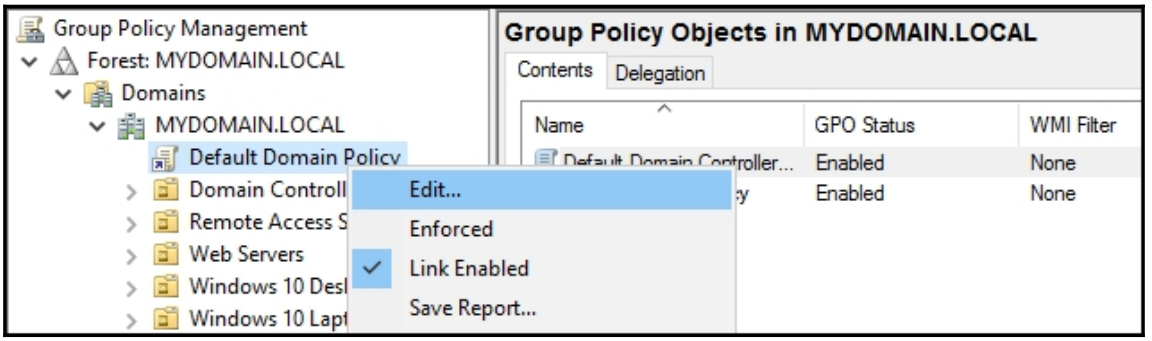
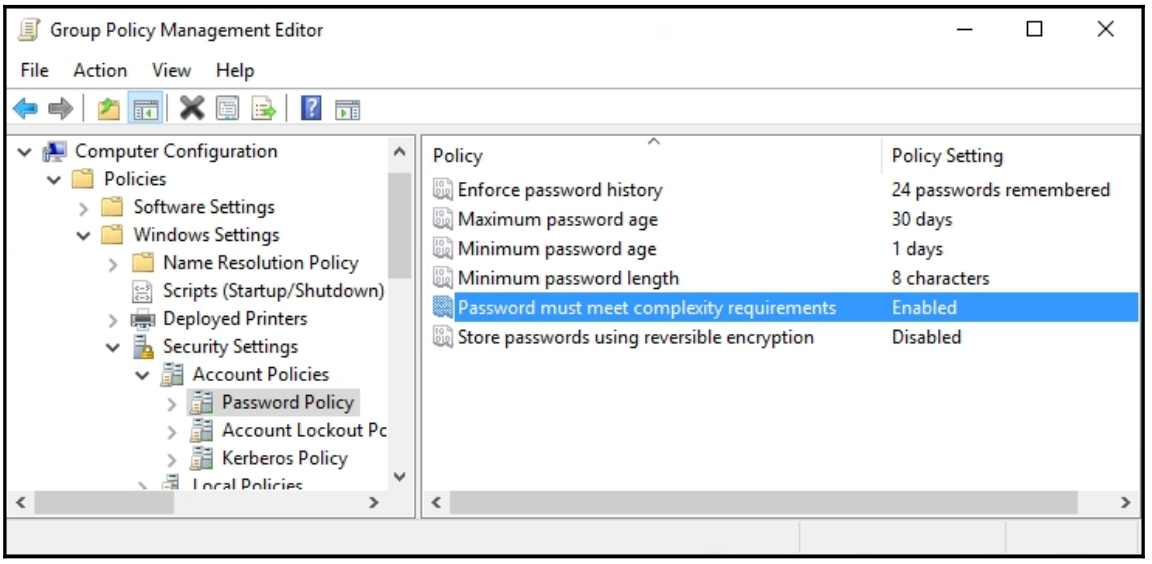
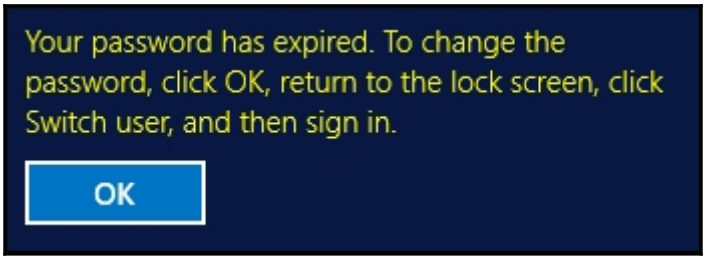
Chapter 1: Security and Networking







Does this rule apply to all local ports or specific local ports?

- ○ **All local ports**
- ◉ **Specific local ports:** 445, 3389

Example: 80, 443, 5000-5010

Inbound Rules

Name

- Block ICMPv4
- Block File and RDP Access
- AllJoyn Router (TCP-In)
- AllJoyn Router (UDP-In)
- BranchCache Content Retriev
- BranchCache Hosted Cache S

Block ICMPv4 Properties

General | Programs and Services | Remote Computers
Protocols and Ports | Scope | Advanced | Local Principals | Remote Users

Protocols and ports

Protocol type: ICMPv4

Protocol number: 1

- Wds
- WinStations
  - Console
  - RDP-Tcp

PdName	REG_SZ	tcp
PdName1	REG_SZ	tssecsrv
PortNumber	REG_DWORD	0x000012d6 (4822)
SecurityLayer	REG_DWORD	0x00000002 (2)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

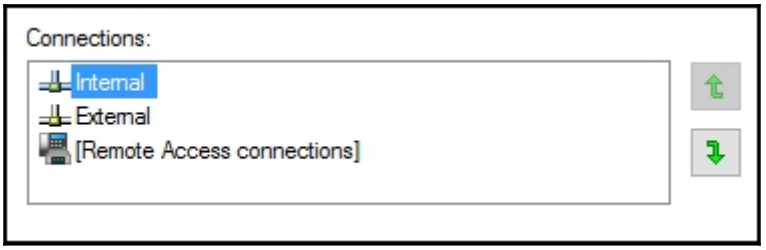
Remote Desktop Connection

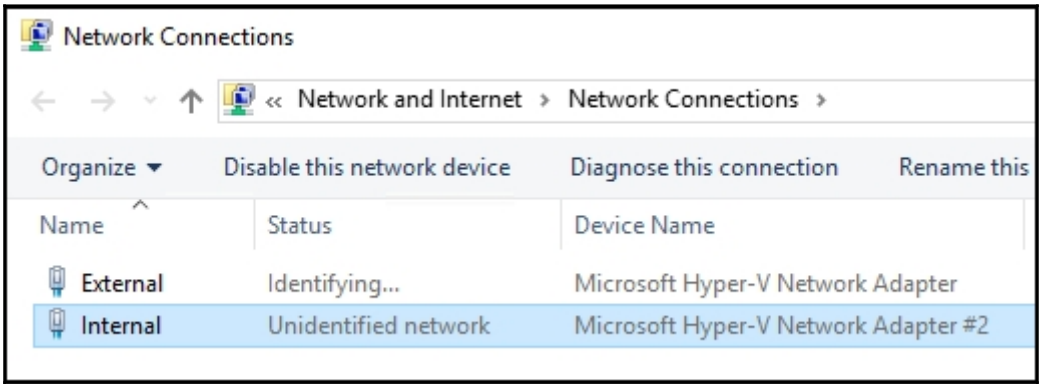
Computer: WEB1:4822

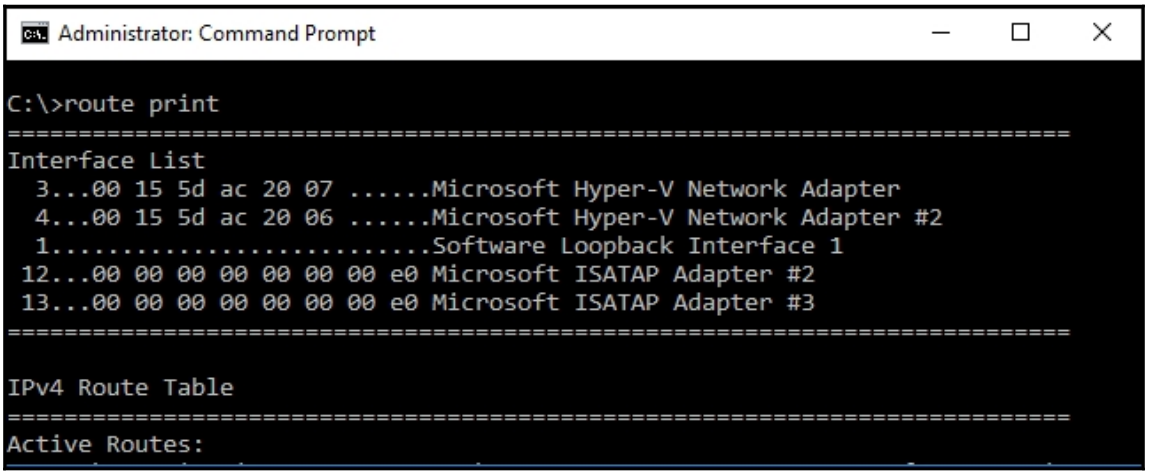
User name: None specified

You will be asked for credentials when you connect.

Show Options | Connect | Help


Connections:
Internal
External
[Remote Access connections]


Network Connections
« Network and Internet › Network Connections ›
Organize
Disable this network device
Diagnose this connection
Rename this
Name
Status
Device Name
External
Identifying...
Microsoft Hyper-V Network Adapter
Internal
Unidentified network
Microsoft Hyper-V Network Adapter #2


Administrator: Command Prompt
C:\>route print
===
Interface List
3...00 15 5d ac 20 07 ......Microsoft Hyper-V Network Adapter
4...00 15 5d ac 20 06 ......Microsoft Hyper-V Network Adapter #2
1...........................Software Loopback Interface 1
12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===
IPv4 Route Table
===
Active Routes:

Administrator: Command Prompt

```
C:\>route add -p 10.0.1.0 mask 255.255.255.0 10.0.0.254 if 4
 OK!

C:\>
```

