Lesson 11: Configuring DirectAccess

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 3.4: Configure DirectAccess
- Understanding DirectAccess

Understanding DirectAccess

Lesson 11: Configuring DirectAccess

DirectAccess

- Overcomes limitations of VPNs
- Automatically establishes a bi-directional connection from client computers to the network using IPsec and IPv6
- Transition mechanisms for IPv6:
  - 6to4
  - Teredo
  - Intra-Site Automatic Tunnel Addressing (ISATAP)

DirectAccess Connection Process

1. The DirectAccess client computer running Windows 8, Windows 7 Enterprise, or Windows 7 Ultimate detects that it is connected to a network.
2. The DirectAccess client computer determines whether it is connected to the intranet. If the client is connected to the intranet, it does not use DirectAccess.
3. The DirectAccess client connects to the DirectAccess server by using IPv6 and IPsec.
4. If the client is not using IPv6, it will try to use 6to4 or Teredo tunneling to send IPv4-encapsulated IPv6 traffic.
5. If the client cannot reach the DirectAccess server using 6to4 or Teredo tunneling, the client tries to connect using the Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) protocol. IP-HTTPS uses a Secure Sockets Layer (SSL) connection to encapsulate IPv6 traffic.

DirectAccess Connection Process

6. As part of establishing the IPsec session for the tunnel to reach the intranet DNS server and domain controller, the DirectAccess client and server authenticate each other using computer certificates for authentication.
7. If Network Access Protection (NAP) is enabled and configured for health validation, the Network Policy Server (NPS) determines whether the client is compliant with system health requirements. If it is compliant, the client receives a health certificate, which is submitted to the DirectAccess server for authentication.
8. When the user logs on, the DirectAccess client establishes a second IPsec tunnel to access the resources of the intranet. The DirectAccess client and server authenticate each other using a combination of computer and user credentials.
9. The DirectAccess server forwards traffic between the DirectAccess client and the intranet resources to which the user has been granted access.

DirectAccess Server Requirements

- The server must be part of an Active Directory domain.
- The server must be running Windows Server 2008 R2 or Windows Server 2012.
- If the DirectAccess server is connected to the intranet and published over Microsoft Forefront Threat Management Gateway (TMG) or Microsoft Forefront Unified Access Gateway 2010 (UAG), a single network adapter is required.
  - If the DirectAccess server is connected as an edge server, it will need two network adapters (one for the Internet and one for the intranet).

DirectAccess Server Requirements

- Implementation of DirectAccess in Windows Server 2012 does not require two consecutive static, public IPv4 addresses as was required with Windows Server 2008 R2.
  - To achieve two-factor authentication with a smart card or Operational Data Provider (OTP) deployment, DirectAccess server still needs two public IP addresses.

DirectAccess Server Requirements

- You can deploy Windows Server 2012 DirectAccess behind a NAT support, which avoids the need for additional public addresses.
  - Only IP over HTTPS (IP-HTTPS) is deployed, allowing a secure IP tunnel to be established using a secure HTTP connection.
- With Windows Server 2012, you can use Network Load Balancing (up to eight nodes) to achieve high availability and scalability for both DirectAccess and RRAS.

Network Infrastructure for DirectAccess

- An Active Directory domain
- Group policy
- One domain controller
- Public Key Infrastructure (PKI)
- IPsec policies

Network Infrastructure for DirectAccess

- Internet Control Message Protocol Version 6 (ICMPv6) Echo Request traffic
- IPv6 and transition technologies such as ISATAP, Teredo, or 6to4
- (Optional) Network Access Protection (NAP)

DirectAccess Client Requirements

Operating system

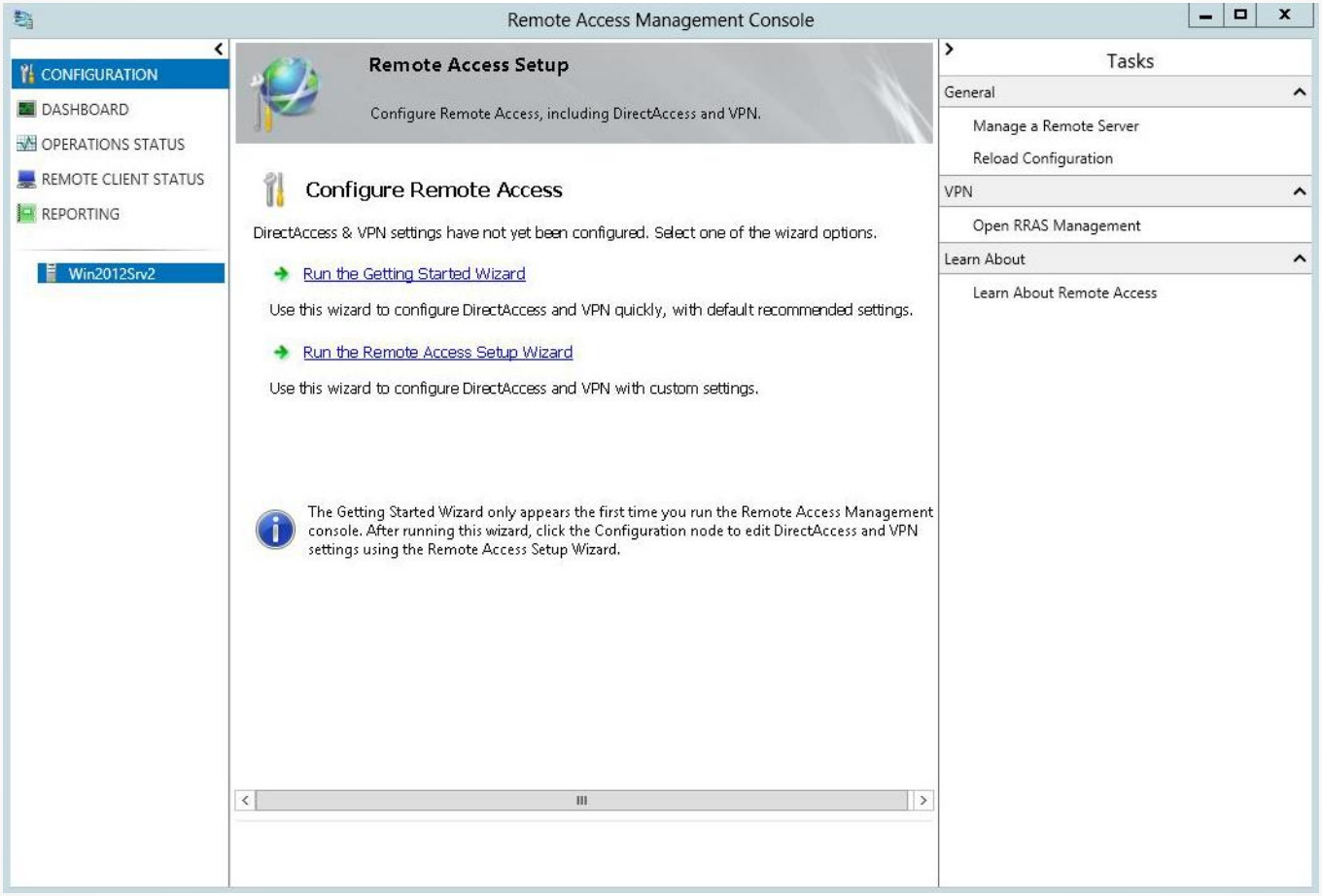
- Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, or Windows Server 2012

