN-CA-1
Issued by: bkr-WIN-QBIHS0DUREN-CA-1
Valid from 4/2/2024 to 4/2/2029
You have a private key that corresponds to this certificate.
Issuer Statement
OK
Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
231ce8de97ac46aa477b16ff2...
Signature algorithm
sha512RSA
Signature hash algorithm
sha512
Issuer
bkr-WIN-QBIHS0DUREN-CA-1,...
Valid from
Tuesday, April 2, 2024 8:49:4...
Valid to
Monday, April 2, 2029 8:59:40...
Edit Properties...
Copy to File...
OK

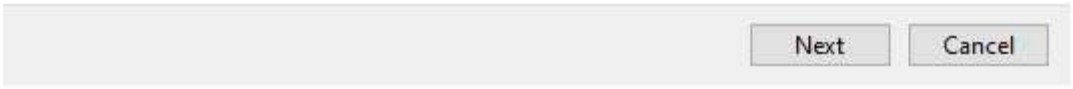

Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Valid to
Monday, April 2, 2029 8:59:40...
Subject
bkr-WIN-QBIHS0DUREN-CA-1,...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Key Usage
Digital Signature, Certificate Si...
Subject Key Identifier
5ecdadb36e0c0076d5b7dd62...
CA Version
V0.0
30 82 01 0a 02 82 01 01 00 bd cb 49 a1 bc
0b c0 87 51 33 02 78 10 36 b0 64 93 fe 7b
7b 52 bc 61 31 0d e6 d5 0c eb a3 77 ee 5e
4f f9 ca 83 79 62 aa e4 9c 48 ae 2e c8 cf
16 b0 22 d2 be e5 fd a1 33 72 5c 1f 49 a0
af 27 c7 fd 45 bc 57 00 d9 d0 e4 52 fe 09
f0 ae 6c d0 45 a2 d7 7d 32 10 17 d0 9a e1
22 b2 29 12 92 3b 85 d4 ce 81 12 ea bf b8
43 58 c1 28 19 9b 87 de b8 9e 61 e6 e1 0a
Edit Properties...
Copy to File...
OK

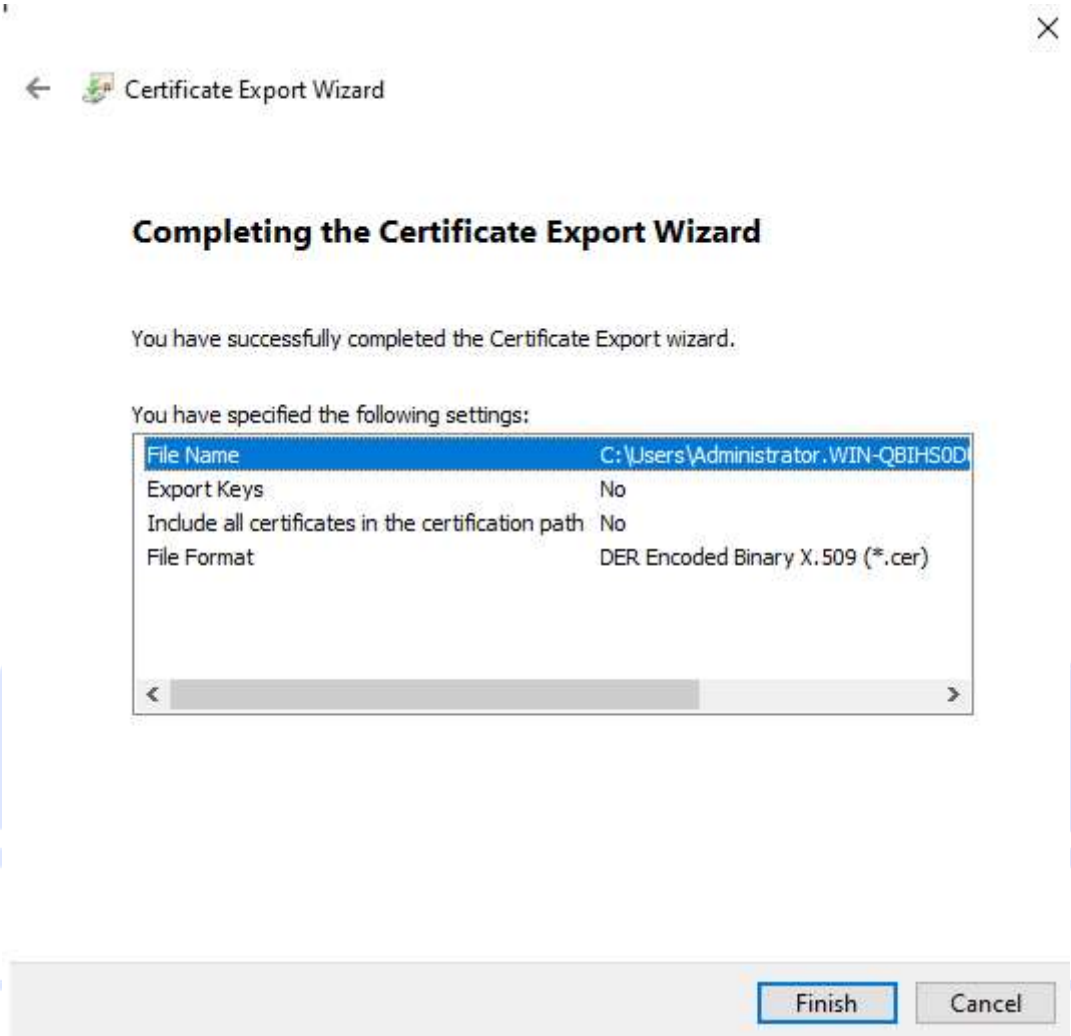

Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Status
Certificate
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2029
<All>
<None>
WIN-QBIHS0DUREN.bkr.corp
4/2/2025
Client Authenticati...
<None>
Domain C
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