Administrator: Command Prompt

```
Pinging web1.MYDOMAIN.LOCAL [10.0.0.85] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.85:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Administrator: Command Prompt

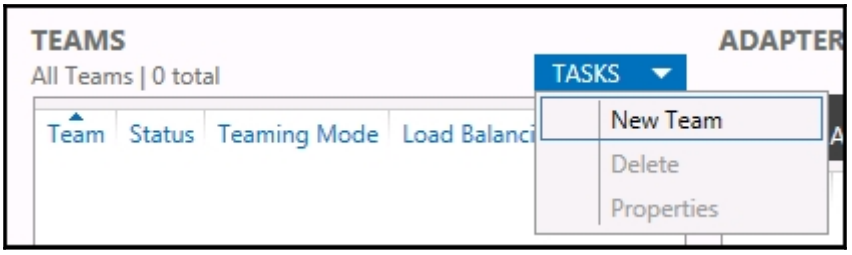
```
C:\>telnet web1 80
```

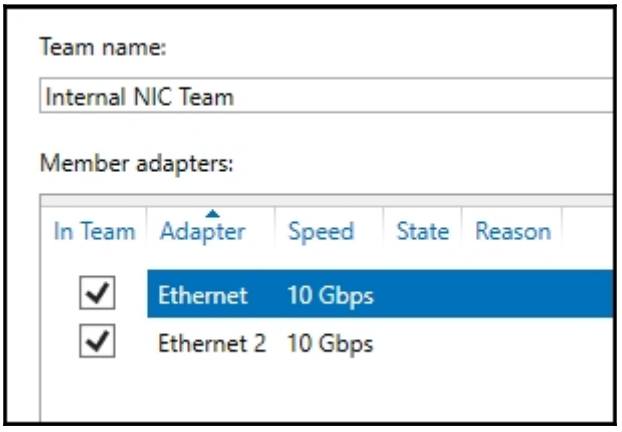
Telnet web1

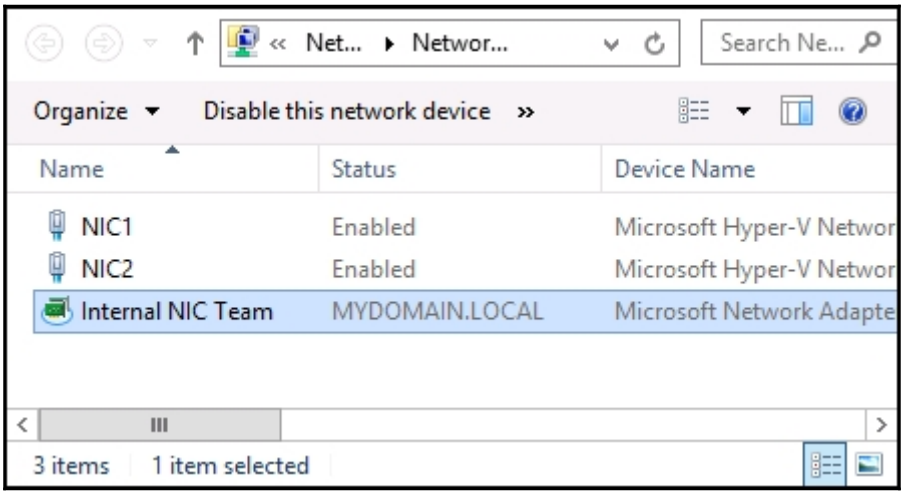
Administrator: Command Prompt

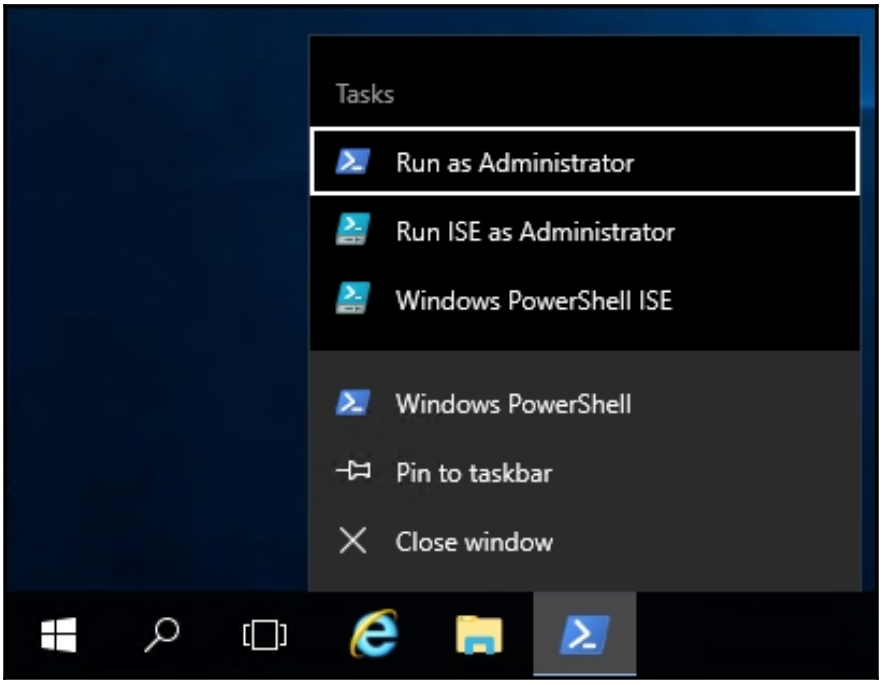
```
C:\>pathping dc1

Tracing route to DC1.MYDOMAIN.LOCAL [10.0.0.1]
over a maximum of 30 hops:
  0  WEB1.MYDOMAIN.LOCAL [10.0.0.85]
  1  DC1 [10.0.0.1]

Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           WEB1.MYDOMAIN.LOCAL [10.0.0.85]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  DC1 [10.0.0.1]

Trace complete.

C:\>
```

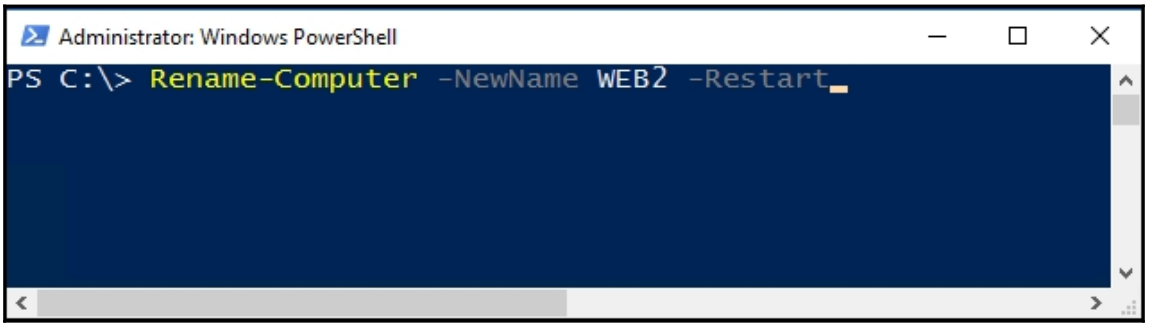
Windows Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
NIC1	IPv4 address assigned by DHCP, IPv6 enabled
NIC2	IPv4 address assigned by DHCP, IPv6 enabled

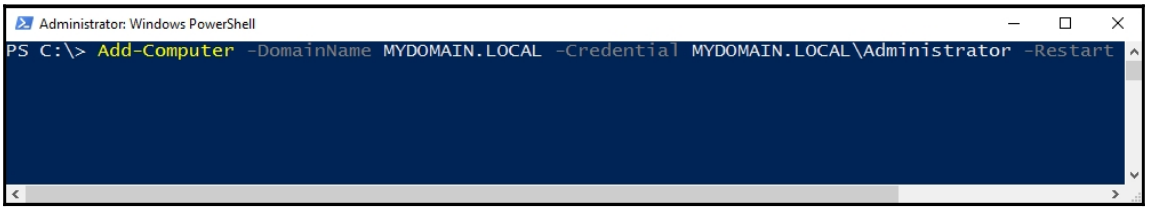

TEAMS
All Teams | 0 total
ADAPTER
TASKS
Team
Status
Teaming Mode
Load Balanci
New Team
Delete
Properties

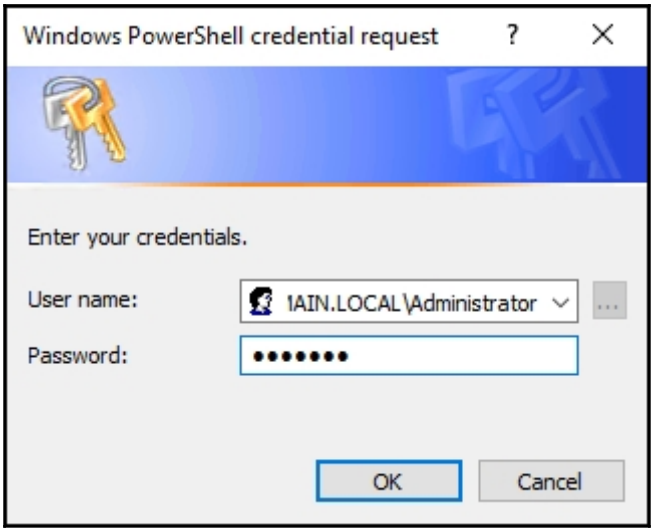

Team name:
Internal NIC Team
Member adapters:
In Team
Adapter
Speed
State
Reason
Ethernet
10 Gbps
Ethernet 2
10 Gbps

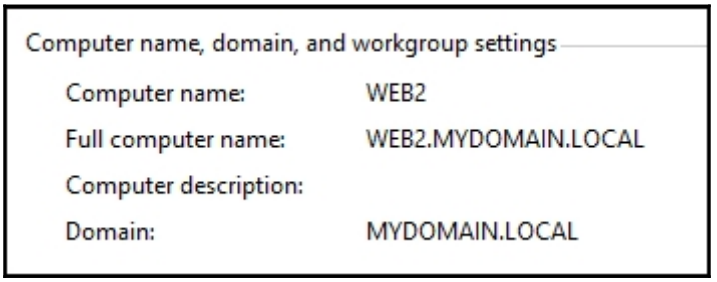

Net...
Networ...
Search Ne...
Organize
Disable this network device
Name
Status
Device Name
NIC1
Enabled
Microsoft Hyper-V Networ
NIC2
Enabled
Microsoft Hyper-V Networ
Internal NIC Team
MYDOMAIN.LOCAL
Microsoft Network Adapte
3 items
1 item selected

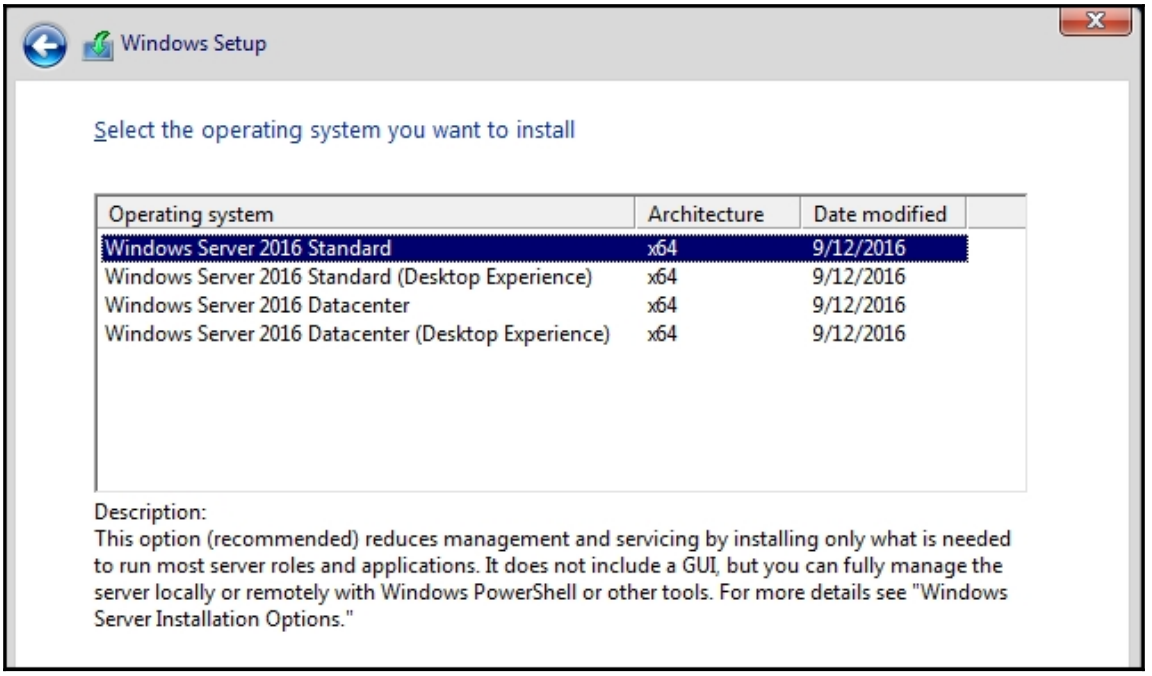

Tasks
Run as Administrator
Run ISE as Administrator
Windows PowerShell ISE
Windows PowerShell
Pin to taskbar
Close window

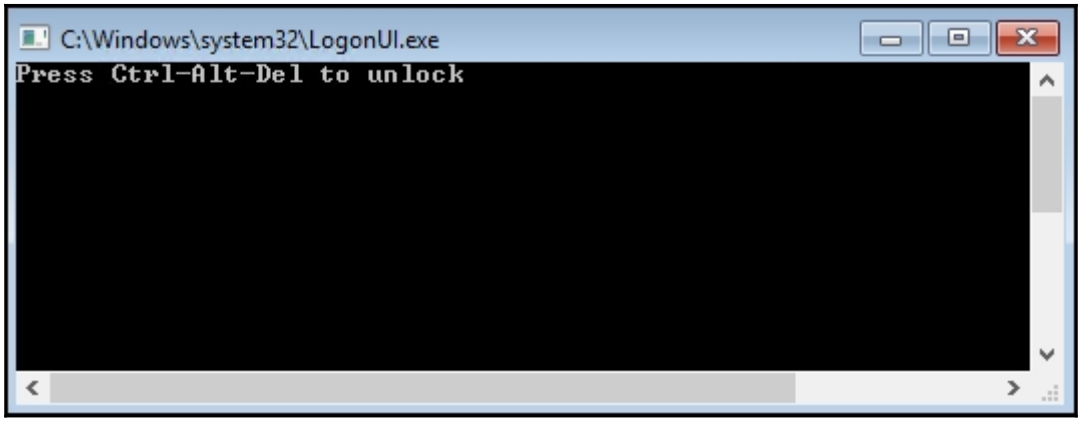

Administrator: Windows PowerShell
PS C:\> Rename-Computer -NewName WEB2 -Restart


Administrator: Windows PowerShell
PS C:\> Add-Computer -DomainName MYDOMAIN.LOCAL -Credential MYDOMAIN.LOCAL\Administrator -Restart


Windows PowerShell credential request
Enter your credentials.
User name:
1AIN.LOCAL\Administrator
Password:
OK
Cancel


Computer name, domain, and workgroup settings
Computer name: WEB2
Full computer name: WEB2.MYDOMAIN.LOCAL
Computer description:
Domain: MYDOMAIN.LOCAL


Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2016 Standard
x64
9/12/2016
Windows Server 2016 Standard (Desktop Experience)
x64
9/12/2016
Windows Server 2016 Datacenter
x64
9/12/2016
Windows Server 2016 Datacenter (Desktop Experience)
x64
9/12/2016
Description:
This option (recommended) reduces management and servicing by installing only what is needed to run most server roles and applications. It does not include a GUI, but you can fully manage the server locally or remotely with Windows PowerShell or other tools. For more details see "Windows Server Installation Options."


C:\Windows\system32\LogonUI.exe
Press Ctrl-Alt-Del to unlock

Administrator: C:\Windows\system32\cmd.exe - powershell