Client must be joined to an Active Directory domain

Running the DirectAccess Getting Started Wizard

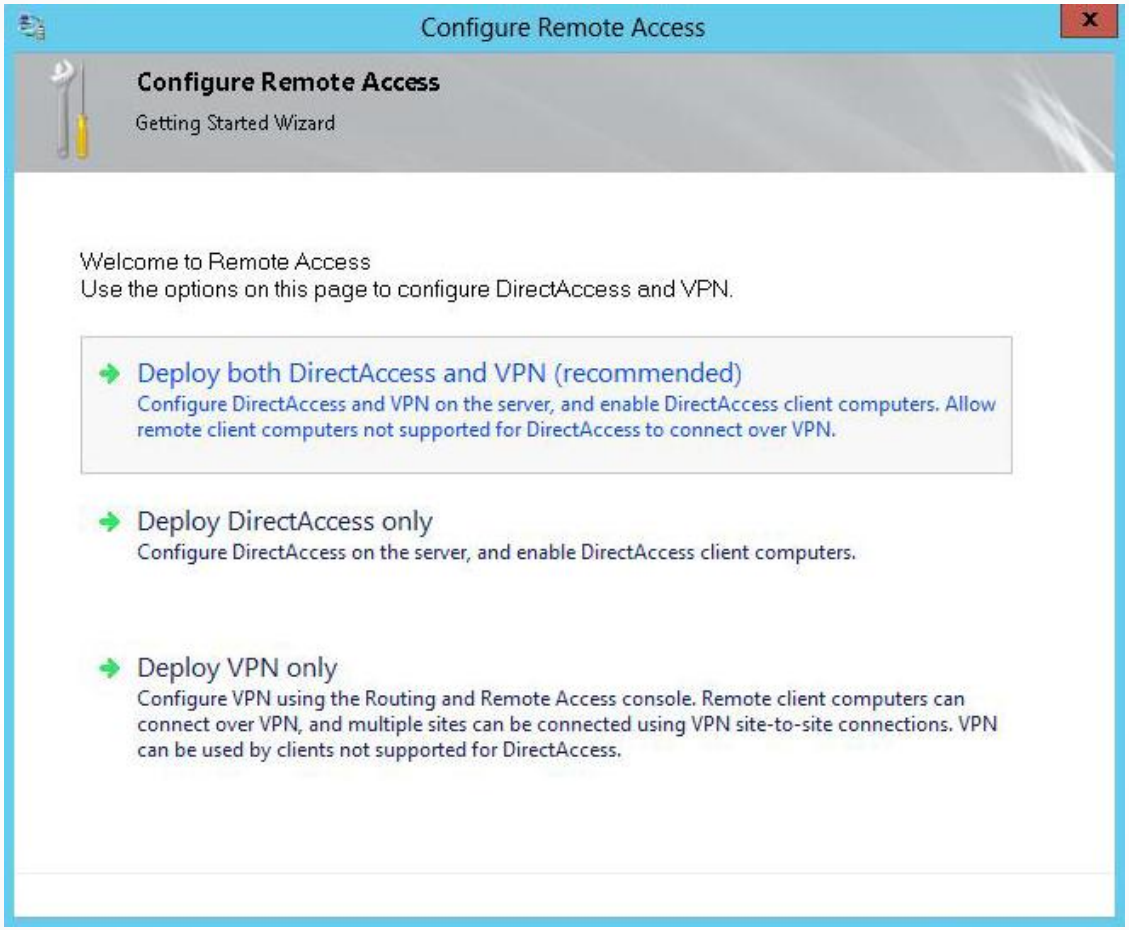
- Configures DirectAccess
- Can run from Remote Access Management console

Run the DirectAccess Getting Started Wizard



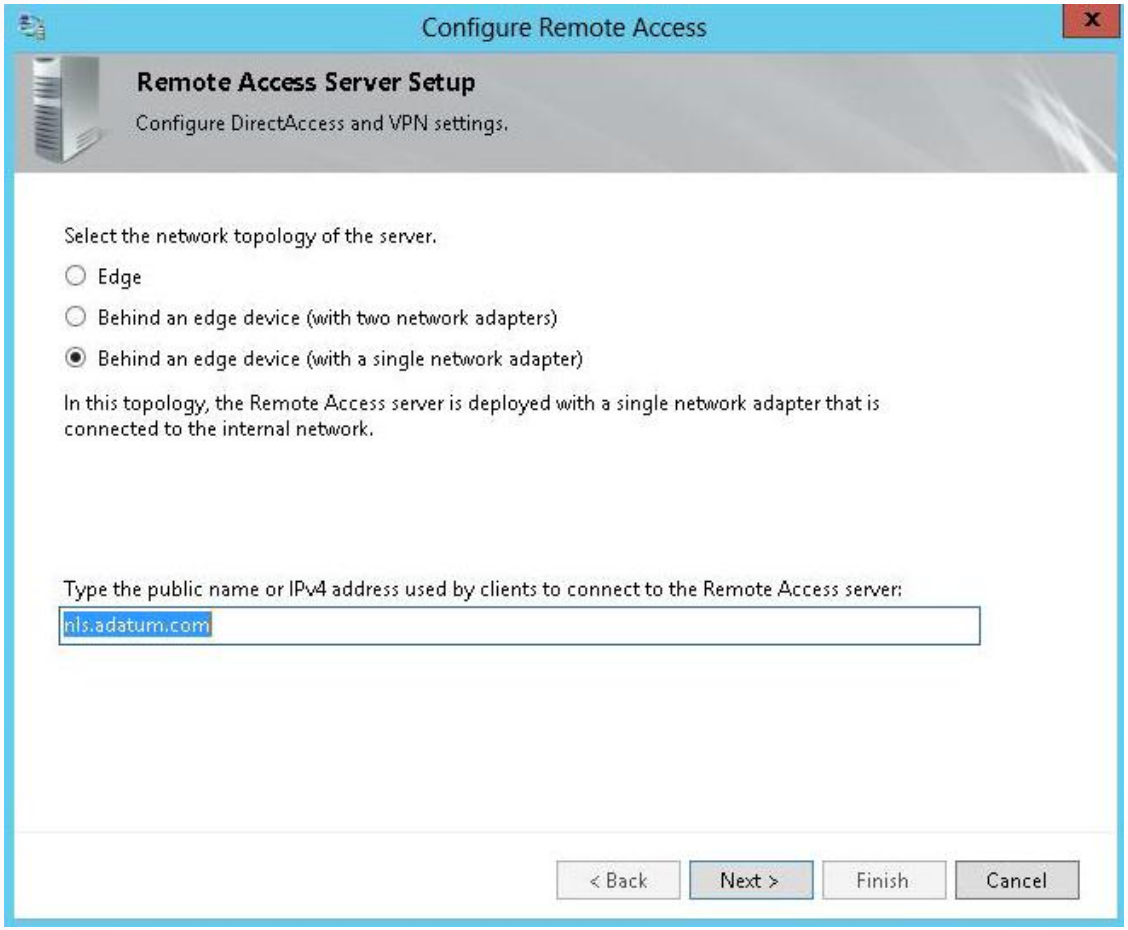
Opening the Remote Access Management console