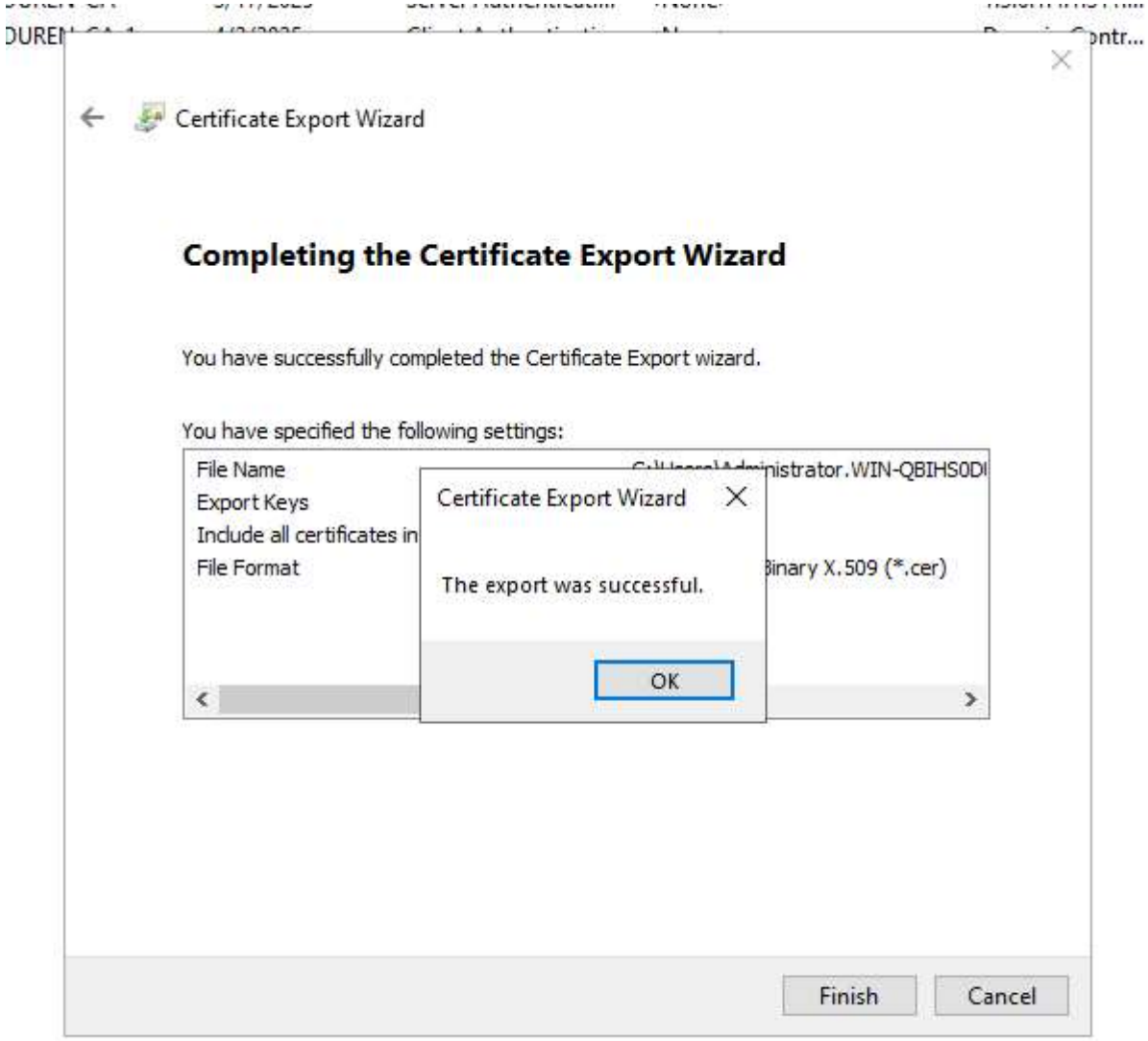

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel

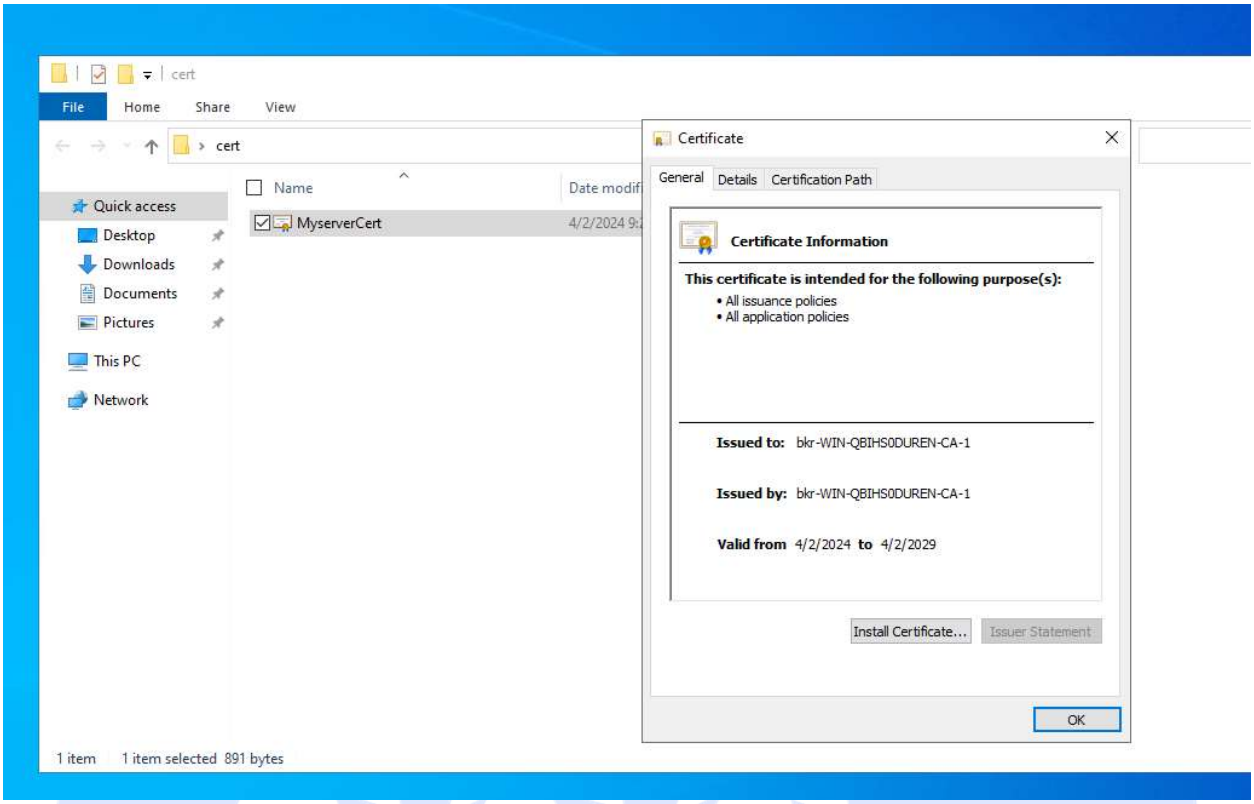




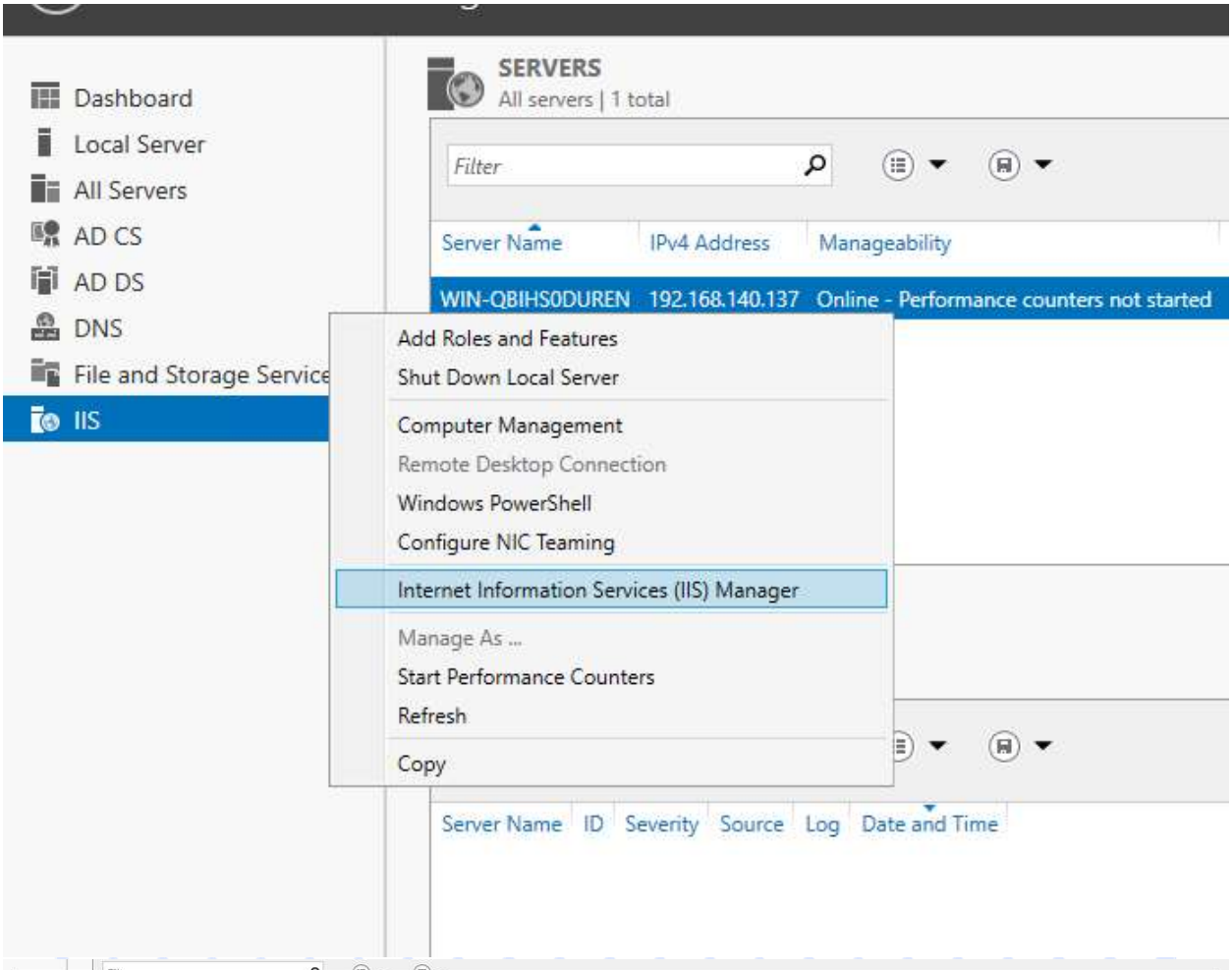


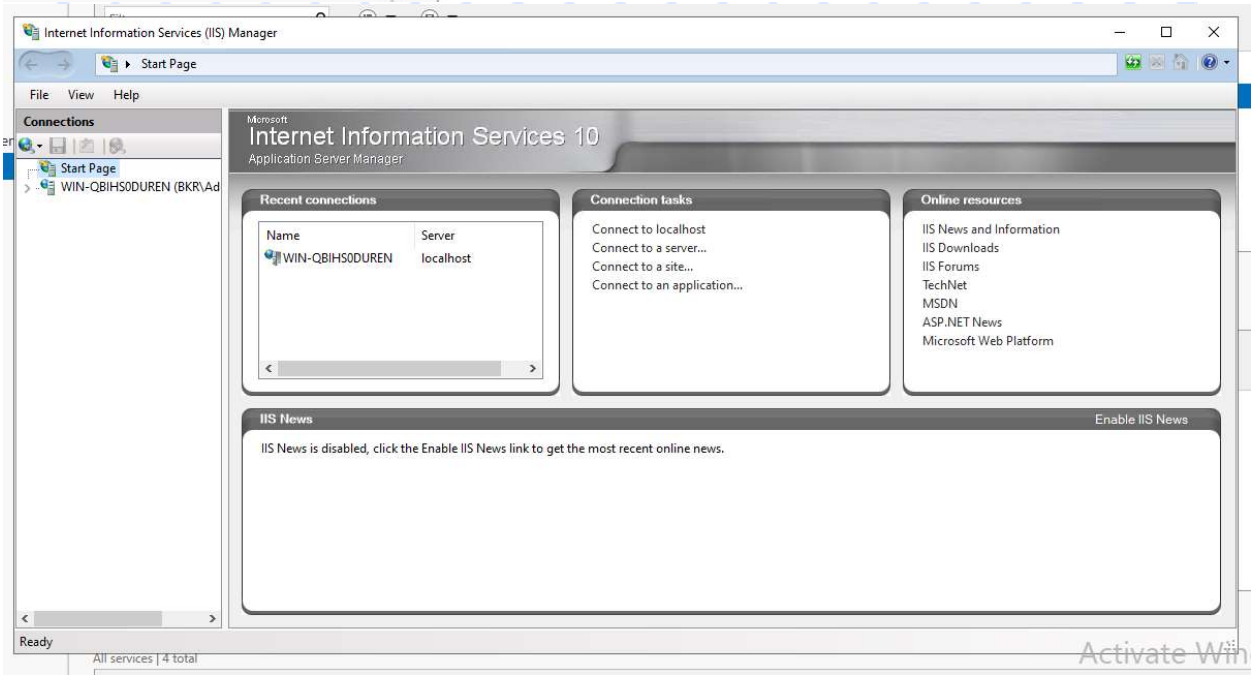