```
C:\>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\> Rename-Computer CORE1
```

Administrator: C:\Windows\system32\cmd.exe - powershell

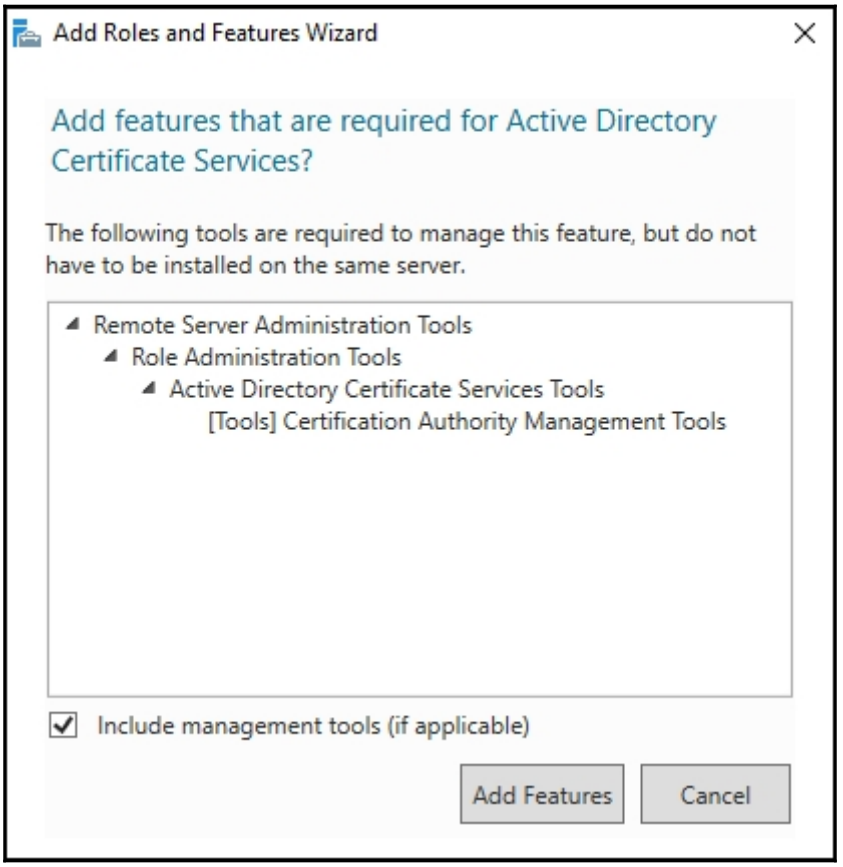
```
PS C:\> notepad.exe
PS C:\>
```

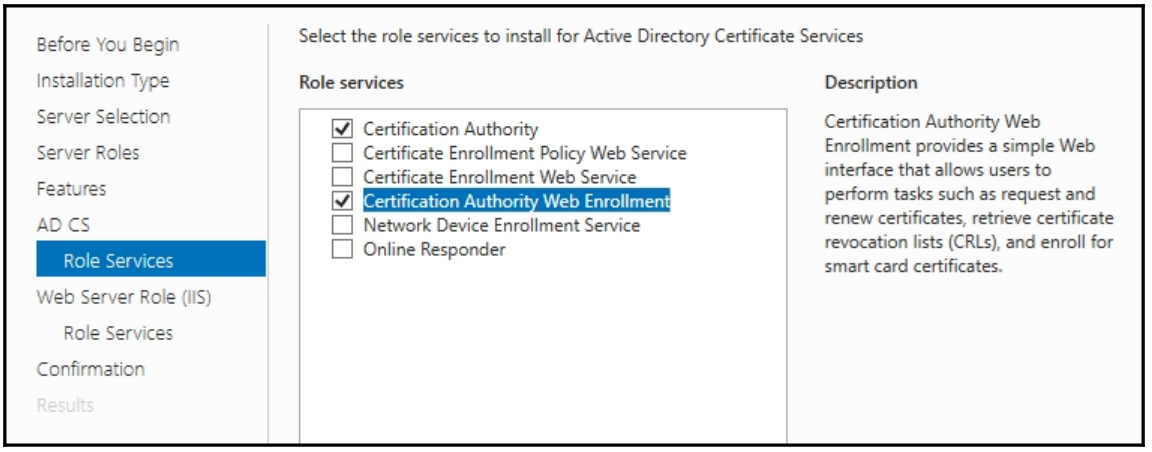
Untitled - Notepad

File Edit Format View Help

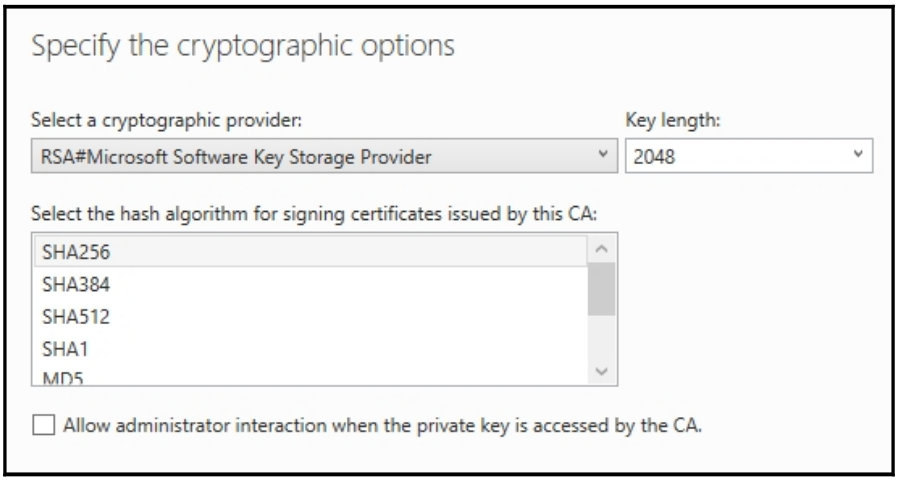
Testing Notepad inside Server Core

Chapter 2: Working with Certificates




Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Active Directory Certificate Services
Role services
Certification Authority
Certificate Enrollment Policy Web Service
Certificate Enrollment Web Service
Certification Authority Web Enrollment
Network Device Enrollment Service
Online Responder
Description
Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.


Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
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


Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.

Common name for this CA:

MyDomain-CertServer

Distinguished name suffix:

DC=MYDOMAIN,DC=LOCAL

Preview of distinguished name:

CN=MyDomain-CertServer,DC=MYDOMAIN,DC=LOCAL

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

Role services

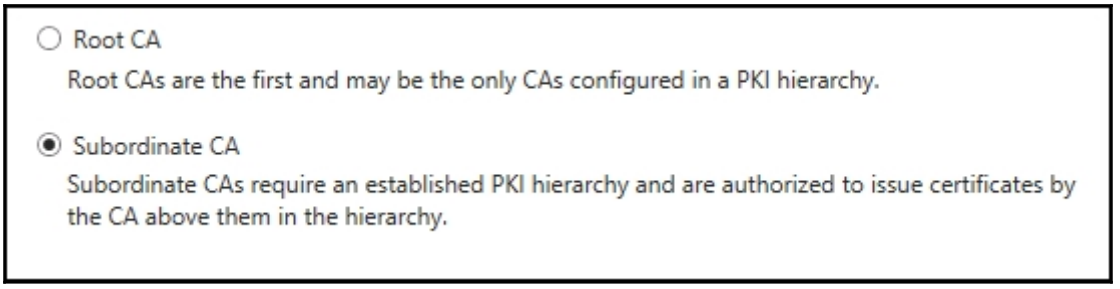
- [x] Certification Authority
- [ ] Certificate Enrollment Policy Web Service
- [ ] Certificate Enrollment Web Service
- [ ] Certification Authority Web Enrollment
- [ ] Network Device Enrollment Service
- [ ] Online Responder

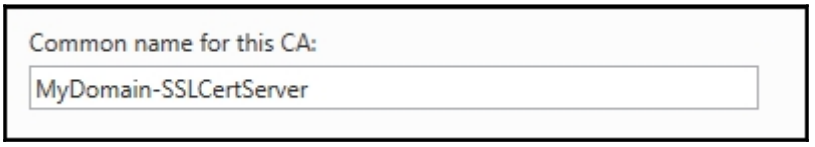
(●) Enterprise CA

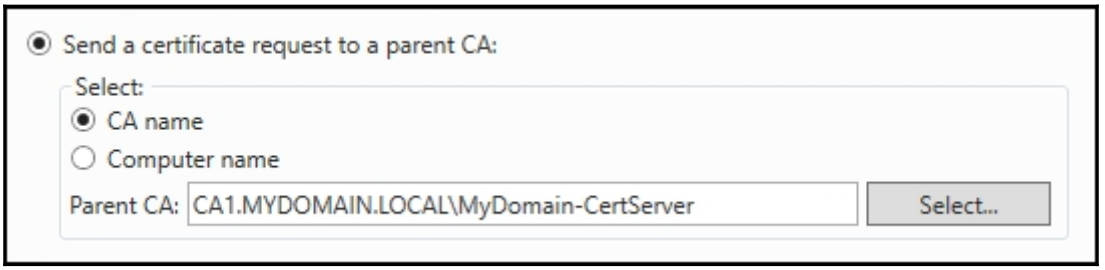
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

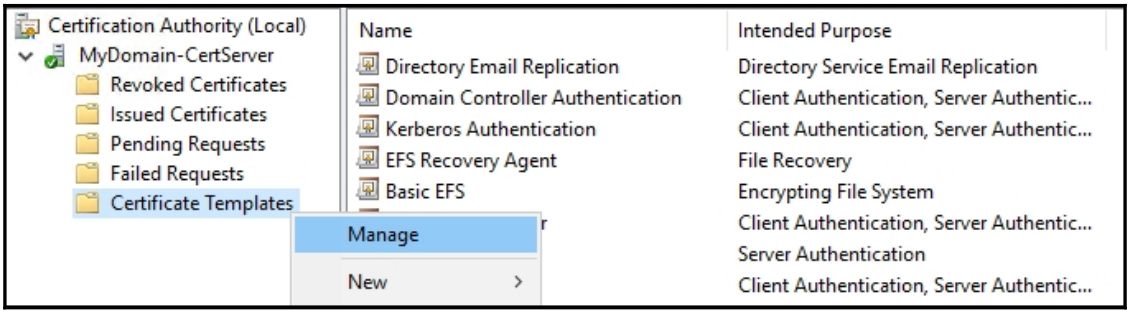
( ) Standalone CA

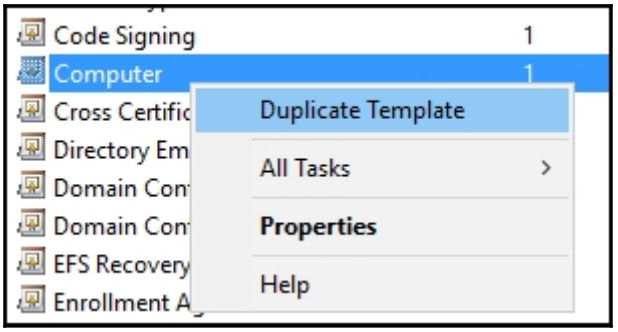
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

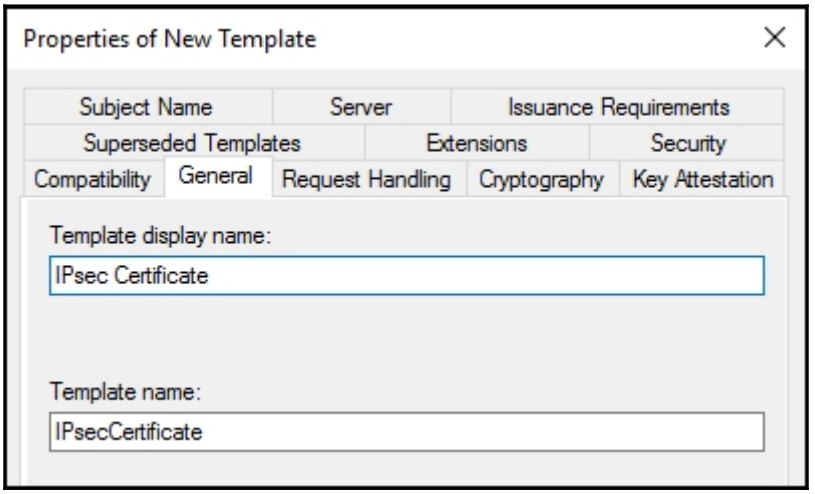

Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

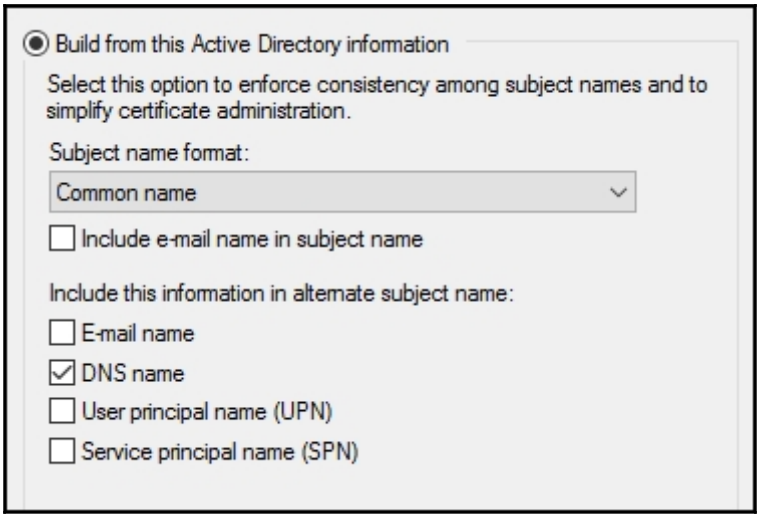

Common name for this CA:
MyDomain-SSLCertServer

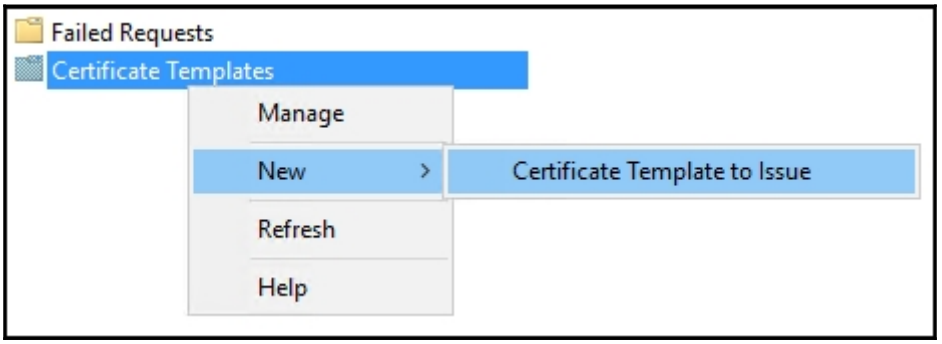

Send a certificate request to a parent CA:
Select:
CA name
Computer name
Parent CA:
CA1.MYDOMAIN.LOCAL\MyDomain-CertServer
Select...

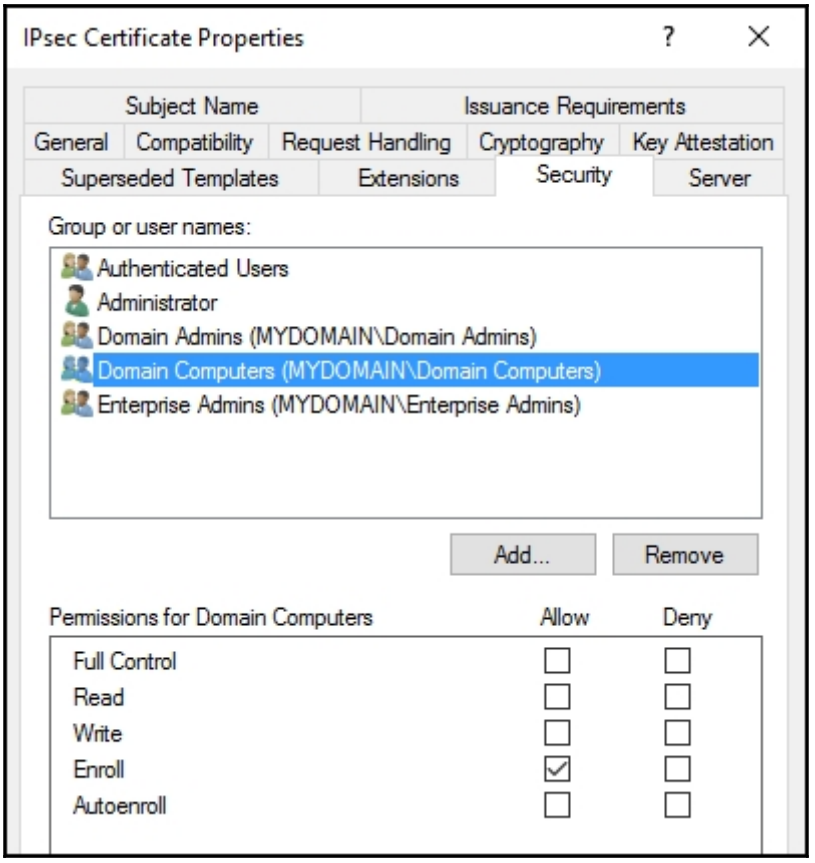

Certification Authority (Local)
MyDomain-CertServer
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
Name
Directory Email Replication
Domain Controller Authentication
Kerberos Authentication
EFS Recovery Agent
Basic EFS
Intended Purpose
Directory Service Email Replication
Client Authentication, Server Authentic...
Client Authentication, Server Authentic...
File Recovery
Encrypting File System
Client Authentication, Server Authentic...