Run the DirectAccess Getting Started Wizard



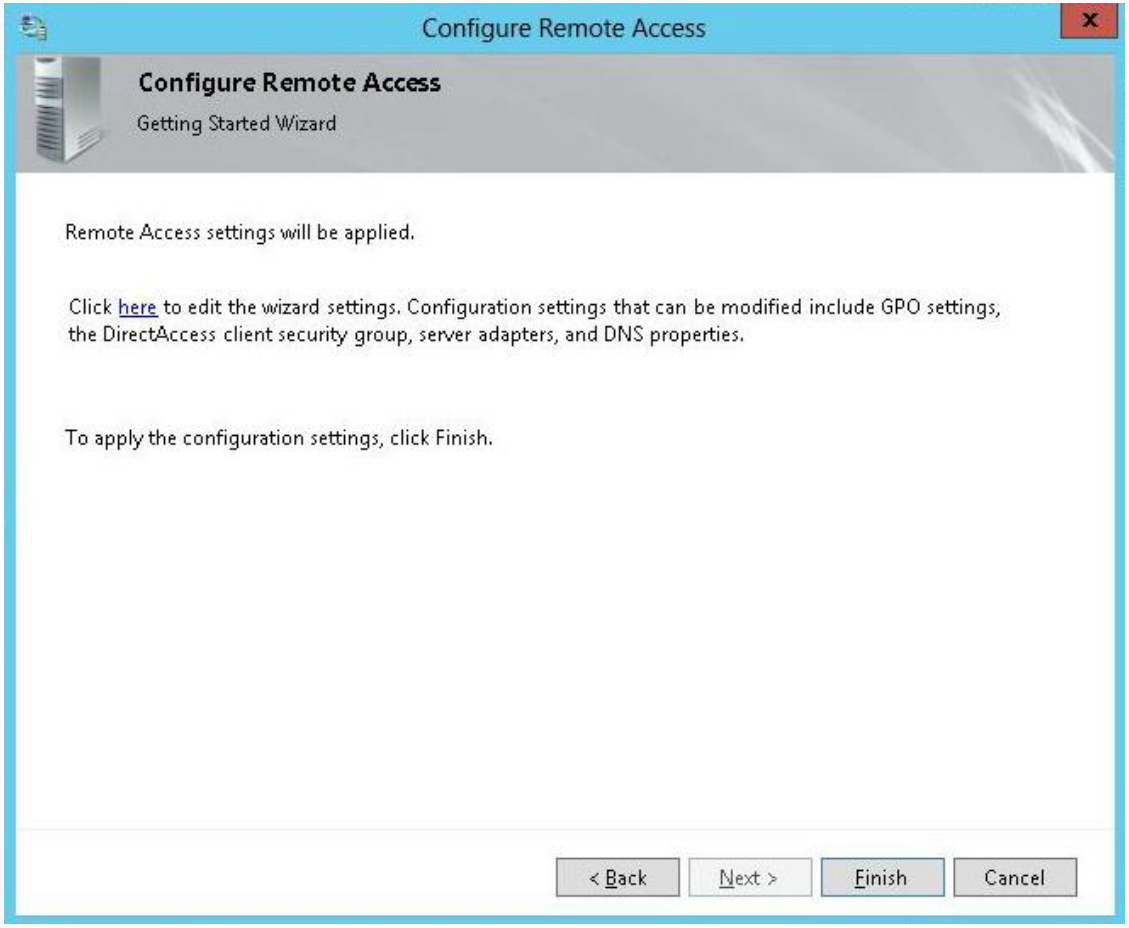
Starting the Configure Remote Access Wizard

Run the DirectAccess Getting Started Wizard



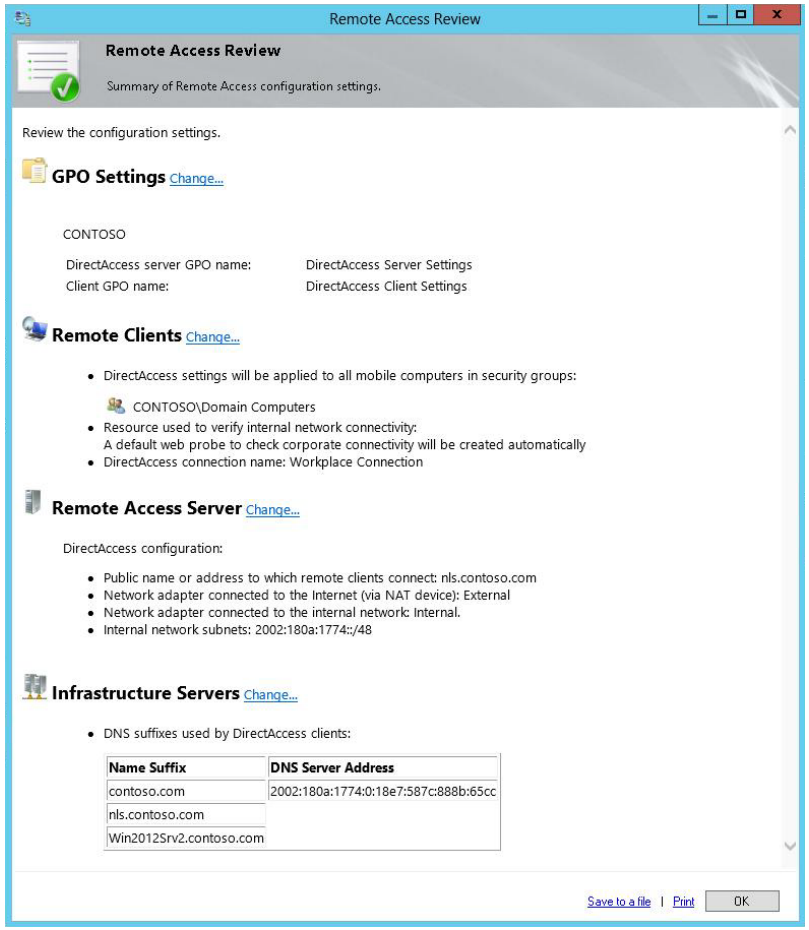
Selecting a topology on the Configure DirectAccess and VPN Settings page