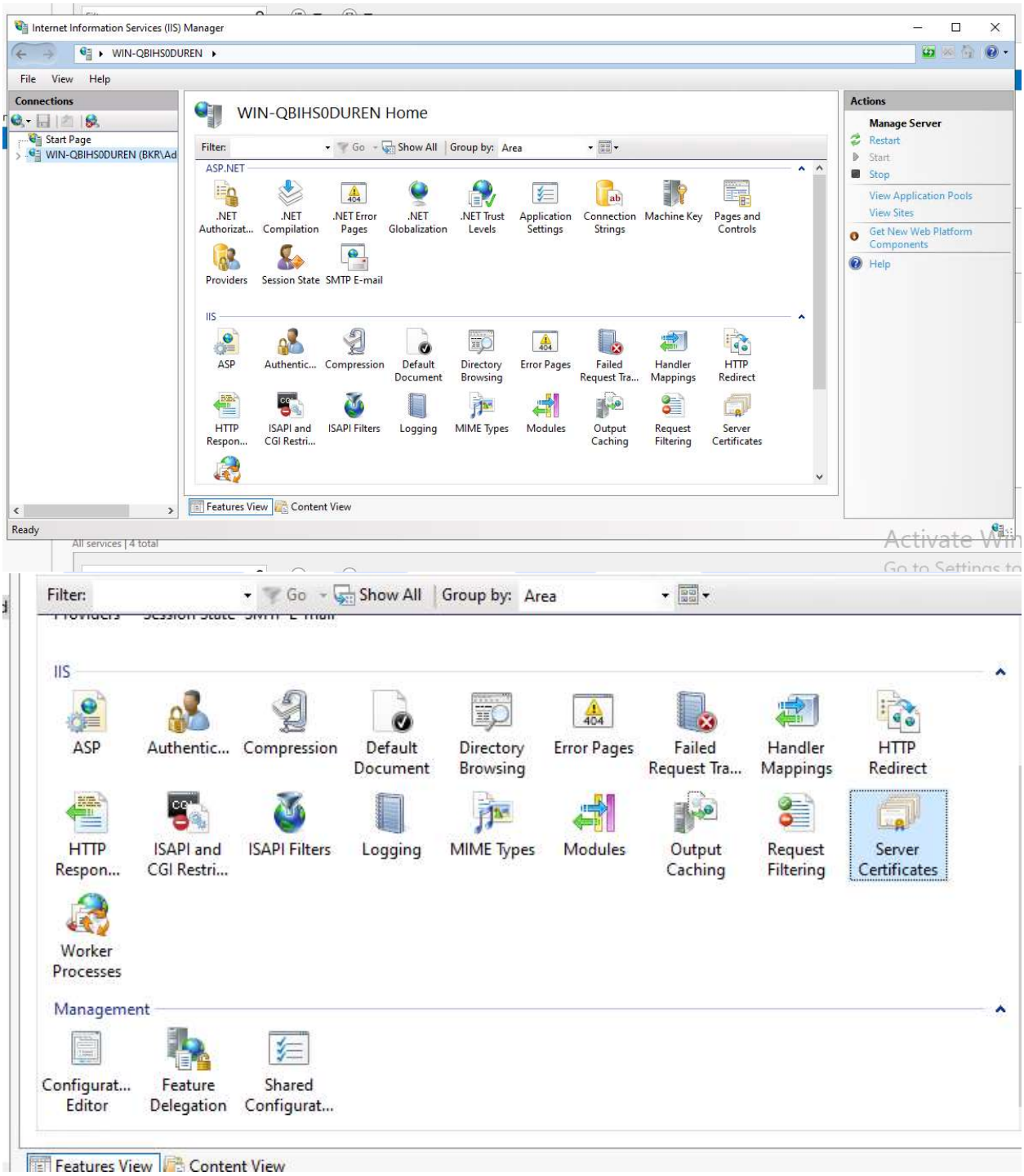


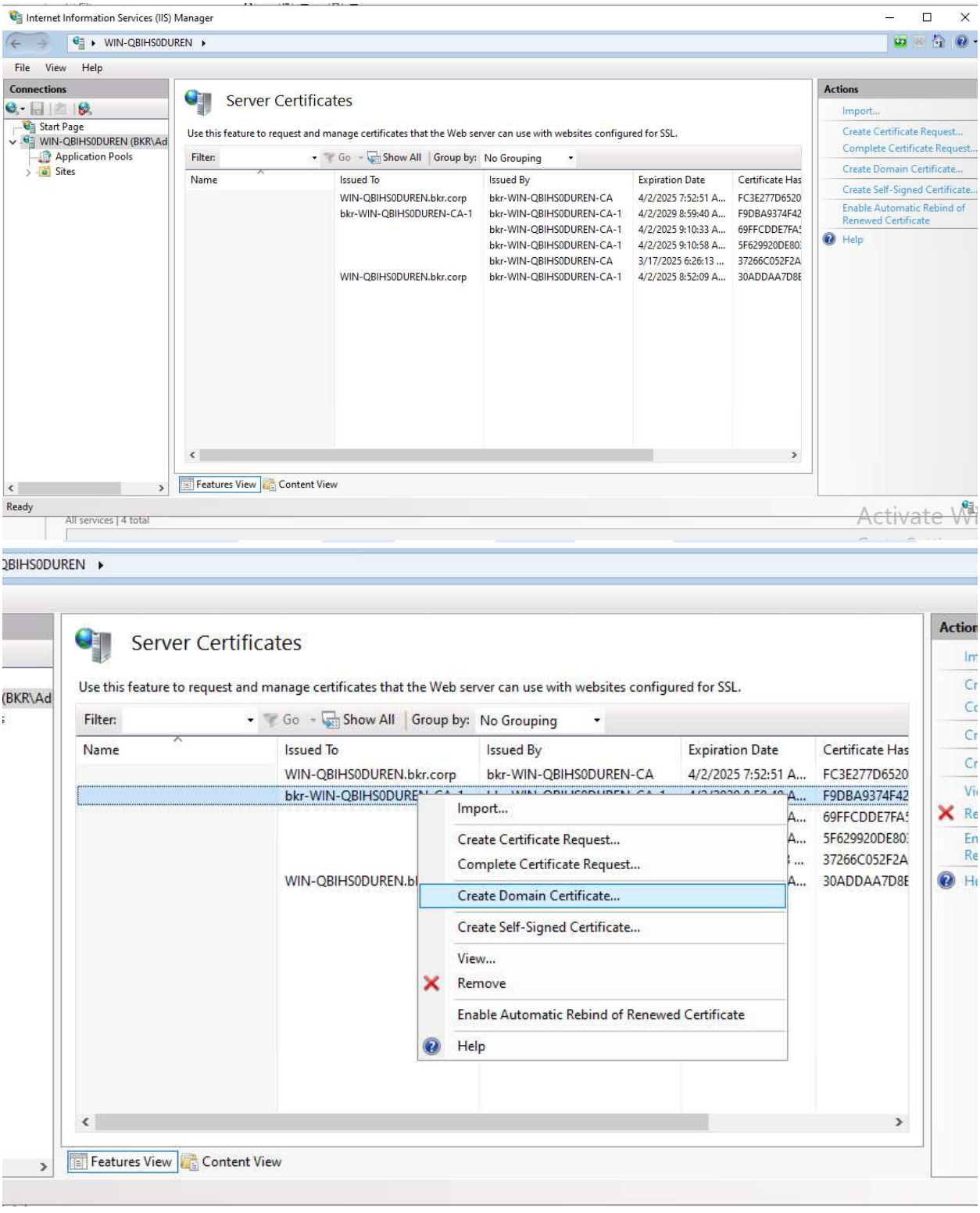


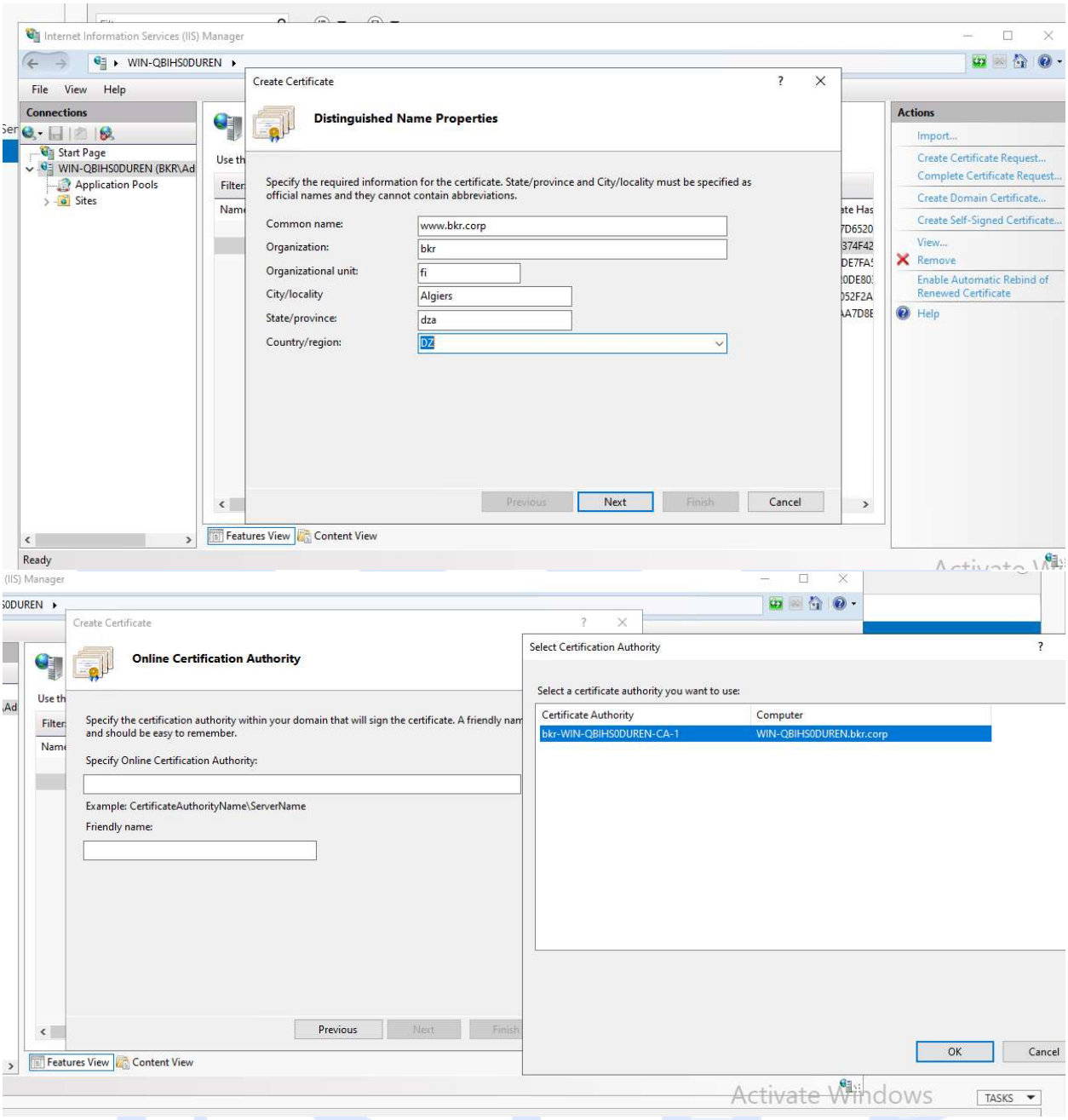
Now that the certificate has been created and exported, we will proceed to utilize it by adding it to our webpage.