Server Authentication
Client Authentication, Server Authentic...

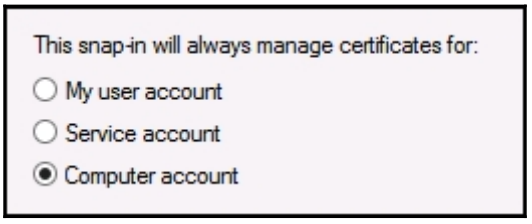

Code Signing 1
Computer 1
Cross Certific
Directory Em
Domain Con
Domain Con
EFS Recovery
Enrollment A
Duplicate Template
All Tasks
Properties
Help

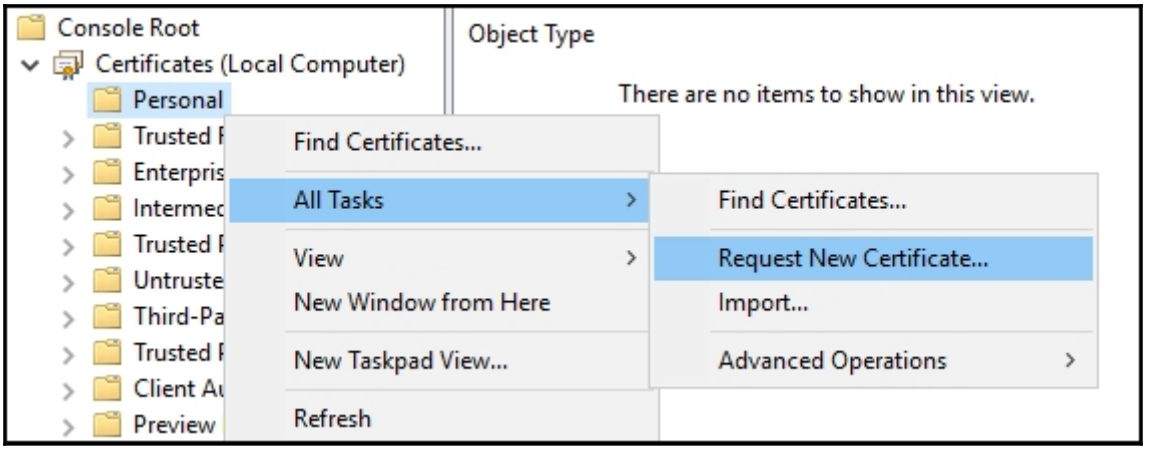

Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
IPsec Certificate
Template name:
IPsecCertificate

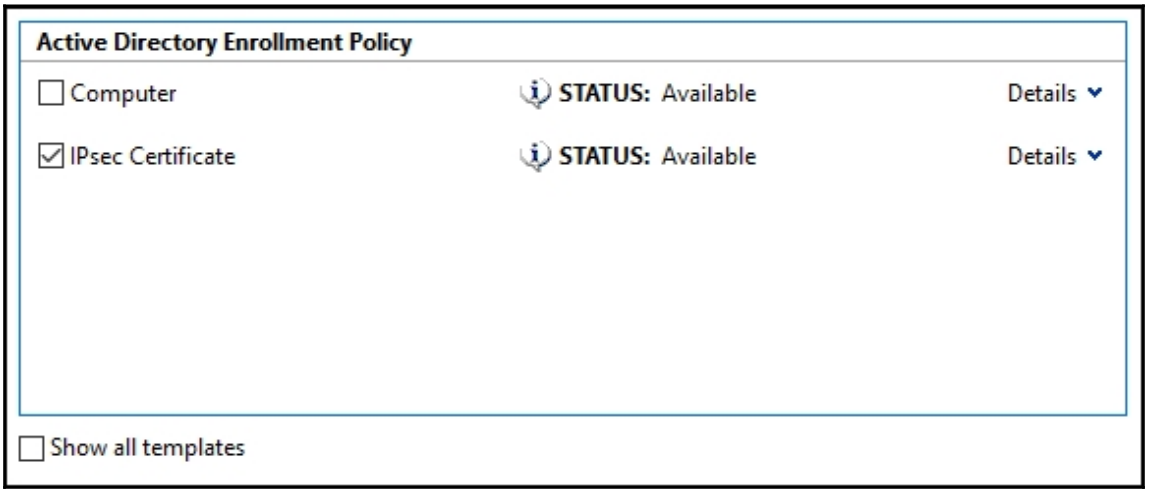

Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.
Subject name format:
Common name
Include e-mail name in subject name
Include this information in alternate subject name:
E-mail name
DNS name
User principal name (UPN)
Service principal name (SPN)

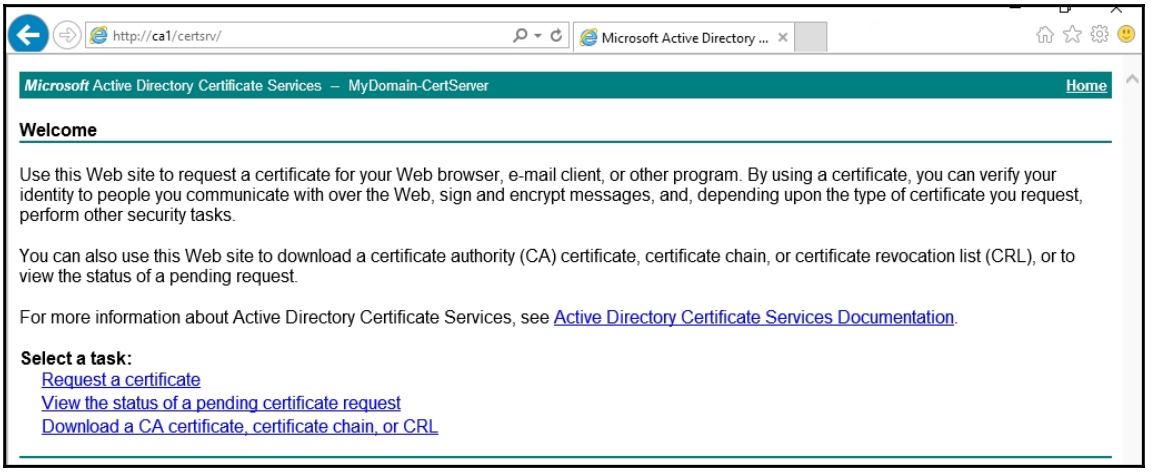

Failed Requests
Certificate Templates
Manage
New
Certificate Template to Issue
Refresh
Help

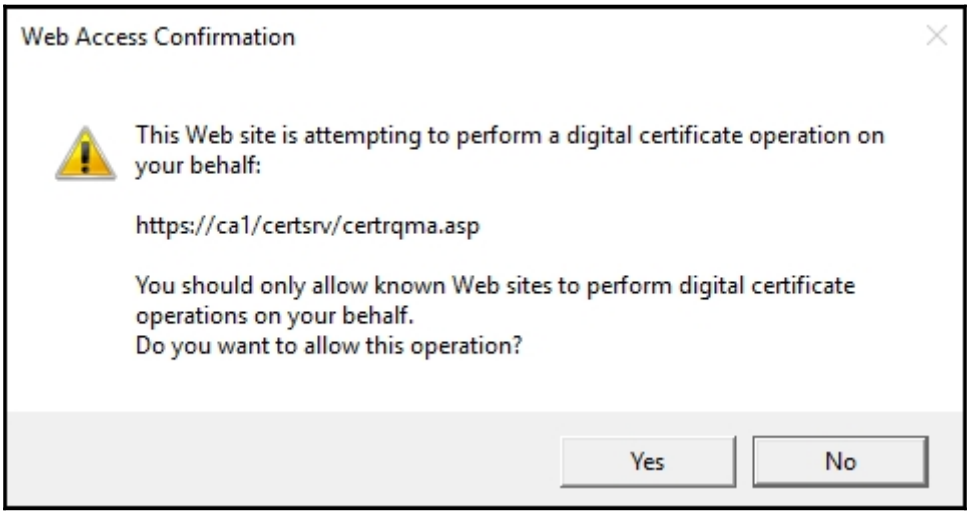

IPsec Certificate Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
Group or user names:
Authenticated Users
Administrator
Domain Admins (MYDOMAIN\Domain Admins)
Domain Computers (MYDOMAIN\Domain Computers)
Enterprise Admins (MYDOMAIN\Enterprise Admins)
Add...
Remove
Permissions for Domain Computers
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll


This snap-in will always manage certificates for:
My user account
Service account
Computer account


Console Root
Certificates (Local Computer)
Personal
Trusted F
Enterpris
Intermec
Trusted F
Untruste
Third-Pa
Trusted F
Client Au
Preview
Object Type
There are no items to show in this view.
Find Certificates...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Find Certificates...
Request New Certificate...
Import...
Advanced Operations


Active Directory Enrollment Policy
Computer
STATUS: Available
Details
IPsec Certificate
STATUS: Available
Details
Show all templates


http://ca1/certsrv/
Microsoft Active Directory ...
Microsoft Active Directory Certificate Services -- MyDomain-CertServer
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL


Web Access Confirmation
This Web site is attempting to perform a digital certificate operation on your behalf:
https://ca1/certsrv/certrqma.asp
You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?
Yes
No

Advanced Certificate Request

Certificate Template:

Custom Web Server

Identifying Information For Offline Template:

Name: sharepoint.mydomain.local

E-Mail:

Company: Your Company name

Department: Web

City: YourCity

State: YourState

Country/Region: US

Key Options:

(•) Create new key set ( ) Use existing key set

CSP: Microsoft RSA SChannel Cryptographic Provider

Key Usage: (•) Exchange