Run the DirectAccess Getting Started Wizard



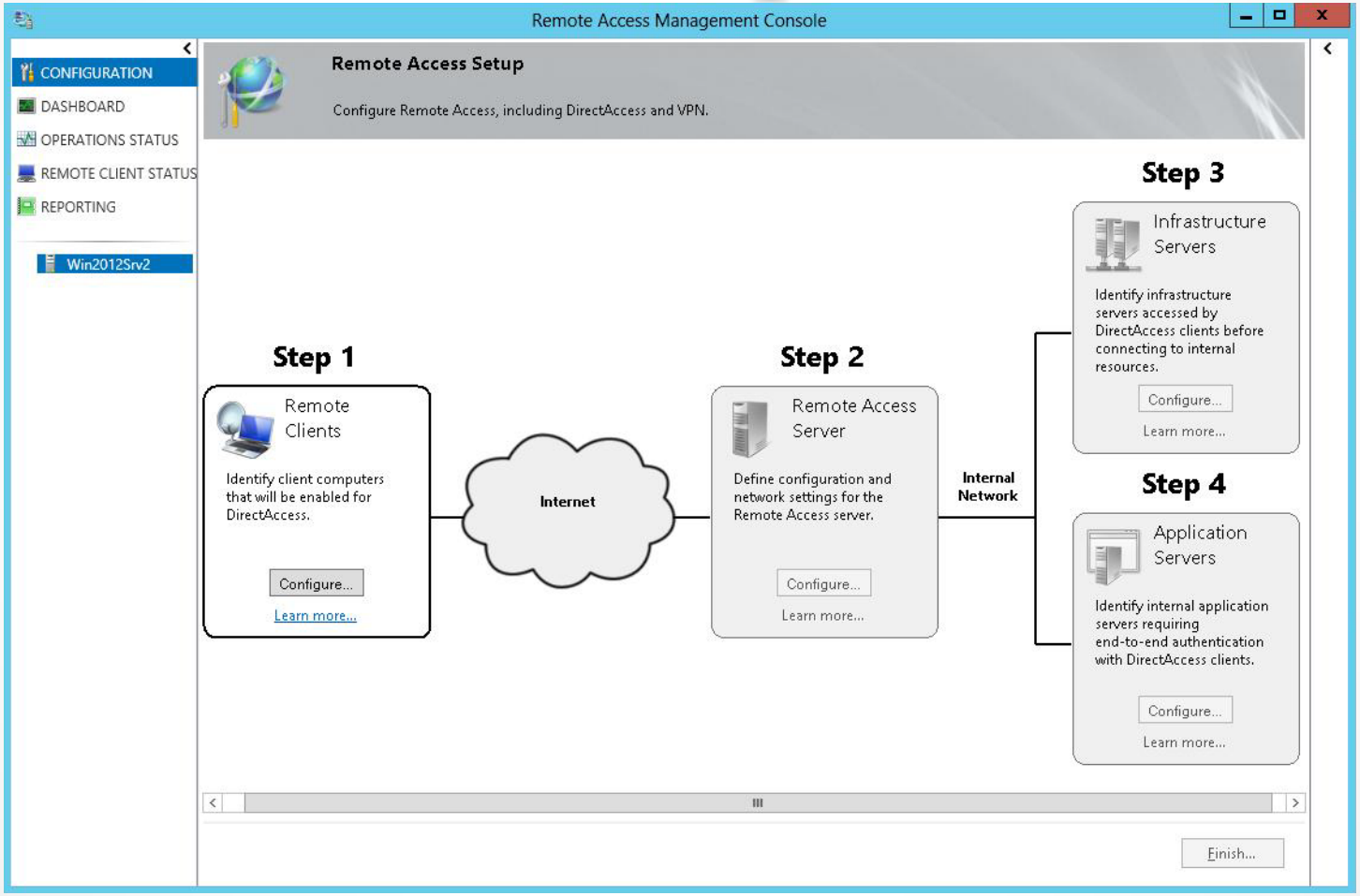
Finishing the Getting Started Wizard

Run the DirectAccess Getting Started Wizard



Viewing the settings applied using the Getting Started Wizard

Running the Remote Access Setup Wizard



Implementing Client Configuration

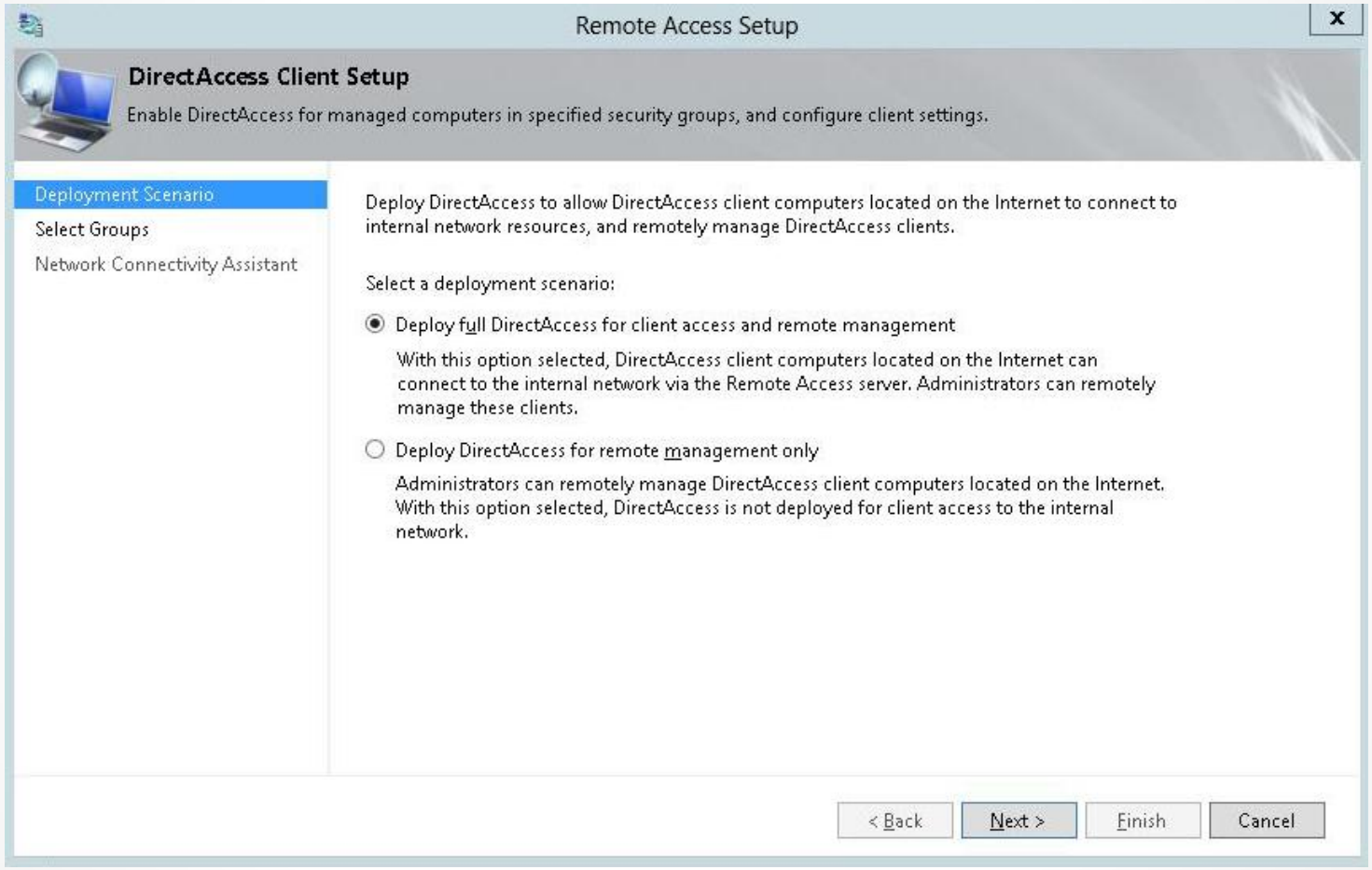
DirectAccess Connectivity Assistant (DCA)