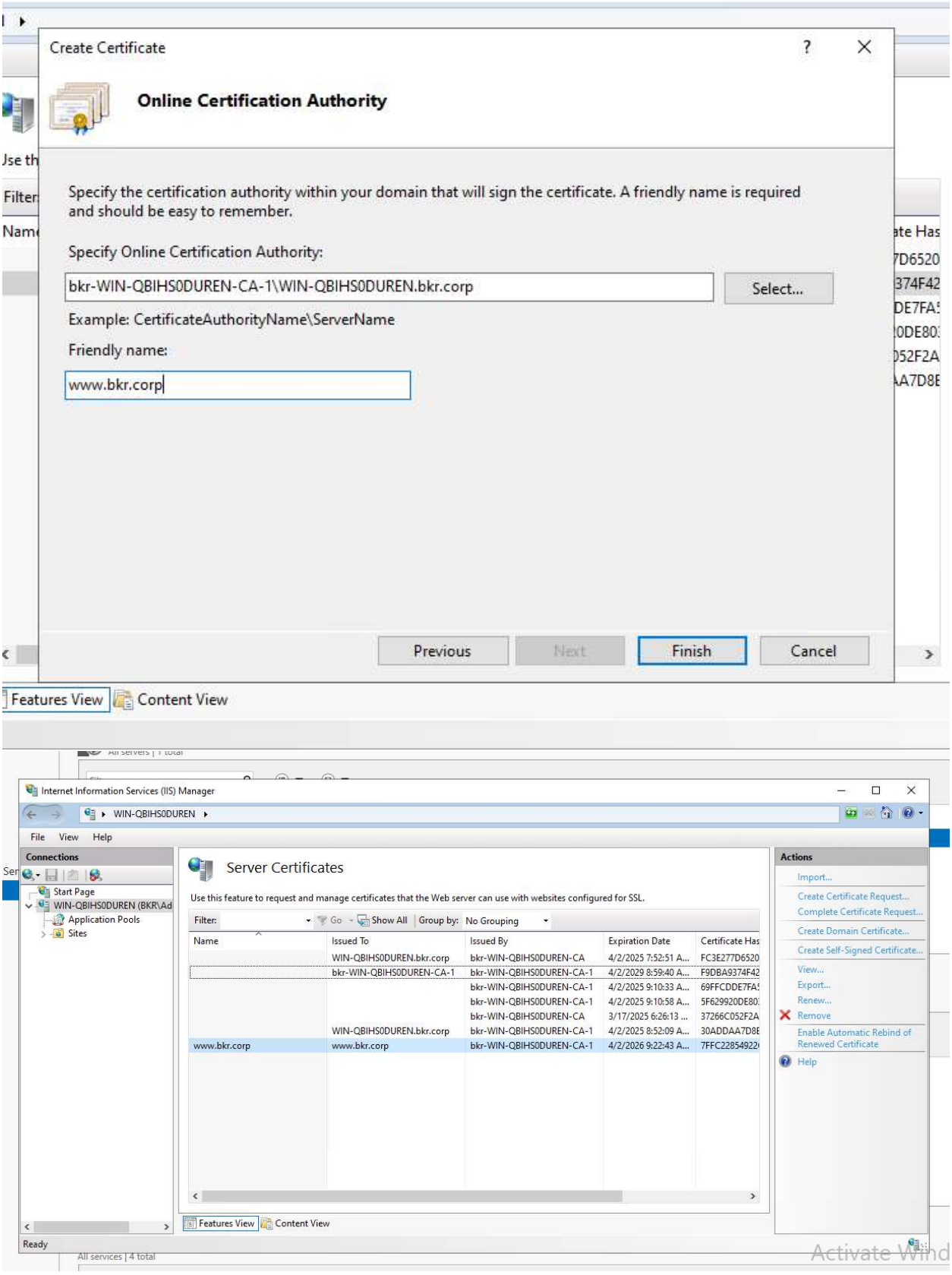

Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Service
IIS
SERVERS
All servers | 1 total
Filter
Server Name
IPv4 Address
Manageability
WIN-QBIHS0DUREN 192.168.140.137 Online - Performance counters not started
Add Roles and Features
Shut Down Local Server
Computer Management
Remote Desktop Connection
Windows PowerShell
Configure NIC Teaming
Internet Information Services (IIS) Manager
Manage As ...
Start Performance Counters
Refresh
Copy
Server Name
ID
Severity
Source
Log
Date and Time

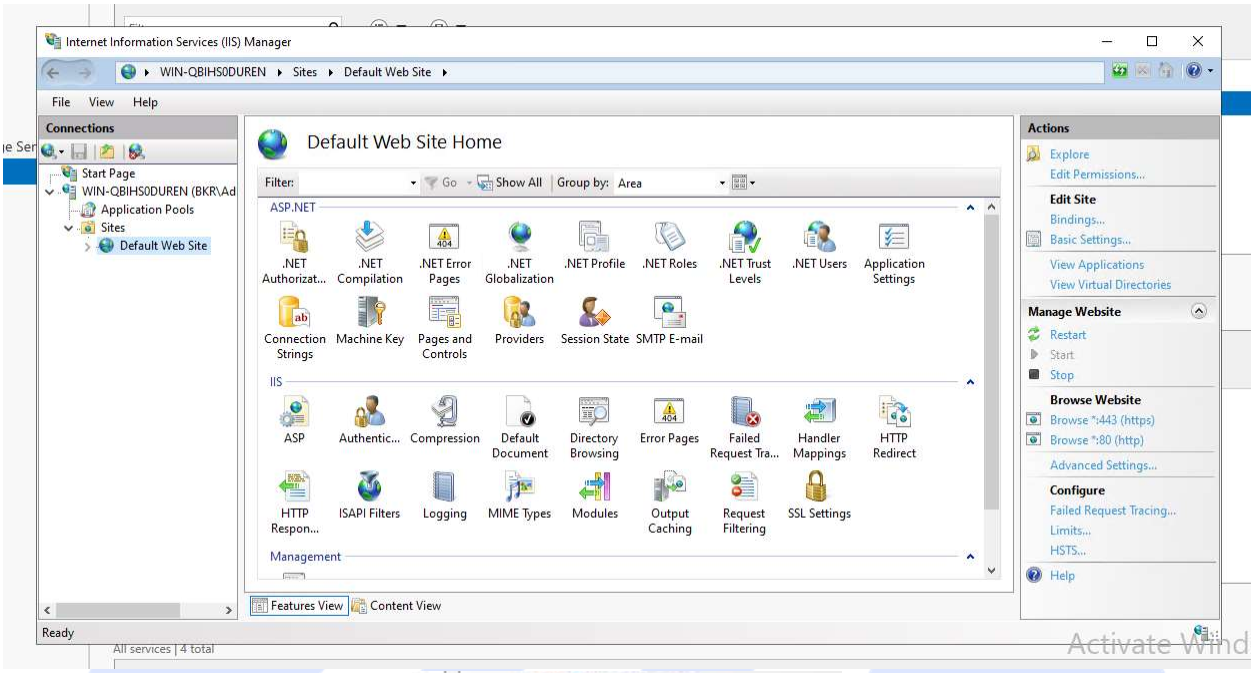

Internet Information Services (IIS) Manager
Start Page
File
View
Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
Microsoft
Internet Information Services 10
Application Server Manager
Recent connections
Name
Server
WIN-QBIHS0DUREN
localhost
Connection tasks
Connect to localhost
Connect to a server...
Connect to a site...
Connect to an application...
Online resources
IIS News and Information
IIS Downloads
IIS Forums
TechNet
MSDN
ASP.NET News
Microsoft Web Platform
IIS News
Enable IIS News
IIS News is disabled, click the Enable IIS News link to get the most recent online news.
Ready
All services | 4 total
Activate Win

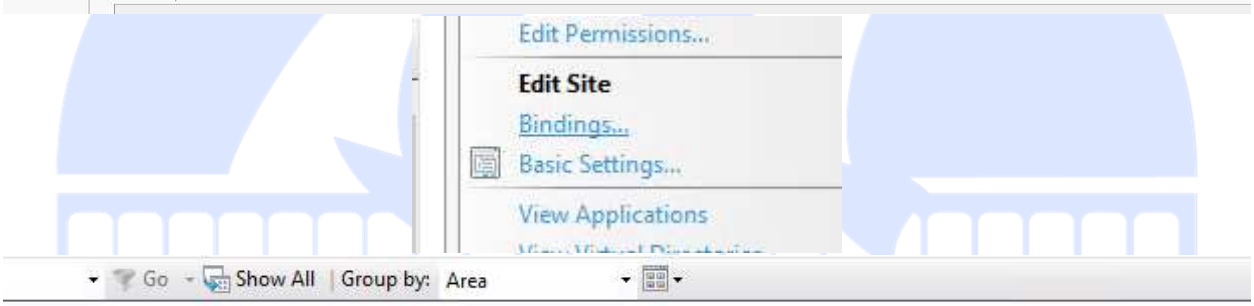

Internet Information Services (IIS) Manager
WIN-QBIHS0DUREN
File View Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
WIN-QBIHS0DUREN Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
ASP
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Features View
Content View
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Get New Web Platform Components
Help
Ready
All services | 4 total
Filter:
Go
Show All
Group by: Area
IIS
ASP
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Configurat... Editor
Feature Delegation
Shared Configurat...
Features View
Content View

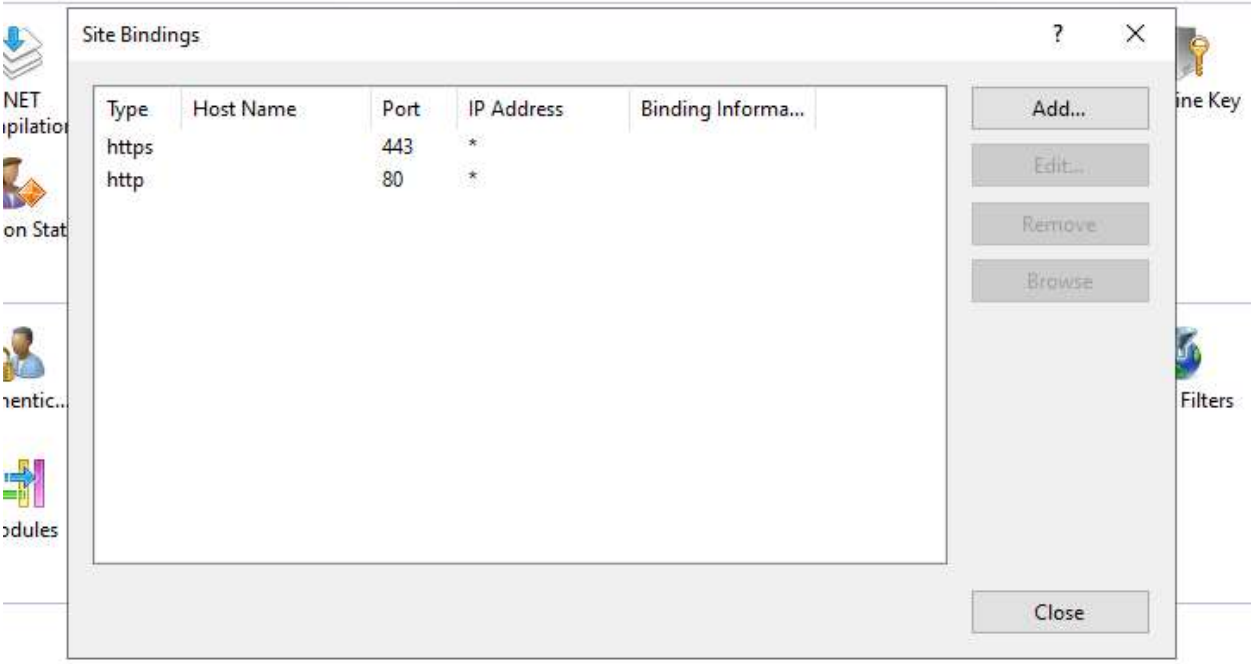

Internet Information Services (IIS) Manager
WIN-QBIHS0DUREN
File View Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by: No Grouping
Name
Issued To
Issued By
Expiration Date
Certificate Has
WIN-QBIHS0DUREN.bkr.corp
bkr-WIN-QBIHS0DUREN-CA
4/2/2025 7:52:51 A...
FC3E277D6520
bkr-WIN-QBIHS0DUREN-CA-1
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2029 8:59:40 A...
F9DBA9374F42
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 9:10:33 A...
69FFCDDE7FA5
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 9:10:58 A...
5F629920DE80
bkr-WIN-QBIHS0DUREN-CA
3/17/2025 6:26:13 ...
37266C052F2A
WIN-QBIHS0DUREN.bkr.corp
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 8:52:09 A...
30ADDAA7D8E
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
All services | 4 total
Activate Wi
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Remove
Enable Automatic Rebind of Renewed Certificate
Help