Key Size: 2048 Min: 2048 Max:16384 (common key sizes: 2048 4096 8192 16384)

(•) Automatic key container name ( ) User specified key container name

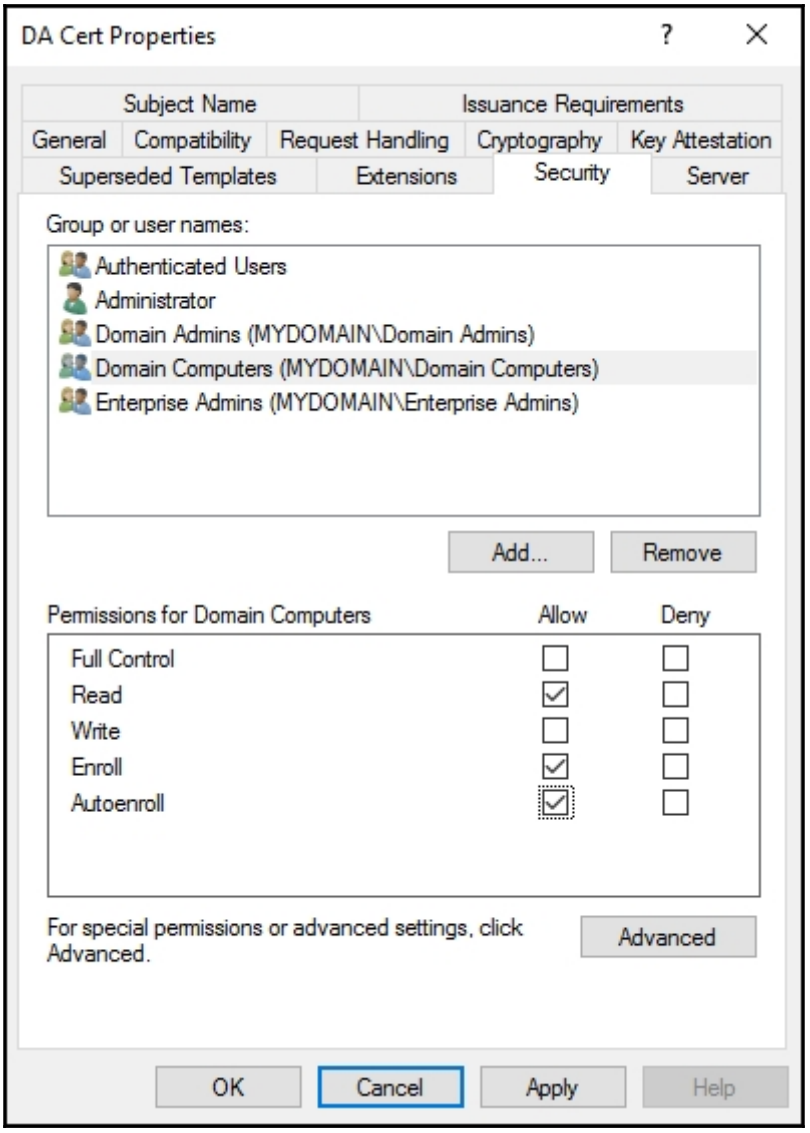
[x] Mark keys as exportable

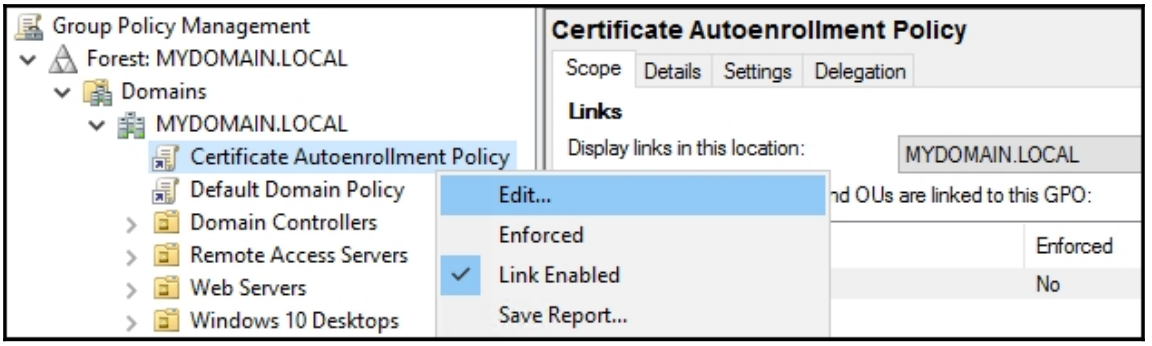
[ ] Enable strong private key protection

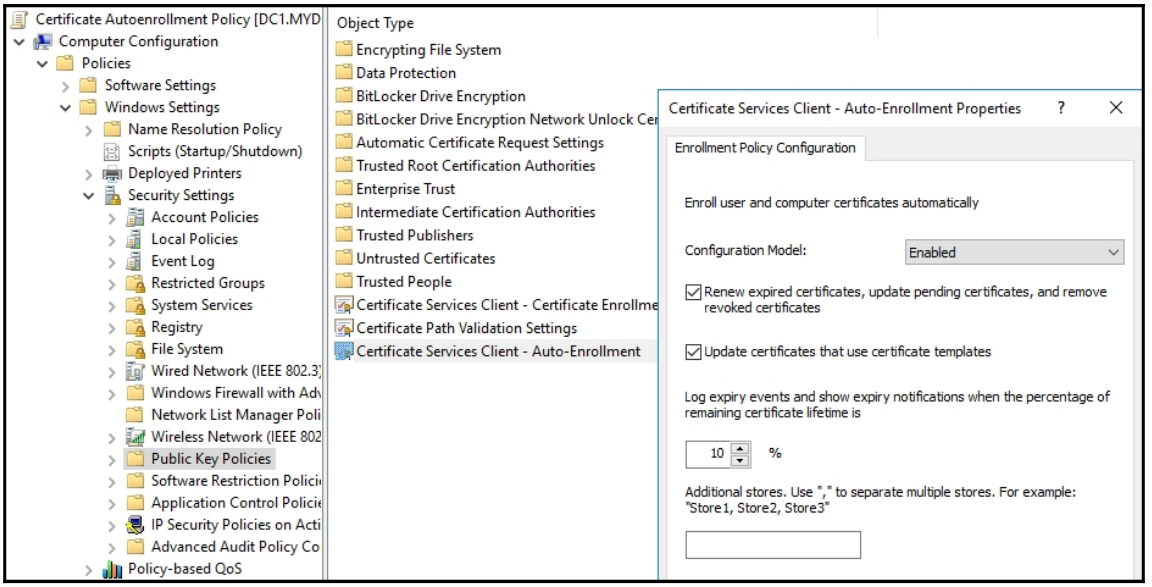
Microsoft Active Directory Certificate Services – MyDomain-CertServer

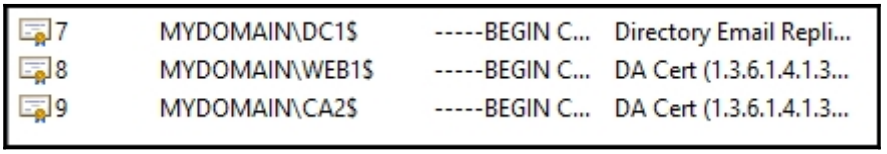
Certificate Installed

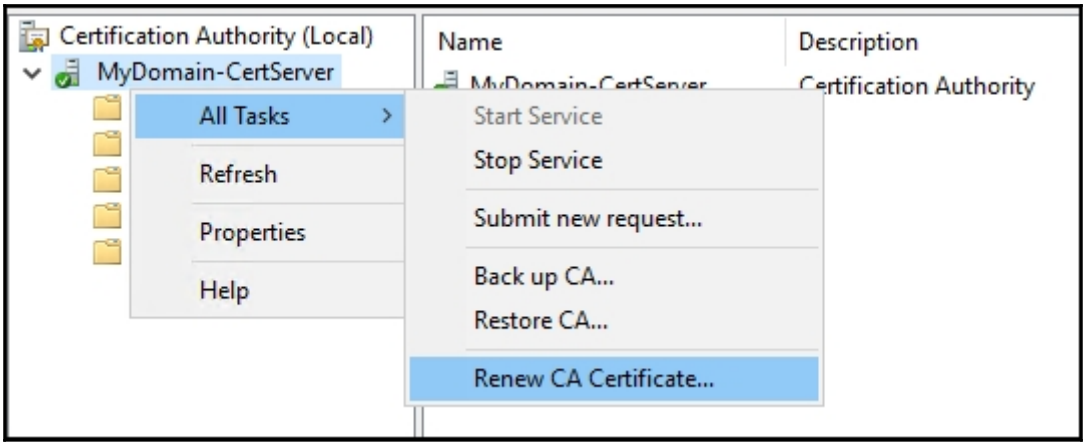
Your new certificate has been successfully installed.

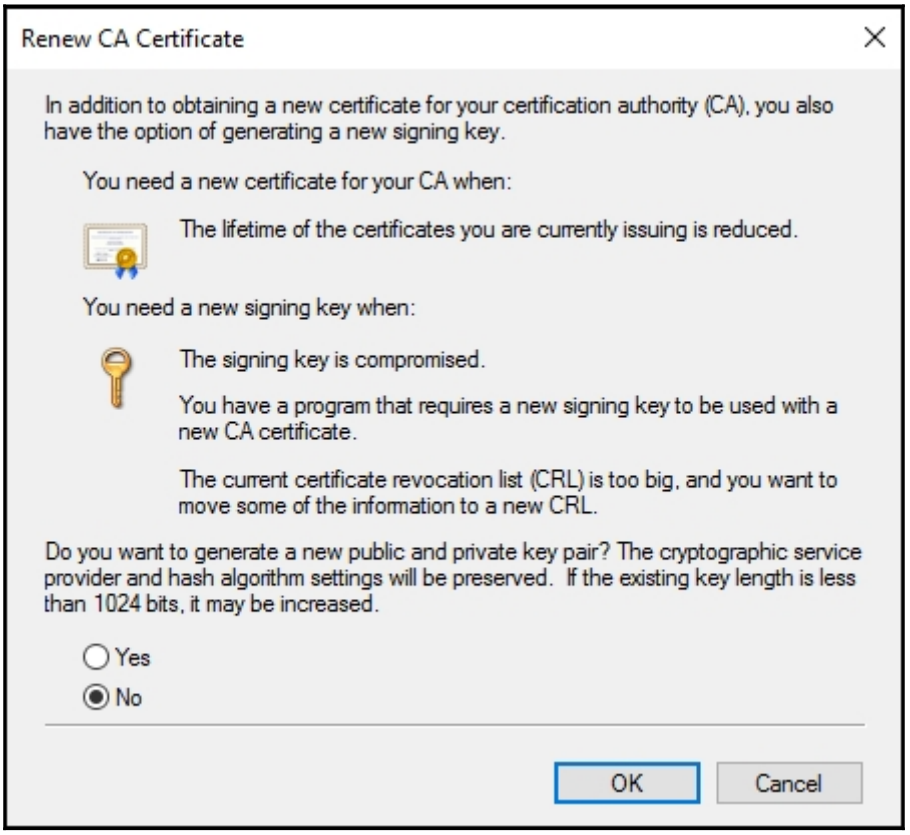

DA Cert Properties
Subject Name
Issuance Requirements
General
Compatibility
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
Server
Group or user names:
Authenticated Users
Administrator
Domain Admins (MYDOMAIN\Domain Admins)
Domain Computers (MYDOMAIN\Domain Computers)
Enterprise Admins (MYDOMAIN\Enterprise Admins)
Add...
Remove
Permissions for Domain Computers
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help


Group Policy Management
Forest: MYDOMAIN.LOCAL
Domains
MYDOMAIN.LOCAL
Certificate Autoenrollment Policy
Default Domain Policy
Domain Controllers
Remote Access Servers
Web Servers
Windows 10 Desktops
Edit...
Enforced
Link Enabled
Save Report...
Certificate Autoenrollment Policy
Scope
Details
Settings
Delegation
Links
Display links in this location:
MYDOMAIN.LOCAL
nd OUs are linked to this GPO:
Enforced
No

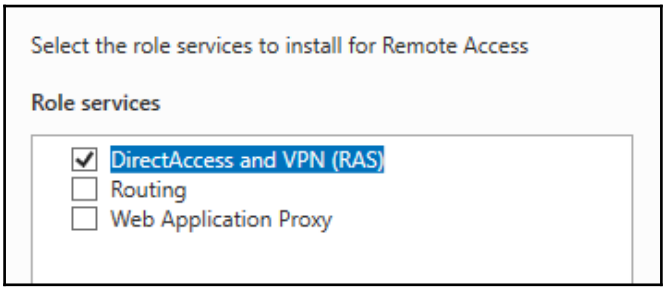

Certificate Autoenrollment Policy [DC1.MYD
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3)
Windows Firewall with Adv
Network List Manager Poli
Wireless Network (IEEE 802
Public Key Policies
Software Restriction Policie
Application Control Policie
IP Security Policies on Acti
Advanced Audit Policy Co
Policy-based QoS
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Cer
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollme
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
Certificate Services Client - Auto-Enrollment Properties
Enrollment Policy Configuration
Enroll user and computer certificates automatically
Configuration Model:
Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates
Update certificates that use certificate templates
Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is
10
%
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

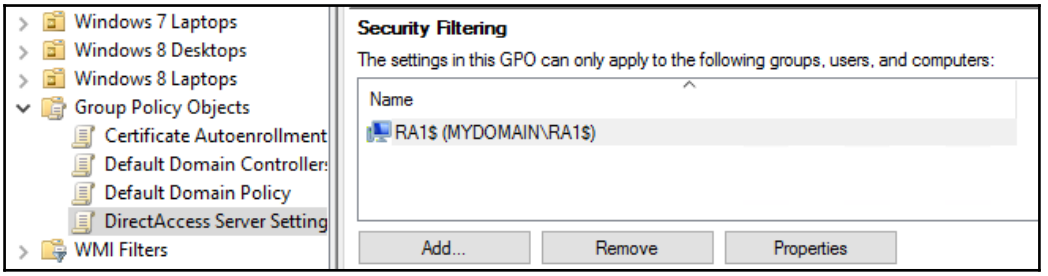

7 MYDOMAIN\DC1$ -----BEGIN C... Directory Email Repli...
8 MYDOMAIN\WEB1$ -----BEGIN C... DA Cert (1.3.6.1.4.1.3...
9 MYDOMAIN\CA2$ -----BEGIN C... DA Cert (1.3.6.1.4.1.3...

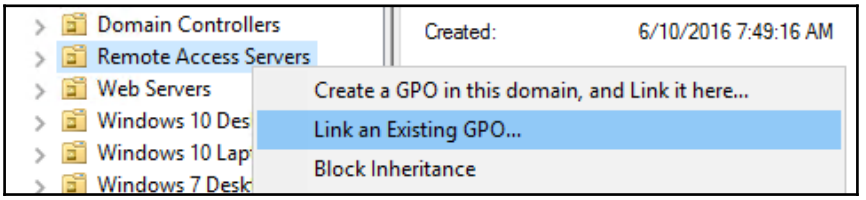