- Window 7 and Windows Server 2008 R2

Network Connectivity Assistant (NCA)

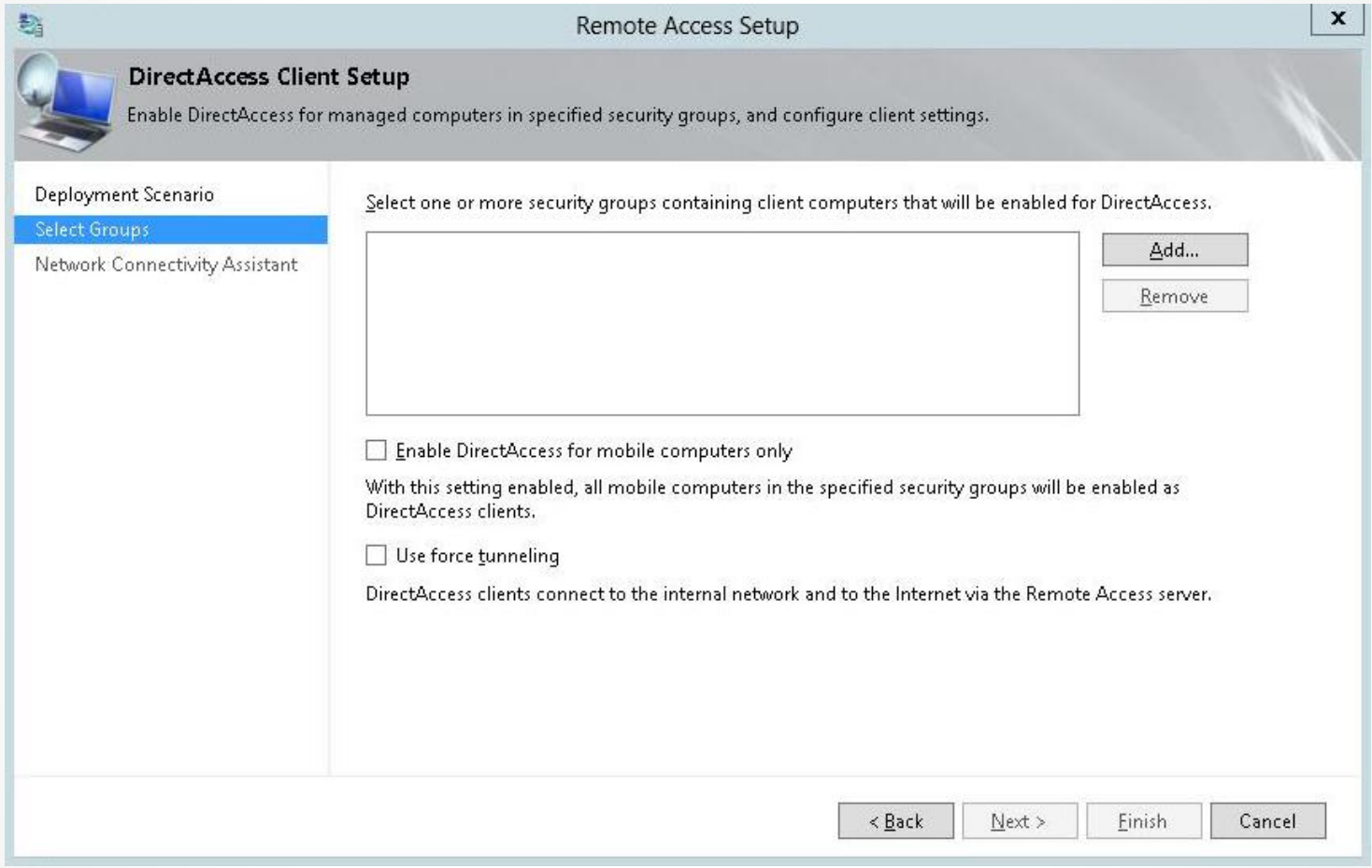
- Windows 8

Configure Remote Clients



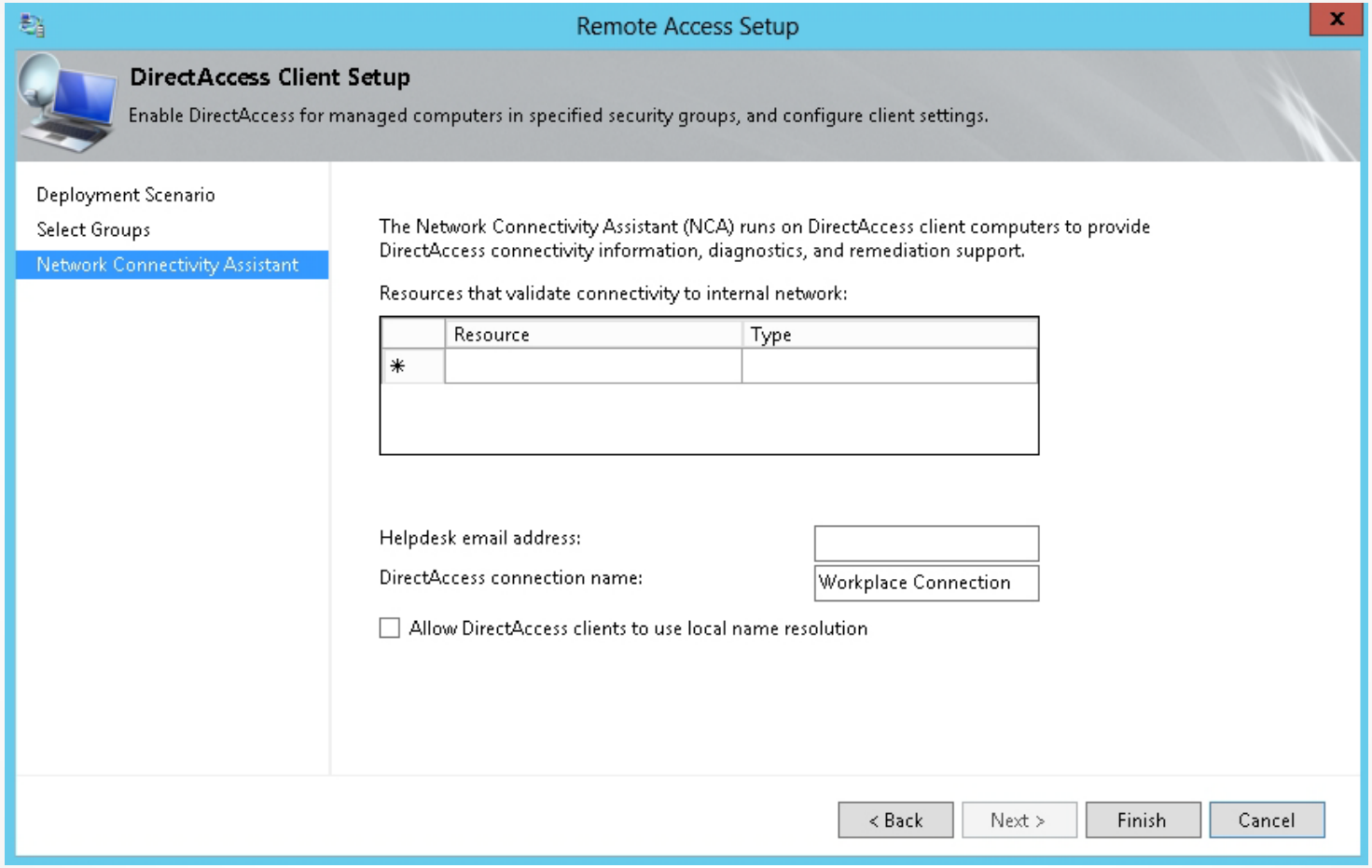
Specifying the deployment scenario

Configure Remote Clients