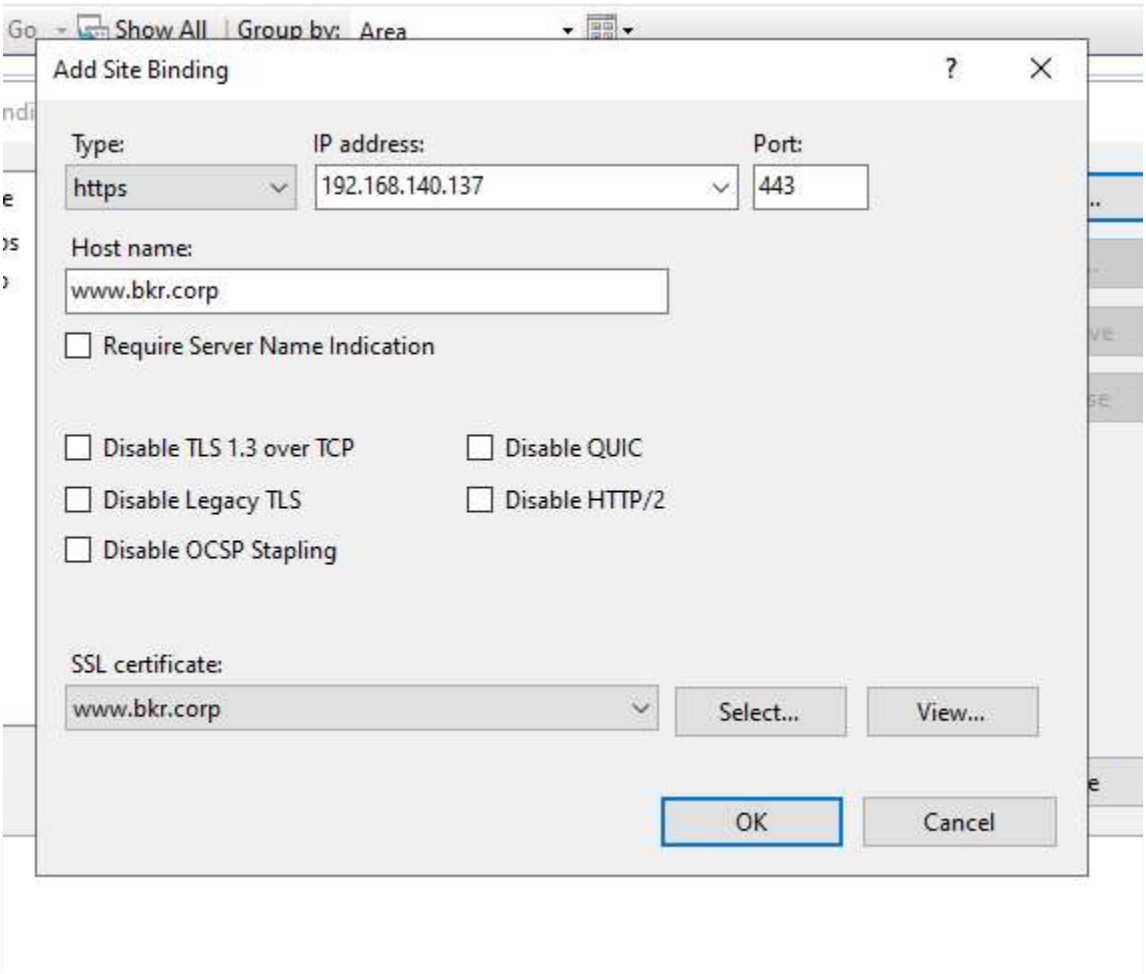

Internet Information Services (IIS) Manager
WIN-QBIHS0DUREN
File View Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
Application Pools
Sites
Create Certificate
Distinguished Name Properties
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.
Common name: www.bkr.corp
Organization: bkr
Organizational unit: fi
City/locality Algiers
State/province: dza
Country/region: DZ
Previous Next Finish Cancel
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View Content View
Ready
Create Certificate
Online Certification Authority
Specify the certification authority within your domain that will sign the certificate. A friendly nam and should be easy to remember.
Specify Online Certification Authority:
Example: CertificateAuthorityName\ServerName
Friendly name:
Previous Next Finish
Select Certification Authority
Select a certificate authority you want to use:
Certificate Authority
Computer
bkr-WIN-QBIHS0DUREN-CA-1
WIN-QBIHS0DUREN.bkr.corp
OK Cancel
Activate Windows
TASKS

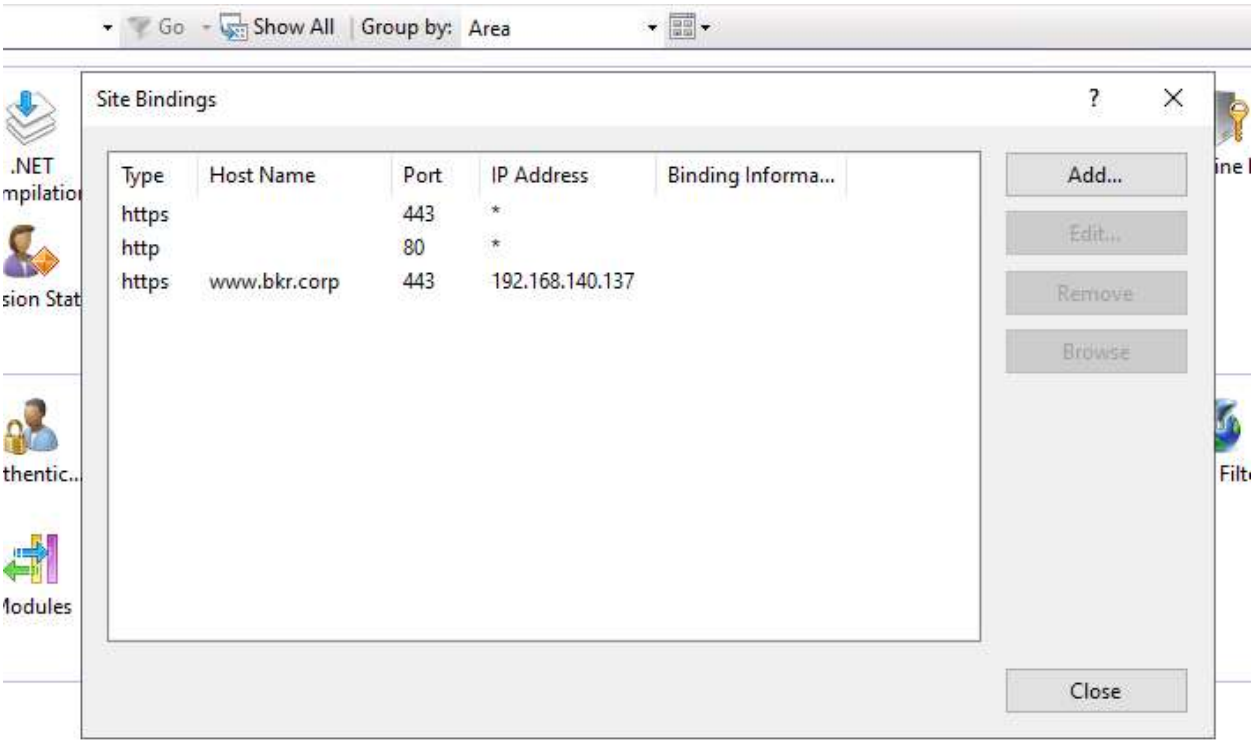

Create Certificate
Online Certification Authority
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.
Specify Online Certification Authority:
bkr-WIN-QBIHS0DUREN-CA-1\WIN-QBIHS0DUREN.bkr.corp
Select...
Example: CertificateAuthorityName\ServerName
Friendly name:
www.bkr.corp
Previous
Next
Finish
Cancel
Features View
Content View
Internet Information Services (IIS) Manager
WIN-QBIHS0DUREN
File View Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by: No Grouping
Name
Issued To
Issued By
Expiration Date
Certificate Has
WIN-QBIHS0DUREN.bkr.corp
bkr-WIN-QBIHS0DUREN-CA
4/2/2025 7:52:51 A...
FC3E277D6520
bkr-WIN-QBIHS0DUREN-CA-1
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2029 8:59:40 A...
F9DBA9374F42
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 9:10:33 A...
69FFCDDE7FA5
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 9:10:58 A...
5F629920DE80
bkr-WIN-QBIHS0DUREN-CA
3/17/2025 6:26:13 ...
37266C052F2A
WIN-QBIHS0DUREN.bkr.corp
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2025 8:52:09 A...
30ADDAA7D8E
www.bkr.corp
www.bkr.corp
bkr-WIN-QBIHS0DUREN-CA-1
4/2/2026 9:22:43 A...
7FFC228549
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
All services | 4 total
Activate Wind

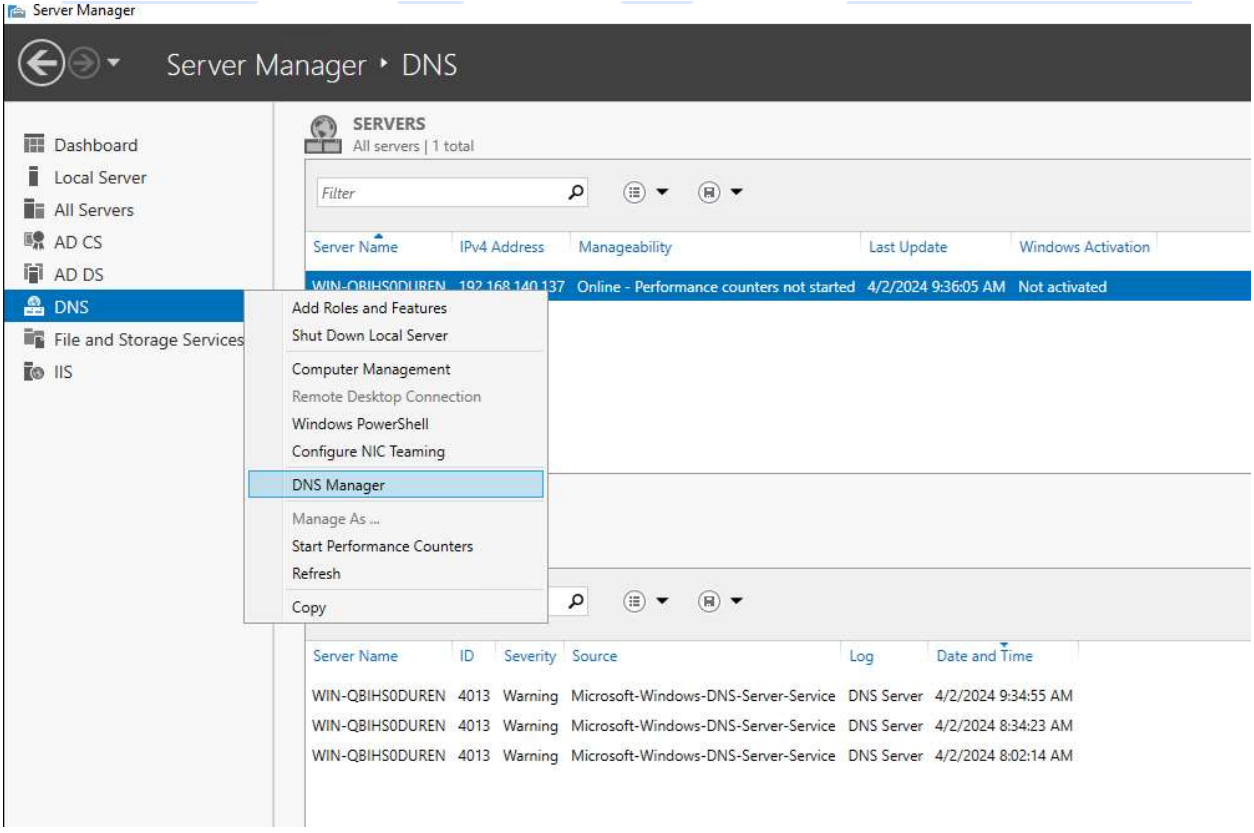

Internet Information Services (IIS) Manager
WIN-QBIHS0DUREN ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
WIN-QBIHS0DUREN (BKR\Ad
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
ASP
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:443 (https)
Browse *:80 (http)
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
HSTS...
Help
Ready
All services | 4 total
Activate Wind