Certification Authority (Local)
MyDomain-CertServer
All Tasks
Refresh
Properties
Help
Start Service
Stop Service
Submit new request...
Back up CA...
Restore CA...
Renew CA Certificate...
Name
Description
Certification Authority

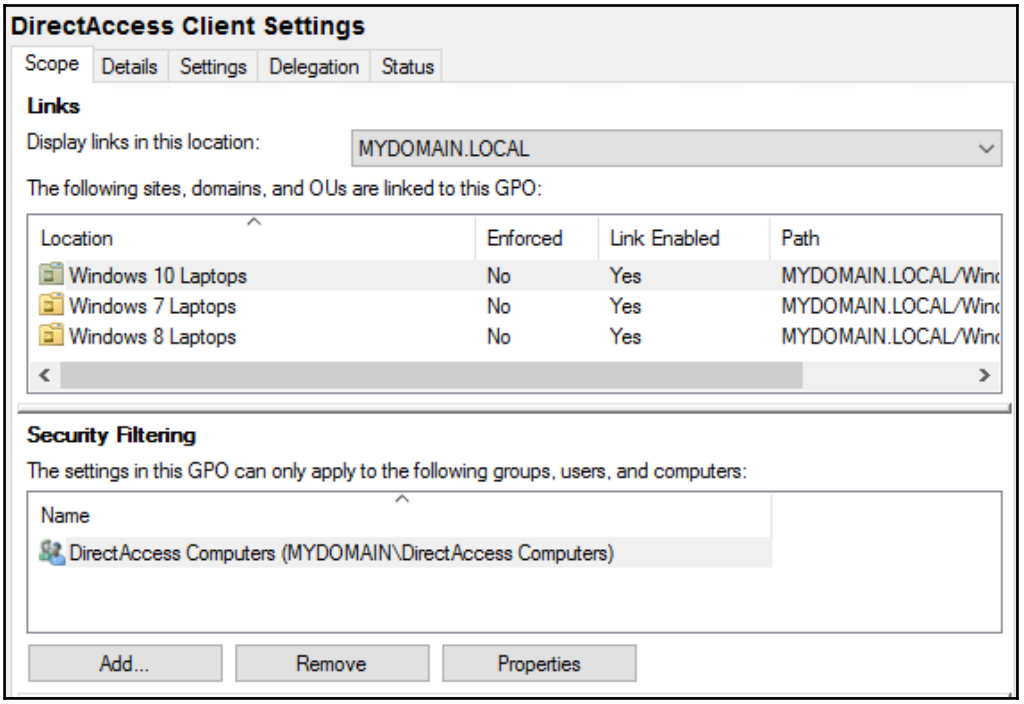

Renew CA Certificate
In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.
You need a new certificate for your CA when:
The lifetime of the certificates you are currently issuing is reduced.
You need a new signing key when:
The signing key is compromised.
You have a program that requires a new signing key to be used with a new CA certificate.
The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.
Do you want to generate a new public and private key pair? The cryptographic service provider and hash algorithm settings will be preserved. If the existing key length is less than 1024 bits, it may be increased.
Yes
No
OK
Cancel

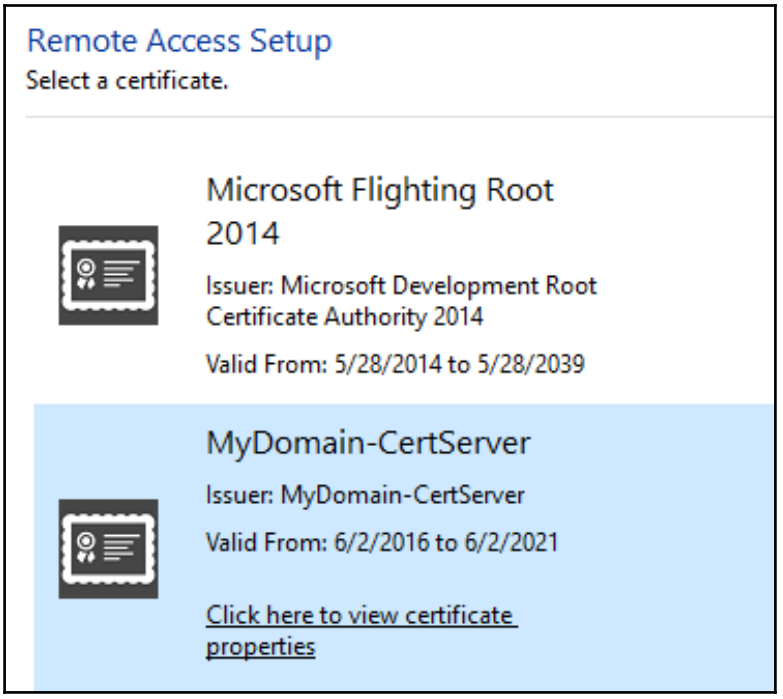
Chapter 3: Remote Access

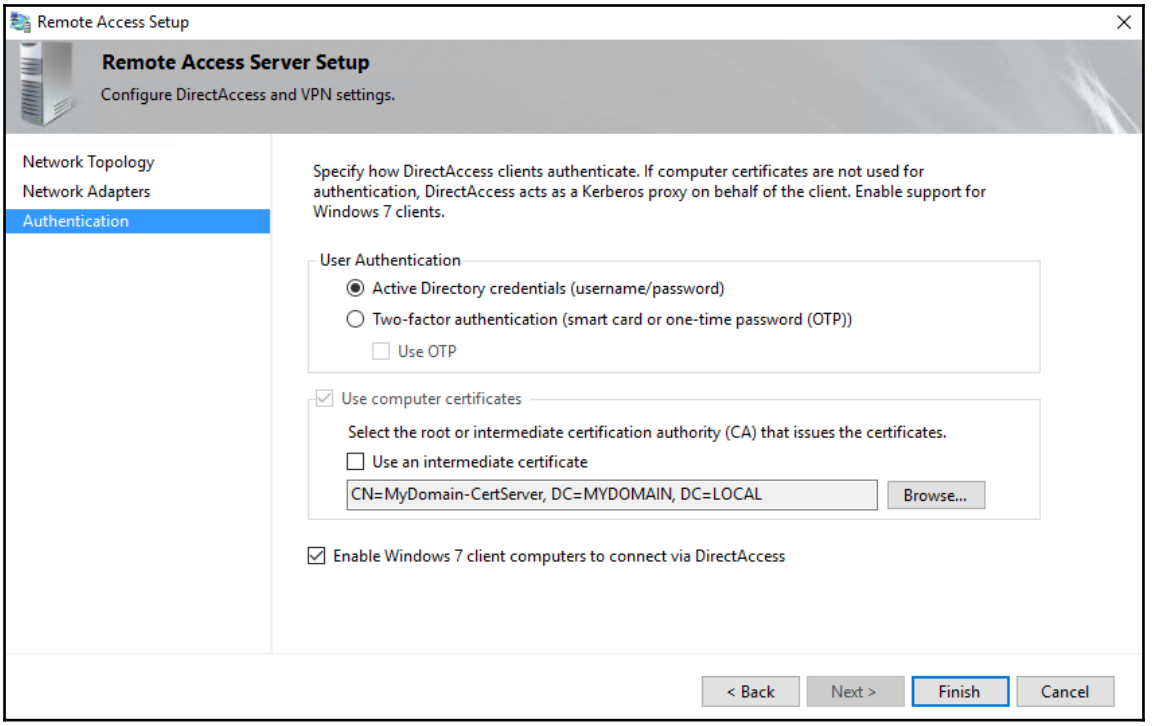


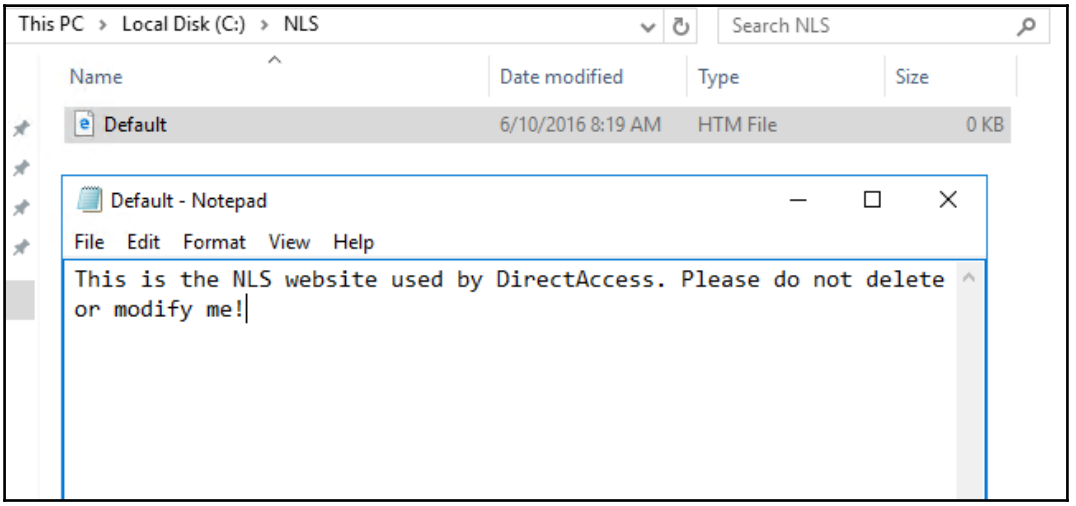


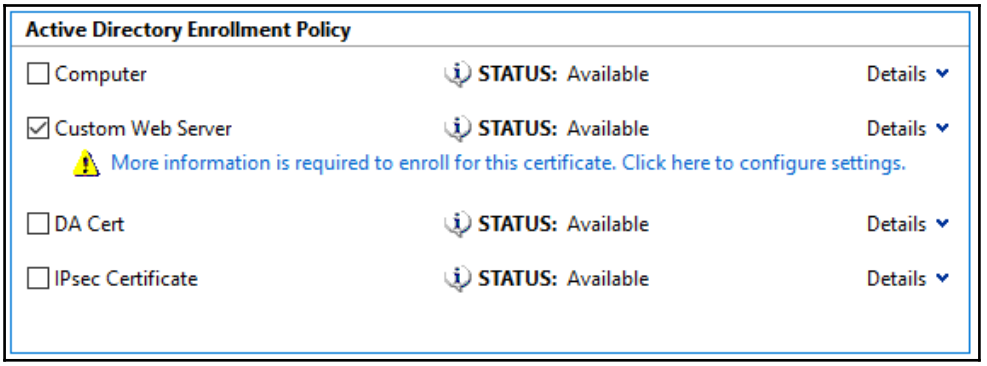


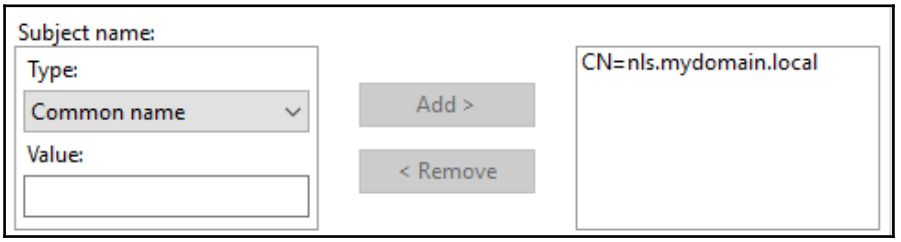

DirectAccess Client Settings
Scope
Details
Settings
Delegation
Status
Links
Display links in this location:
MYDOMAIN.LOCAL
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
Windows 10 Laptops
No
Yes
MYDOMAIN.LOCAL/Winc
Windows 7 Laptops
No
Yes
MYDOMAIN.LOCAL/Winc
Windows 8 Laptops
No
Yes
MYDOMAIN.LOCAL/Winc
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
DirectAccess Computers (MYDOMAIN\DirectAccess Computers)
Add...
Remove
Properties

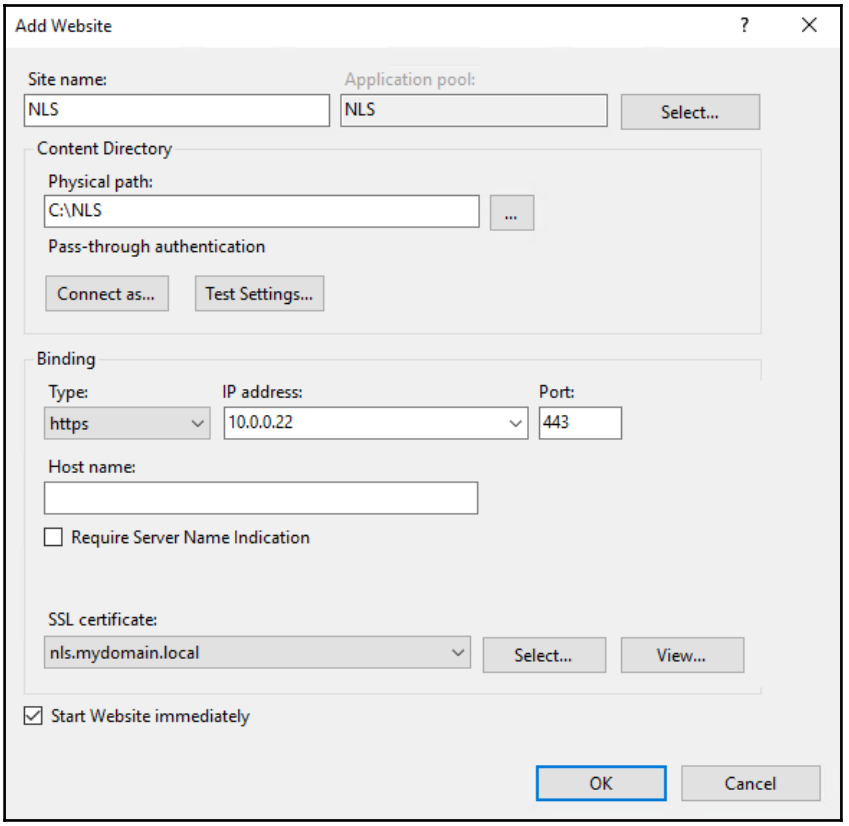

Remote Access Setup
Select a certificate.
Microsoft Flighting Root 2014
Issuer: Microsoft Development Root Certificate Authority 2014
Valid From: 5/28/2014 to 5/28/2039
MyDomain-CertServer
Issuer: MyDomain-CertServer
Valid From: 6/2/2016 to 6/2/2021
Click here to view certificate properties

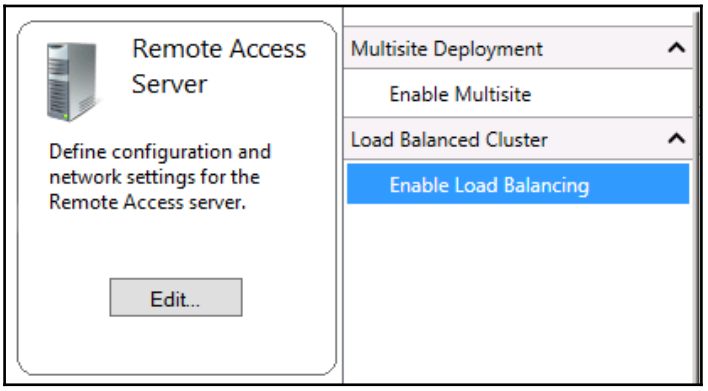

Remote Access Setup
Remote Access Server Setup
Configure DirectAccess and VPN settings.
Network Topology
Network Adapters
Authentication
Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients.
User Authentication
Active Directory credentials (username/password)
Two-factor authentication (smart card or one-time password (OTP))
Use OTP
Use computer certificates
Select the root or intermediate certification authority (CA) that issues the certificates.
Use an intermediate certificate
CN=MyDomain-CertServer, DC=MYDOMAIN, DC=LOCAL
Browse...
Enable Windows 7 client computers to connect via DirectAccess
< Back
Next >
Finish
Cancel