Selecting client groups

Configure Remote Clients

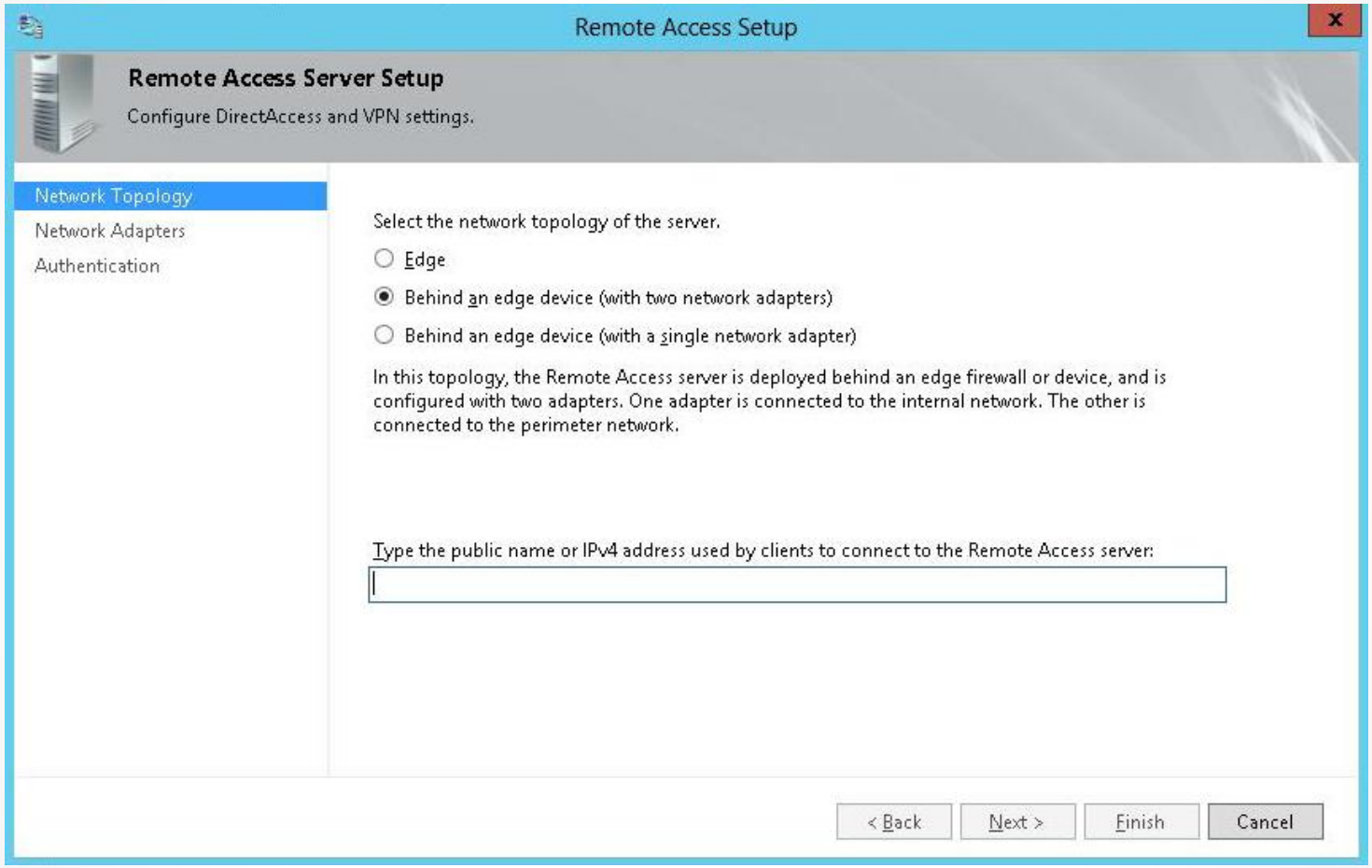


Configuring the Network Connectivity Assistant

Configure Remote Clients

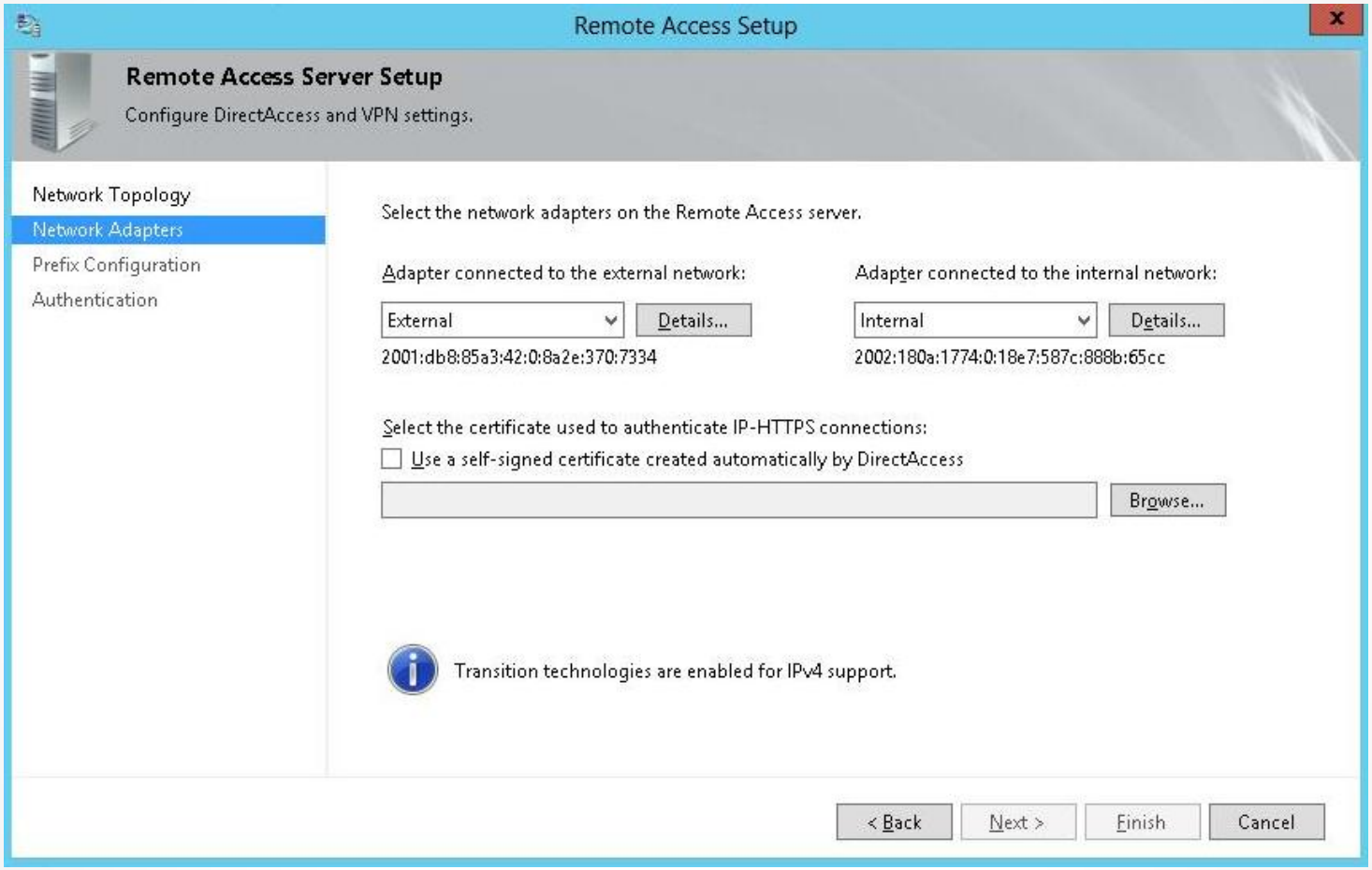
Configuring corporate resources for NCA