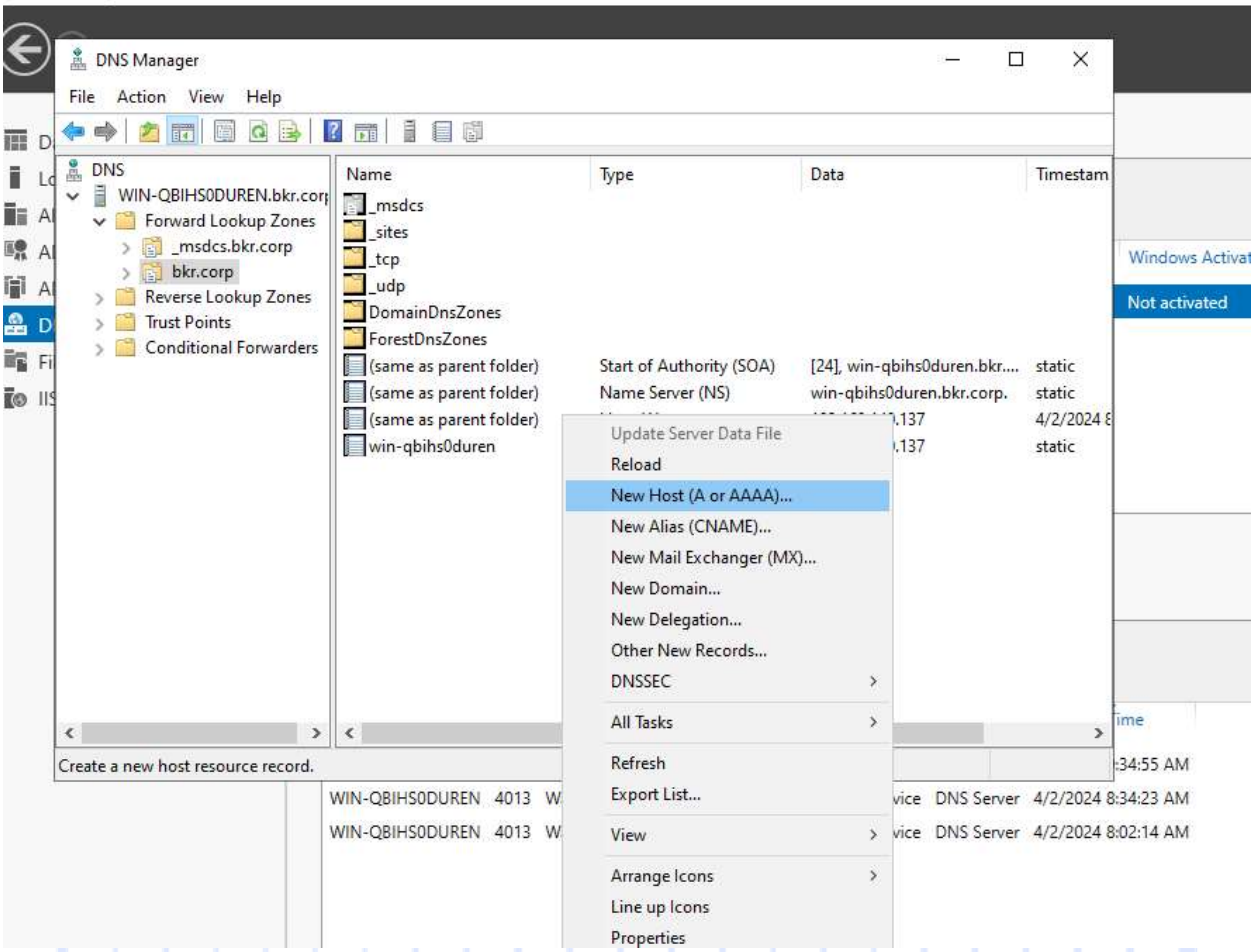

Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
Go
Show All
Group by: Area

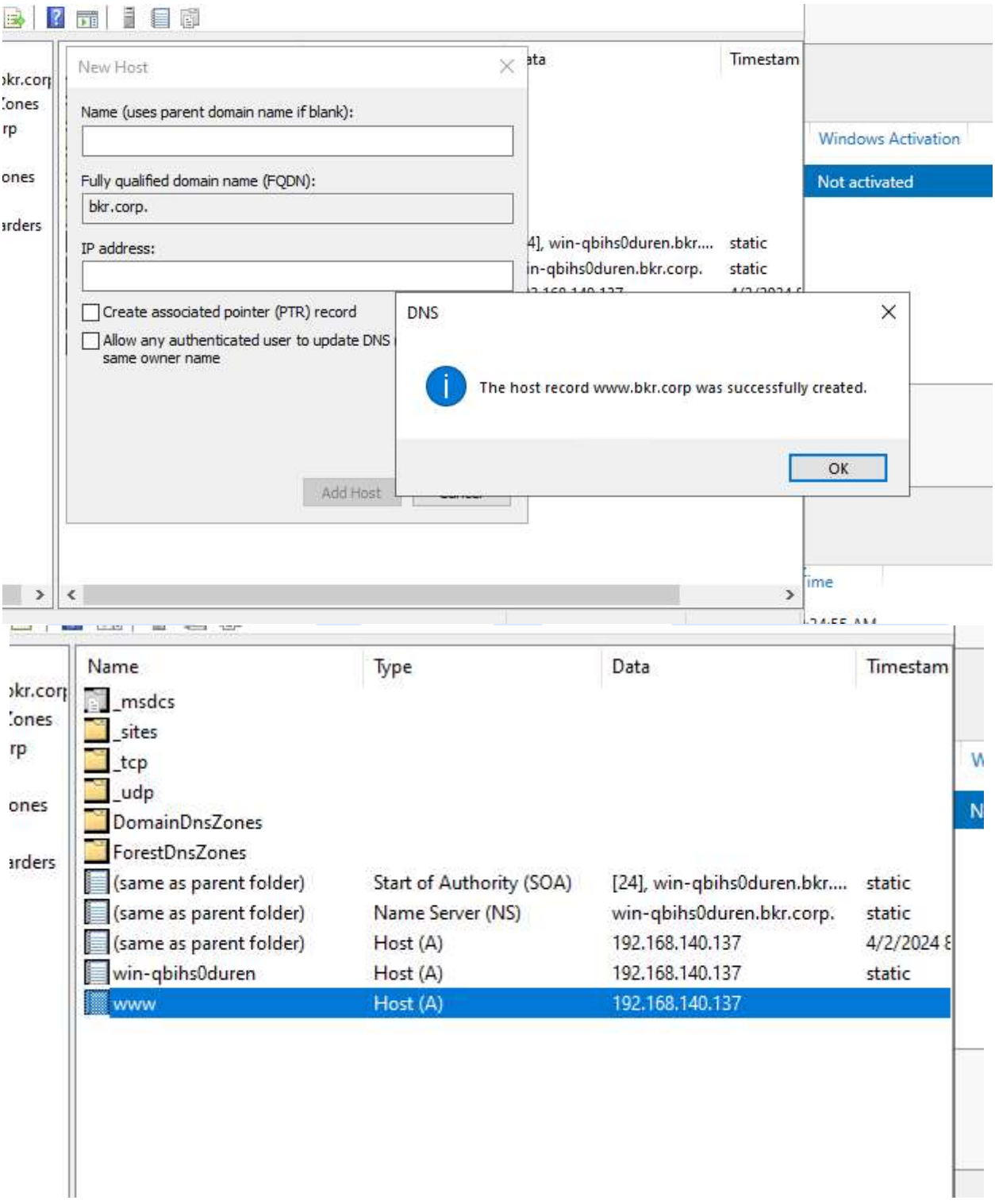

Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
https
443
*
http
80
*
Add...
Edit...
Remove
Browse
Close

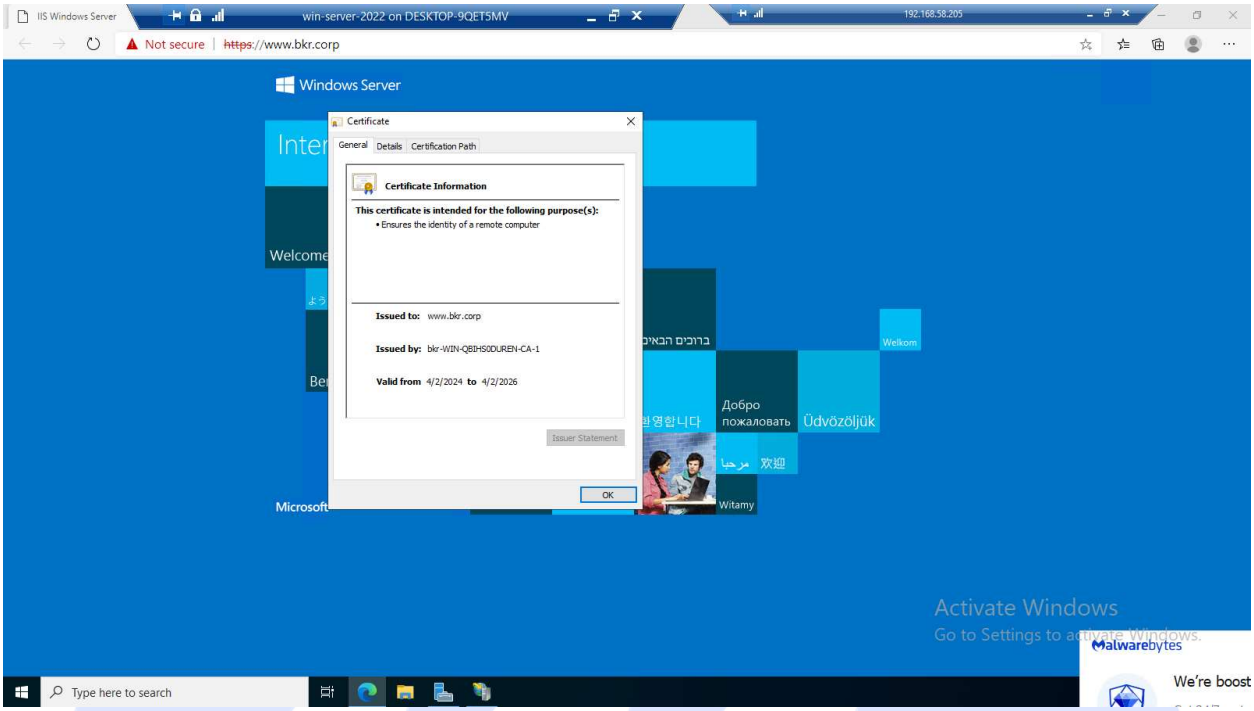



Go
Show All
Group by:
Area
Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
https
443
*
http
80
*
https
www.bkr.corp
443
192.168.140.137
Add...
Edit...
Remove
Browse
Close