This PC > Local Disk (C:) > NLS
Search NLS
Name
Date modified
Type
Size
Default
6/10/2016 8:19 AM
HTM File
0 KB
Default - Notepad
File Edit Format View Help
This is the NLS website used by DirectAccess. Please do not delete or modify me!


Active Directory Enrollment Policy
Computer
STATUS: Available
Details
Custom Web Server
STATUS: Available
Details
More information is required to enroll for this certificate. Click here to configure settings.
DA Cert
STATUS: Available
Details
IPsec Certificate
STATUS: Available
Details


Subject name:
Type:
Common name
Value:
Add >
< Remove
CN=nls.mydomain.local


Add Website
Site name:
NLS
Application pool:
NLS
Select...
Content Directory
Physical path:
C:\NLS
...
Pass-through authentication
Connect as...
Test Settings...
Binding
Type:
https
IP address:
10.0.0.22
Port:
443
Host name:
Require Server Name Indication
SSL certificate:
nls.mydomain.local
Select...
View...
Start Website immediately
OK
Cancel


Remote Access Server
Define configuration and network settings for the Remote Access server.
Edit...
Multisite Deployment
Enable Multisite
Load Balanced Cluster
Enable Load Balancing

External Dedicated IP Addresses

- Before You Begin
- Load Balancing Method
- External DIPs
- Internal DIPs
- Summary
- Completion

Configure dedicated IP addresses (DIPs) for the server external adapter. With load balancing enabled, the current primary DIPs of the network adapters will be used as the virtual IP addresses (VIPs) for the load balanced cluster.

IPv4 address: 1.1.1.12

Example: 203.0.113.18

Subnet mask: 255.255.255.0

Example: 255.255.0.0

Internal Dedicated IP Addresses

- Before You Begin
- Load Balancing Method
- External DIPs
- Internal DIPs
- Summary
- Completion

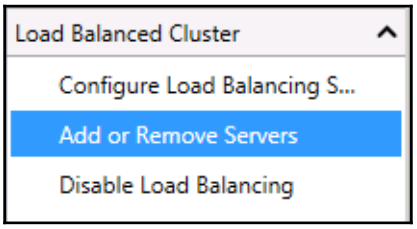
Configure dedicated IP addresses (DIPs) for the server internal adapter. With load balancing enabled, the current primary DIPs of the network adapters will be used as the virtual IP addresses (VIPs) for the load balanced cluster.

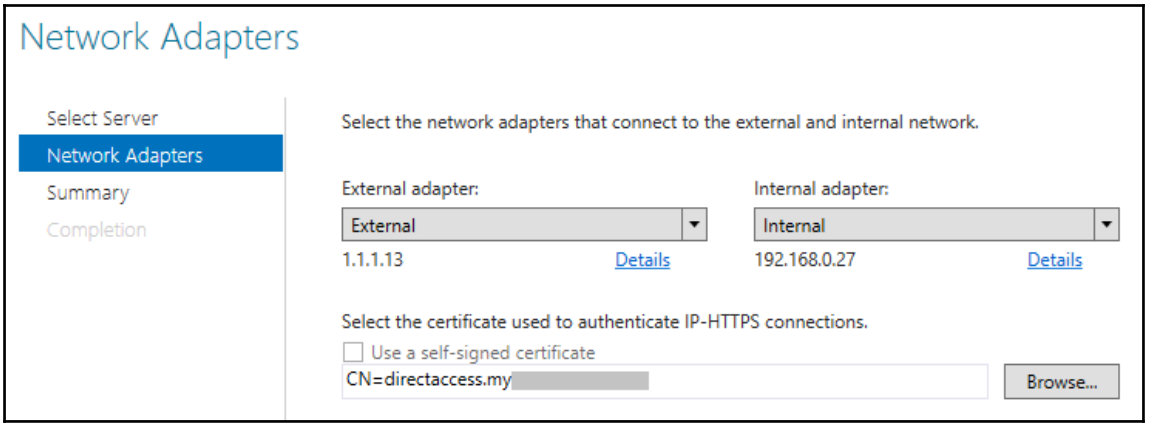
IPv4 address: 10.0.0.8

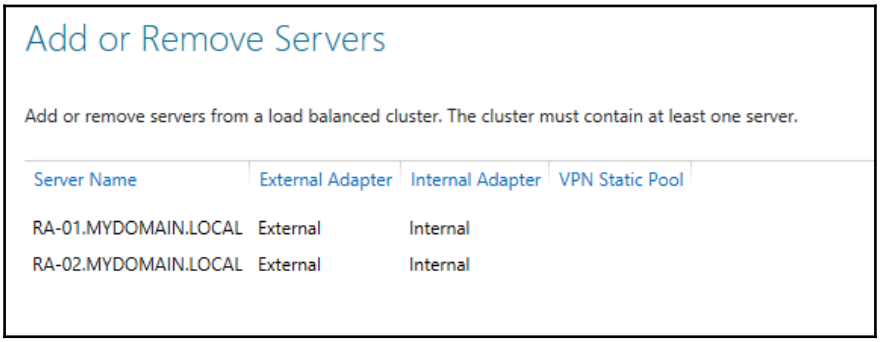
Example: 10.0.0.18

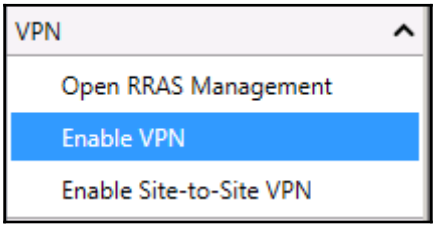
Subnet mask: 255.255.255.0

Example: 255.255.0.0




Network Adapters
Select Server
Network Adapters
Summary
Completion
Select the network adapters that connect to the external and internal network.
External adapter:
External
1.1.1.13
Details
Internal adapter:
Internal
192.168.0.27
Details
Select the certificate used to authenticate IP-HTTPS connections.
Use a self-signed certificate
CN=directaccess.my
Browse...


Add or Remove Servers