Configure the DirectAccess Remote Access Server



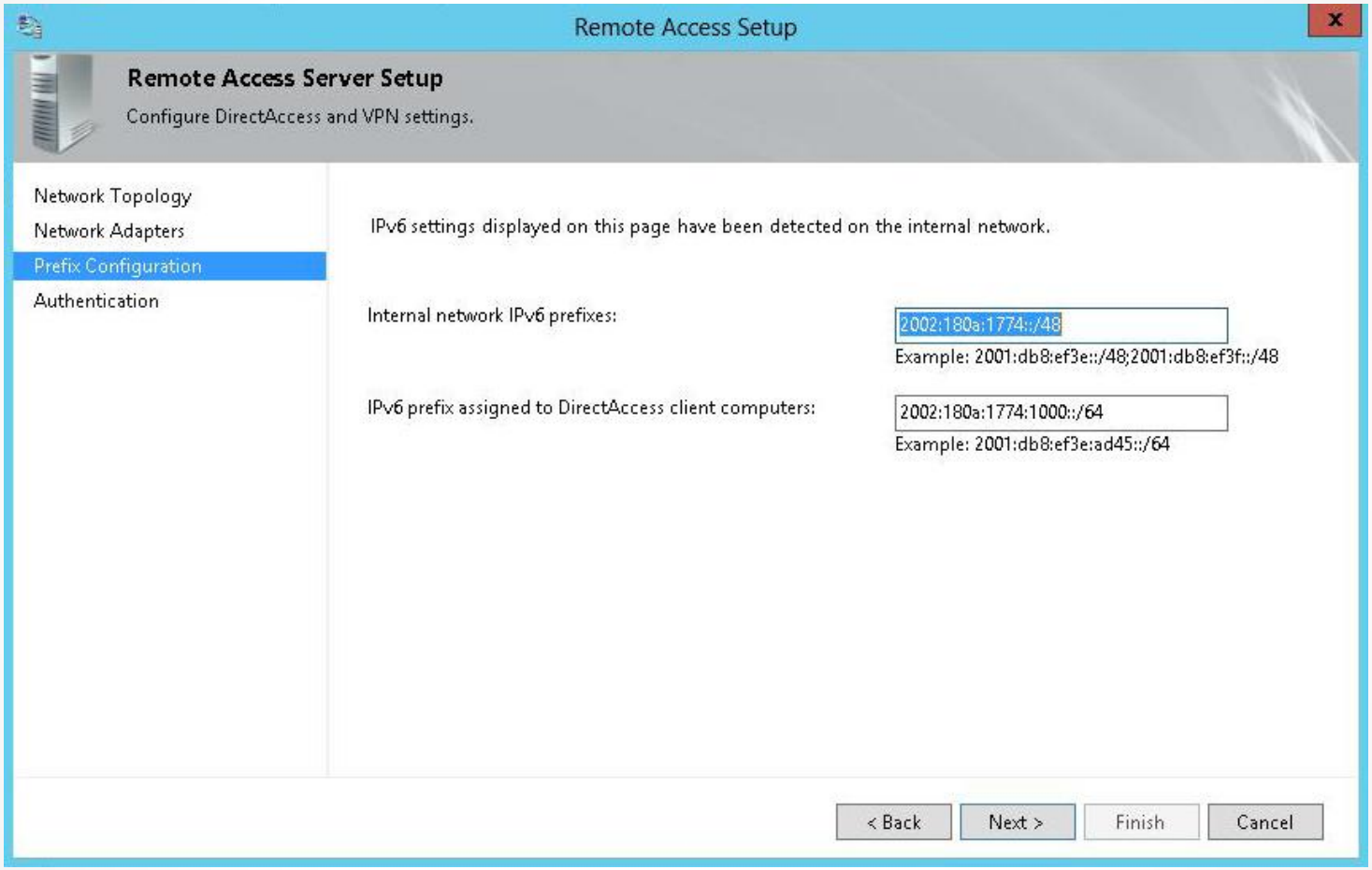
Specifying the network topology

Configure the DirectAccess Remote Access Server



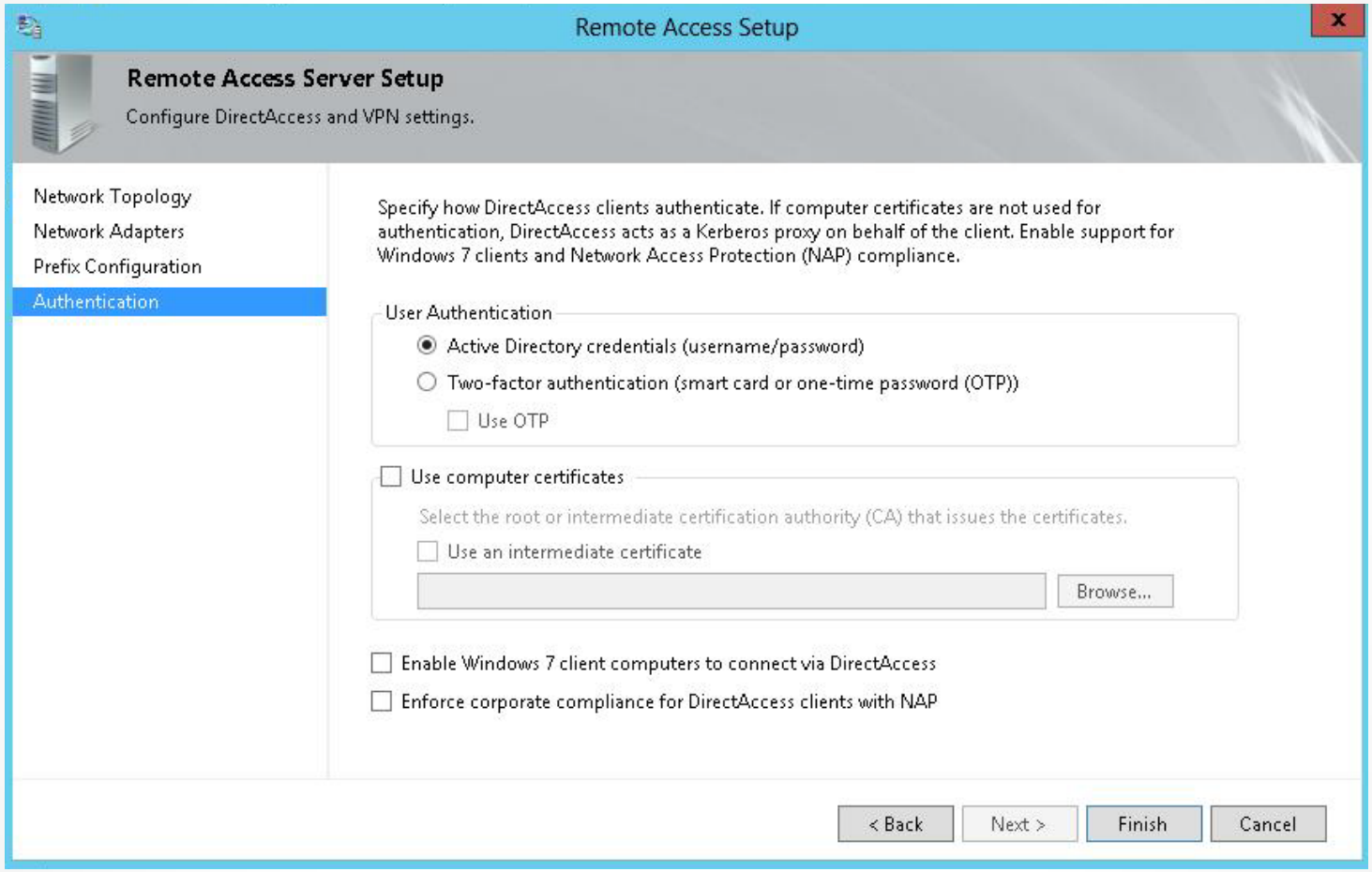
Configuring the network adapters