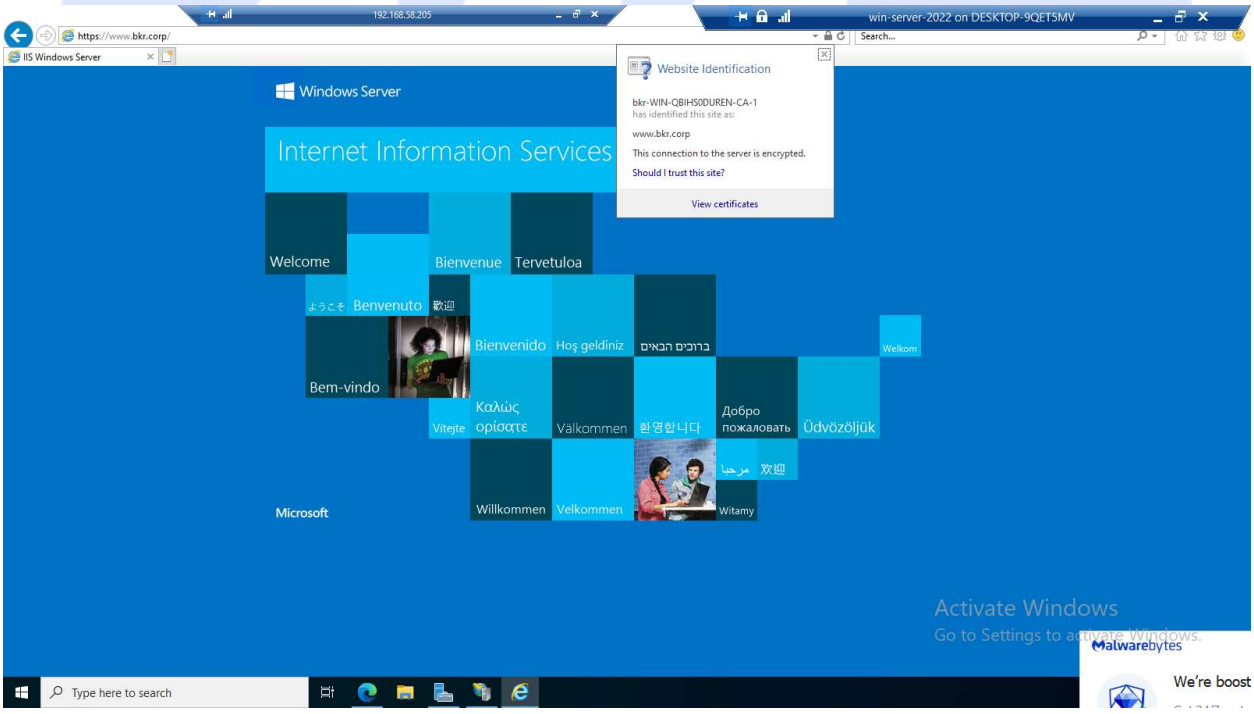

Server Manager
Server Manager ‣ DNS
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
SERVERS
All servers | 1 total
Filter
Server Name
IPv4 Address
Manageability
Last Update
Windows Activation
Online - Performance counters not started
4/2/2024 9:36:05 AM
Not activated
Add Roles and Features
Shut Down Local Server
Computer Management
Remote Desktop Connection
Windows PowerShell
Configure NIC Teaming
DNS Manager
Manage As ...
Start Performance Counters
Refresh
Copy
ID
Severity
Source
Log
Date and Time
WIN-QBIHS0DUREN 4013 Warning Microsoft-Windows-DNS-Server-Service DNS Server 4/2/2024 9:34:55 AM
WIN-QBIHS0DUREN 4013 Warning Microsoft-Windows-DNS-Server-Service DNS Server 4/2/2024 8:34:23 AM
WIN-QBIHS0DUREN 4013 Warning Microsoft-Windows-DNS-Server-Service DNS Server 4/2/2024 8:02:14 AM




New Host
Name (uses parent domain name if blank):
Fully qualified domain name (FQDN):
bkr.corp.
IP address:
Create associated pointer (PTR) record
Allow any authenticated user to update DNS
same owner name
Add Host
DNS
The host record www.bkr.corp was successfully created.
OK
Timestam
Windows Activation
Not activated
4], win-qbihs0duren.bkr.... static
in-qbihs0duren.bkr.corp. static
Name
Type
Data
Timestam
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(same as parent folder) Start of Authority (SOA) [24], win-qbihs0duren.bkr.... static
(same as parent folder) Name Server (NS) win-qbihs0duren.bkr.corp. static
(same as parent folder) Host (A) 192.168.140.137 4/2/2024
win-qbihs0duren Host (A) 192.168.140.137 static
www Host (A) 192.168.140.137



Or using internet explorer:



Conclusion:

In conclusion, the configuration process involved several key steps:

Creation of a Domain and Transformation into a Domain Controller: This step involved setting up a domain and promoting a machine to act as a domain controller. It ensured centralized management of resources and security policies within the network.

Adding the Client to the Domain: The client machine was joined to the domain to allow access to domain resources and services. This step facilitated user authentication and centralized administration.

Installation of the Web Server (IIS): IIS was installed on the client machine to host web pages. While initially using the HTTP protocol, the subsequent configuration for HTTPS was planned to ensure secure communication.

Installation of Active Directory Certificate Services (AD CS): AD CS was installed on the server to manage digital certificates. This ensured secure communication via SSL/TLS by providing cryptographic services, including issuing and managing certificates.

Configuration of Active Directory Certificate Services: During the configuration, the selected options aligned with security best practices, such as choosing SHA512 as the hash algorithm and selecting appropriate role services.

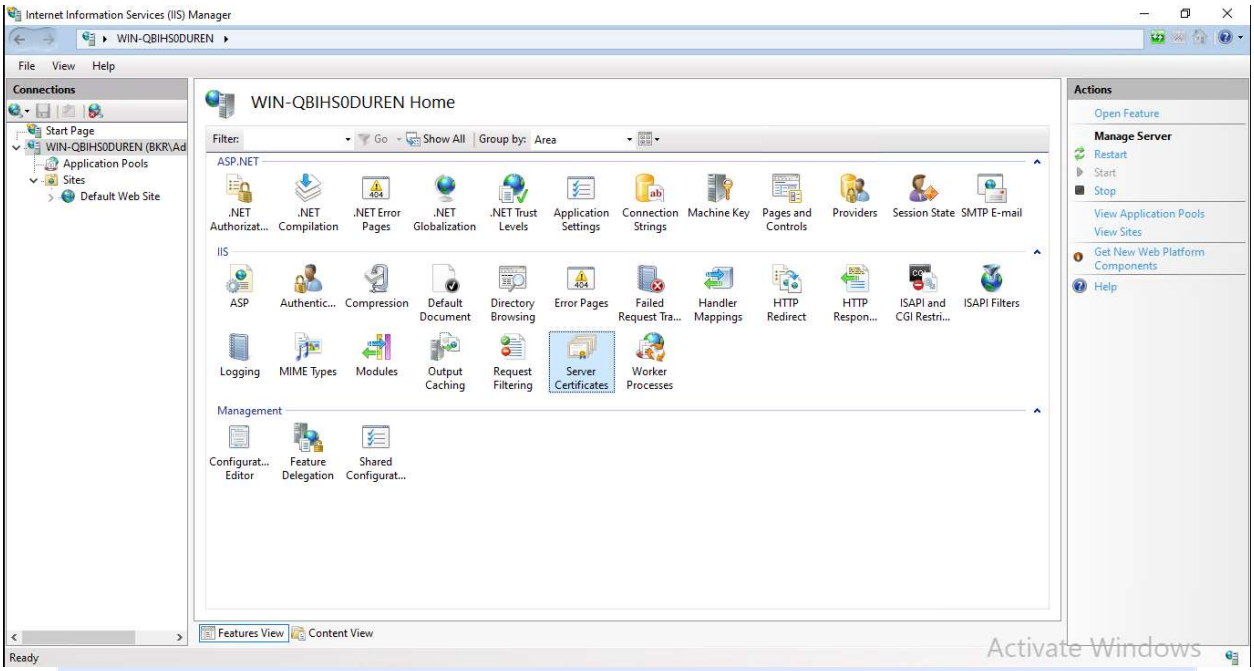
Verification of Web Server Functionality: After configuring IIS, the web server's functionality was verified by accessing hosted web pages, though initially over HTTP.

Viewing Certificate Properties: Properties of certificates were inspected to ensure correct configurations, including details like version, subject, issuer, validity period, and cryptographic properties.