Add or remove servers from a load balanced cluster. The cluster must contain at least one server.
Server Name
External Adapter
Internal Adapter
VPN Static Pool
RA-01.MYDOMAIN.LOCAL
External
Internal
RA-02.MYDOMAIN.LOCAL
External
Internal


VPN
Open RRAS Management
Enable VPN
Enable Site-to-Site VPN

IP Address Assignment | Authentication

Address assignment method:

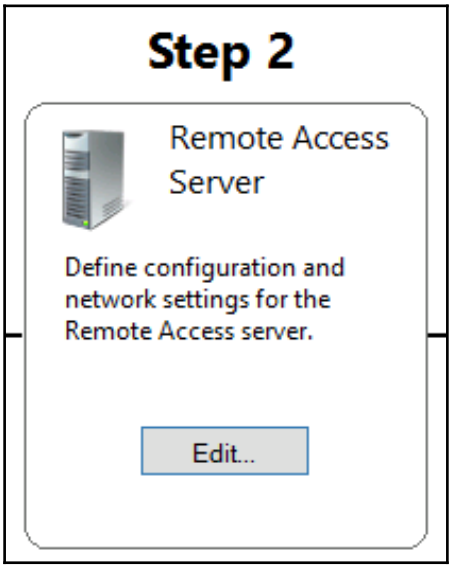
○ Assign addresses automatically

With this option enabled, addresses are assigned by a DHCP server.

◉ Assign addresses from a static address pool

Add IP address ranges to the static pool. Addresses are assigned from the first range before continuing to the next.

	From	To	Number
	10.0.1.1	10.0.1.254	254
▸*			



Select the certificate used to authenticate IP-HTTPS connections:

☐ Use a self-signed certificate created automatically by DirectAccess

CN=directaccess. [redacted] | Browse...

Some configuration changes have not been applied. Click Finish to apply the changes.

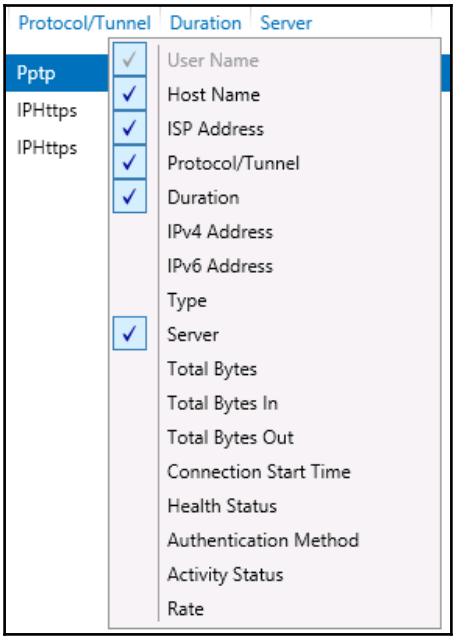
Finish...

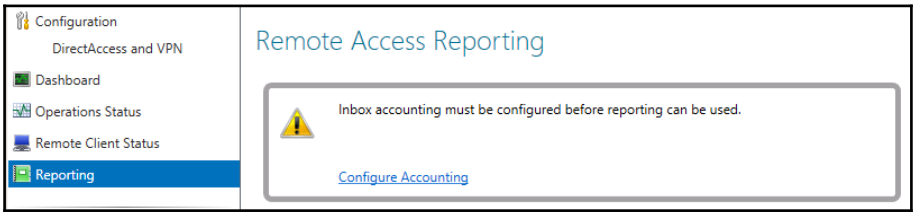
Connection Details

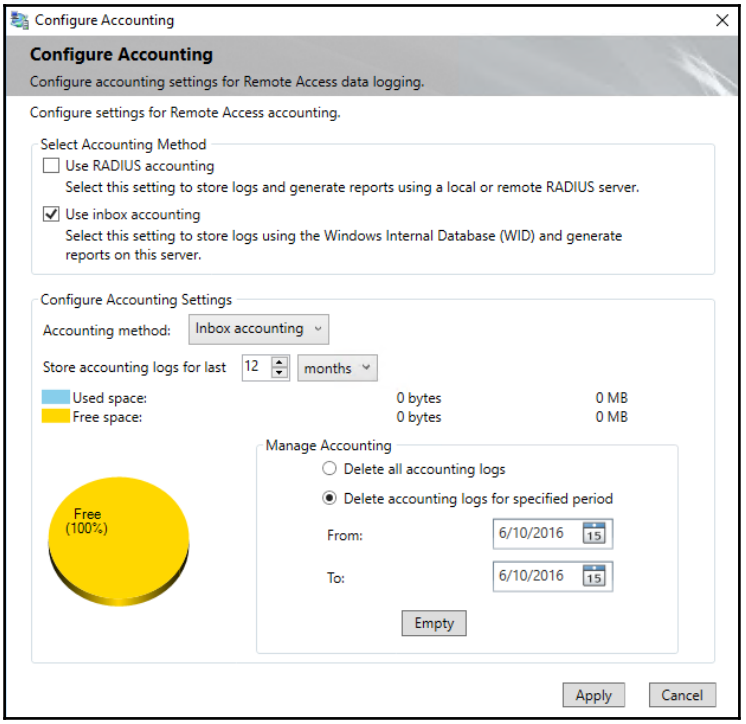
Connect Using	DirectAccess
Total Bytes In	201608
Total Bytes Out	311496
Connection start	6/10/2016 12:52:43 PM
Authentication	Machine Certificate, User Nt
ISP Address	-

Access Details

Protocol	Port	IP Address
6	80	192.168.250.45
6	445	192.168.250.18
17	389	192.168.250.2


Protocol/Tunnel
Duration
Server
Pptp
IPHttps
IPHttps
User Name
Host Name
ISP Address
Protocol/Tunnel
Duration
IPv4 Address
IPv6 Address
Type
Server
Total Bytes
Total Bytes In
Total Bytes Out
Connection Start Time
Health Status
Authentication Method
Activity Status
Rate


Configuration
DirectAccess and VPN
Dashboard
Operations Status
Remote Client Status
Reporting
Remote Access Reporting
Inbox accounting must be configured before reporting can be used.
Configure Accounting


Configure Accounting
Configure Accounting
Configure accounting settings for Remote Access data logging.
Configure settings for Remote Access accounting.
Select Accounting Method
Use RADIUS accounting
Select this setting to store logs and generate reports using a local or remote RADIUS server.
Use inbox accounting
Select this setting to store logs using the Windows Internal Database (WID) and generate reports on this server.
Configure Accounting Settings
Accounting method:
Inbox accounting
Store accounting logs for last
12
months
Used space:
0 bytes
0 MB
Free space:
0 bytes
0 MB
Free (100%)
Manage Accounting
Delete all accounting logs
Delete accounting logs for specified period
From:
6/10/2016
To:
6/10/2016
Empty
Apply
Cancel