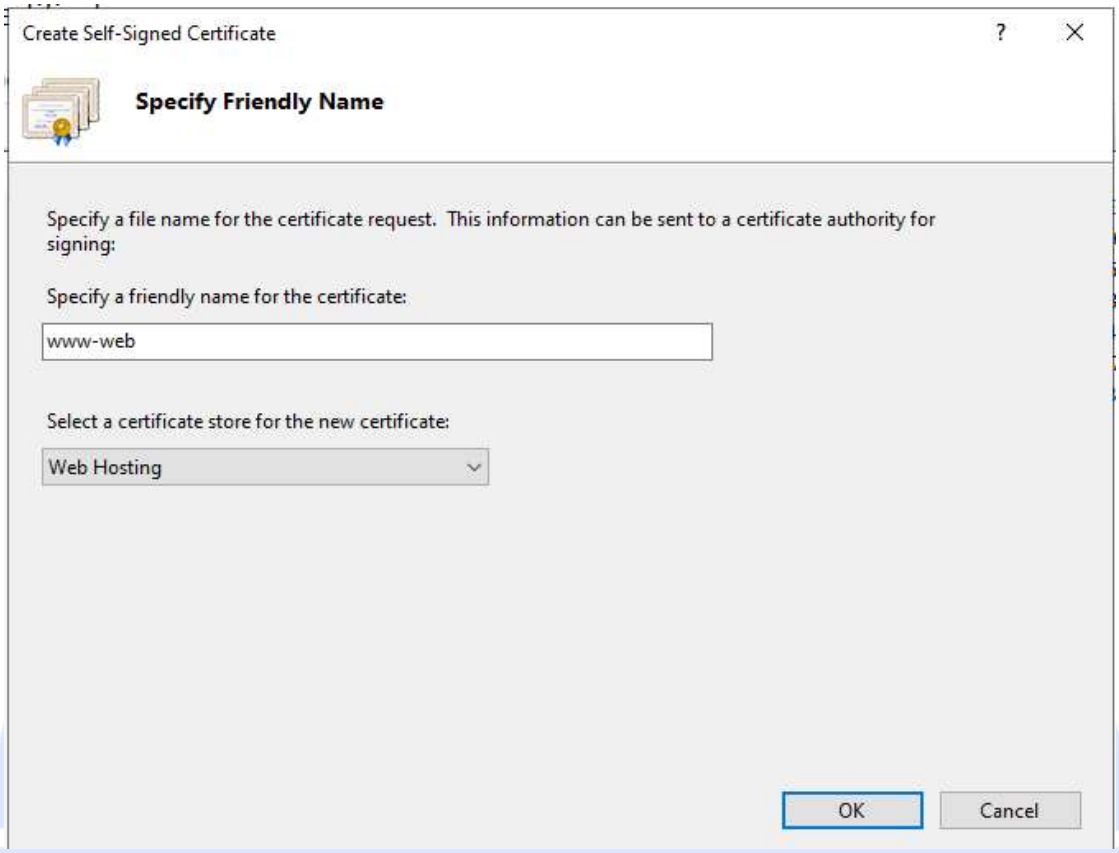
Utilizing the Certificate: Lastly, the created and exported certificate was utilized by adding it to the webpage, thus ensuring secure communication via HTTPS.

Installation of an SSL/TLS certificate on the IIS web server (alternative/short version):

After installing the IIS web server, go to the Internet Information Services (IIS) Manager and Open it.

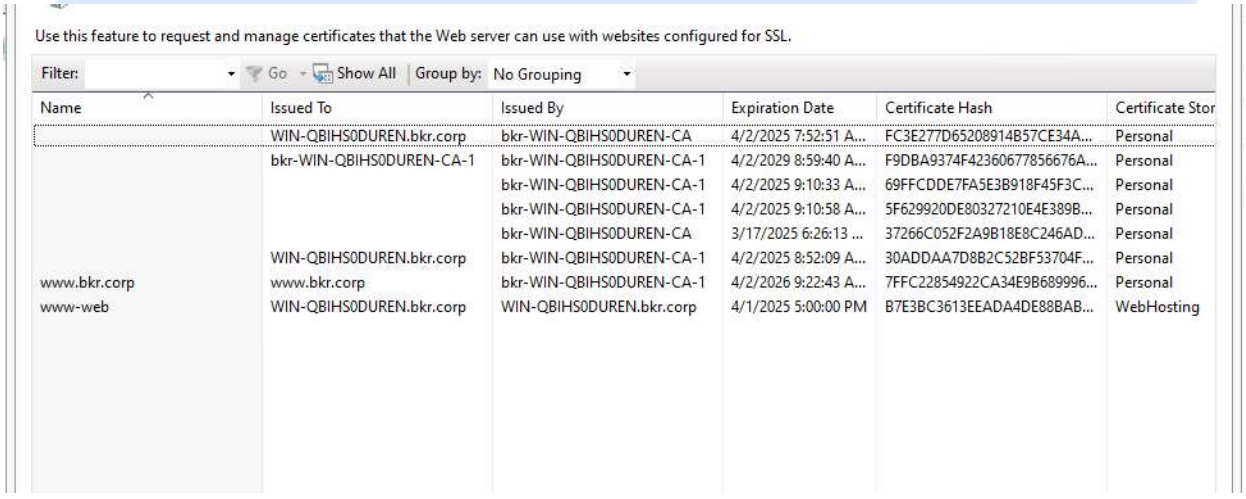


Click on "Server Certificates" and then Under the "Actions" panel on the right-hand side, choose "Create Self-Signed Certificate".

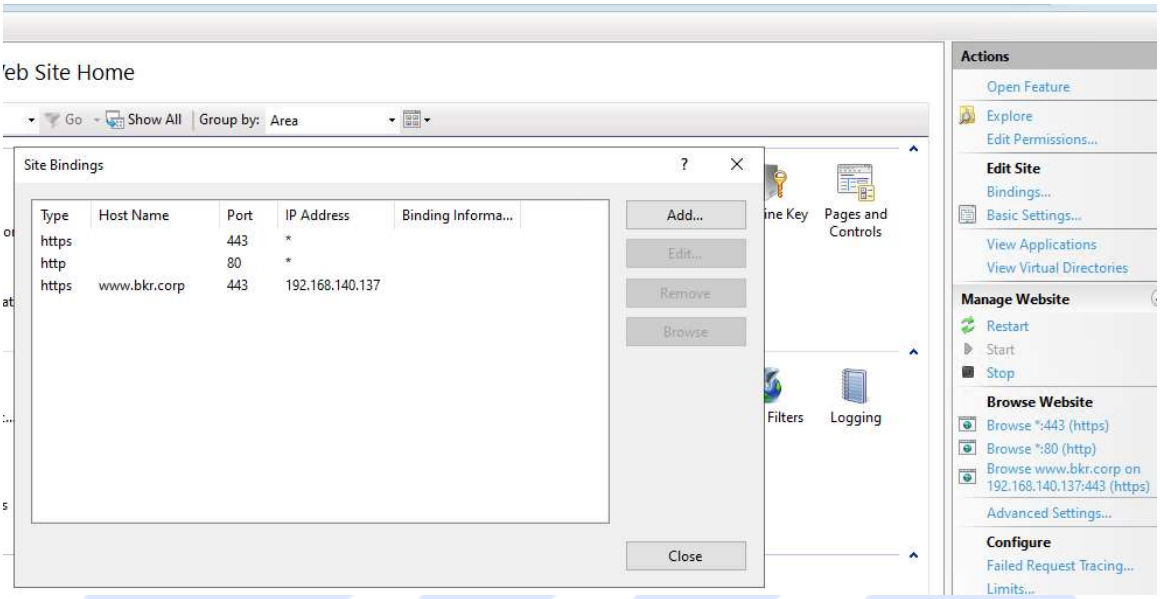


Enter a friendly name and select a certificate store, Provide a user-friendly name for the certificate

From the drop-down menu, select "Web Hosting" as the certificate store, then click on "OK"



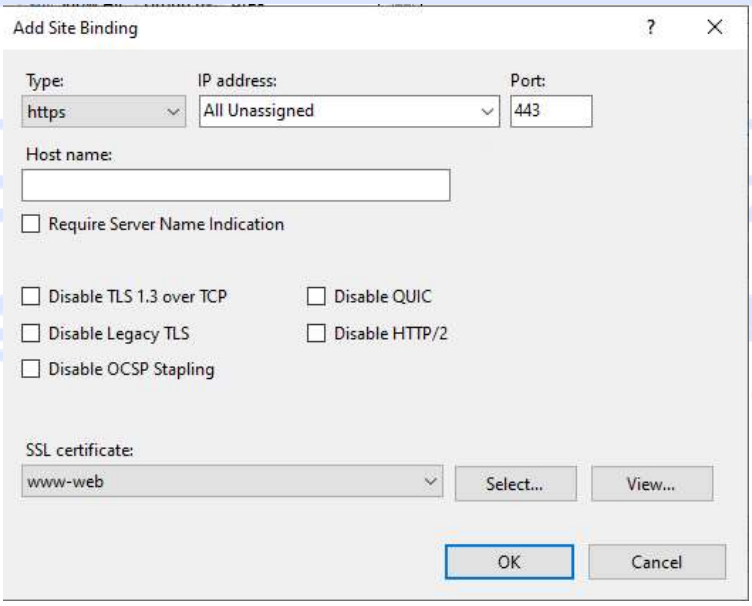
Verify that the certificate has been added successfully



Navigate to the "Bindings" option in the Actions pane on the right, click on "Add" in the 'site bindings' wizard to create a new binding.

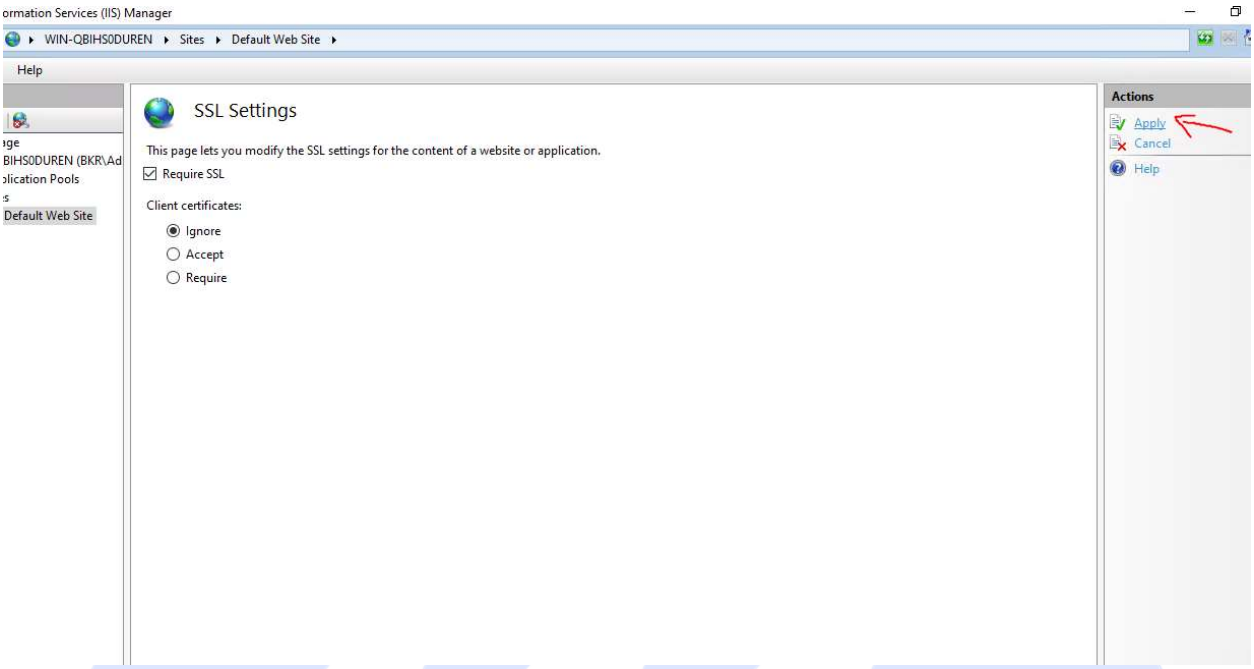
Specify the binding type HTTPS.

Choose the IP address and port for the binding, select the recently created SSL certificate from the drop-down list.



Save the changes by clicking "OK"

Enable "Require SSL" by checking the box and then save the changes by clicking "Apply" in the Actions pane on the right.



Enable "Require SSL" by checking the box.

Save the changes by clicking "Apply" in the Actions pane on the right.