Configure the DirectAccess Remote Access Server



Specifying the IPv6 prefixes

Configure the DirectAccess Remote Access Server

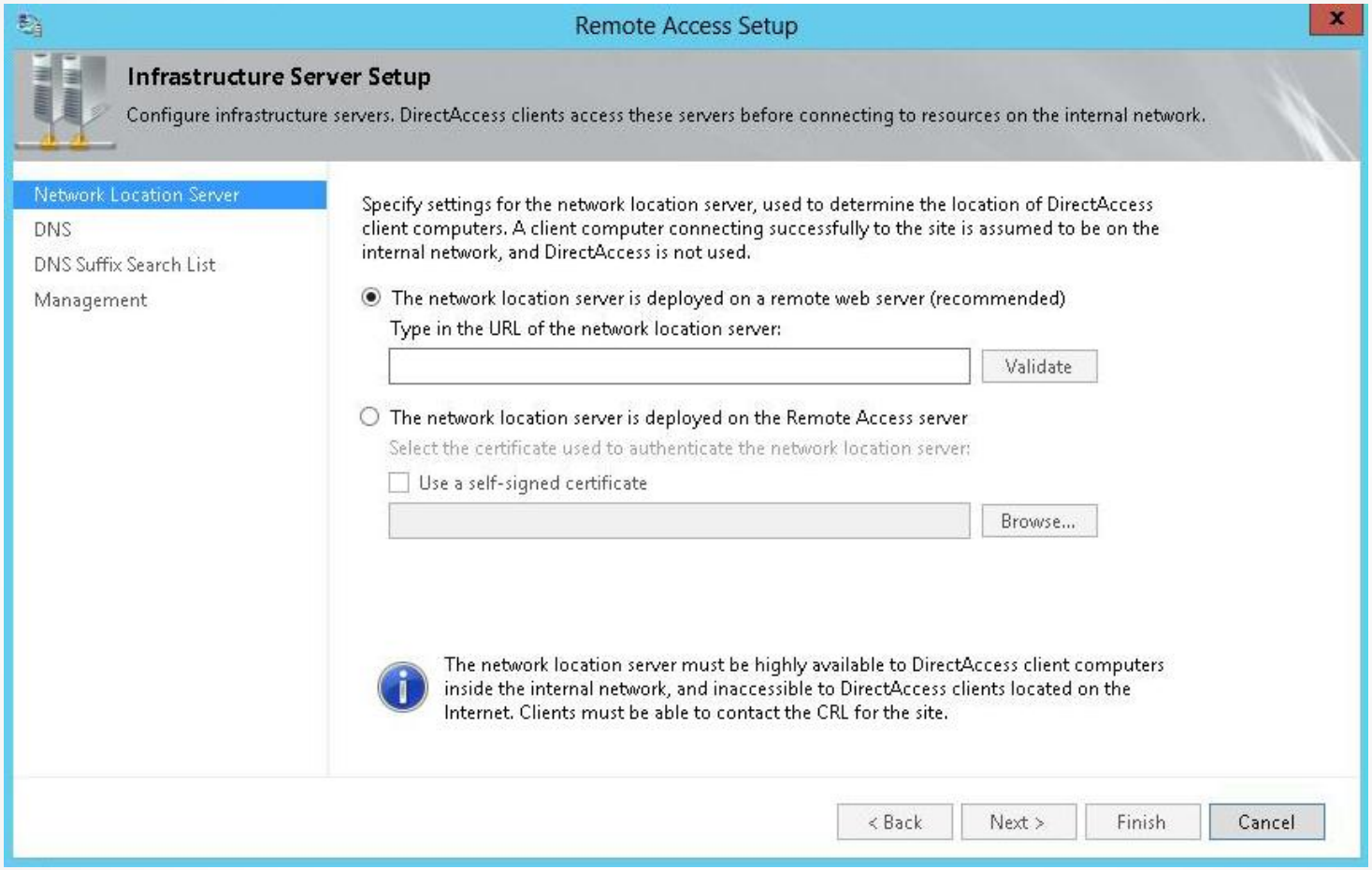


Specifying authentication

Implementing Infrastructure Servers

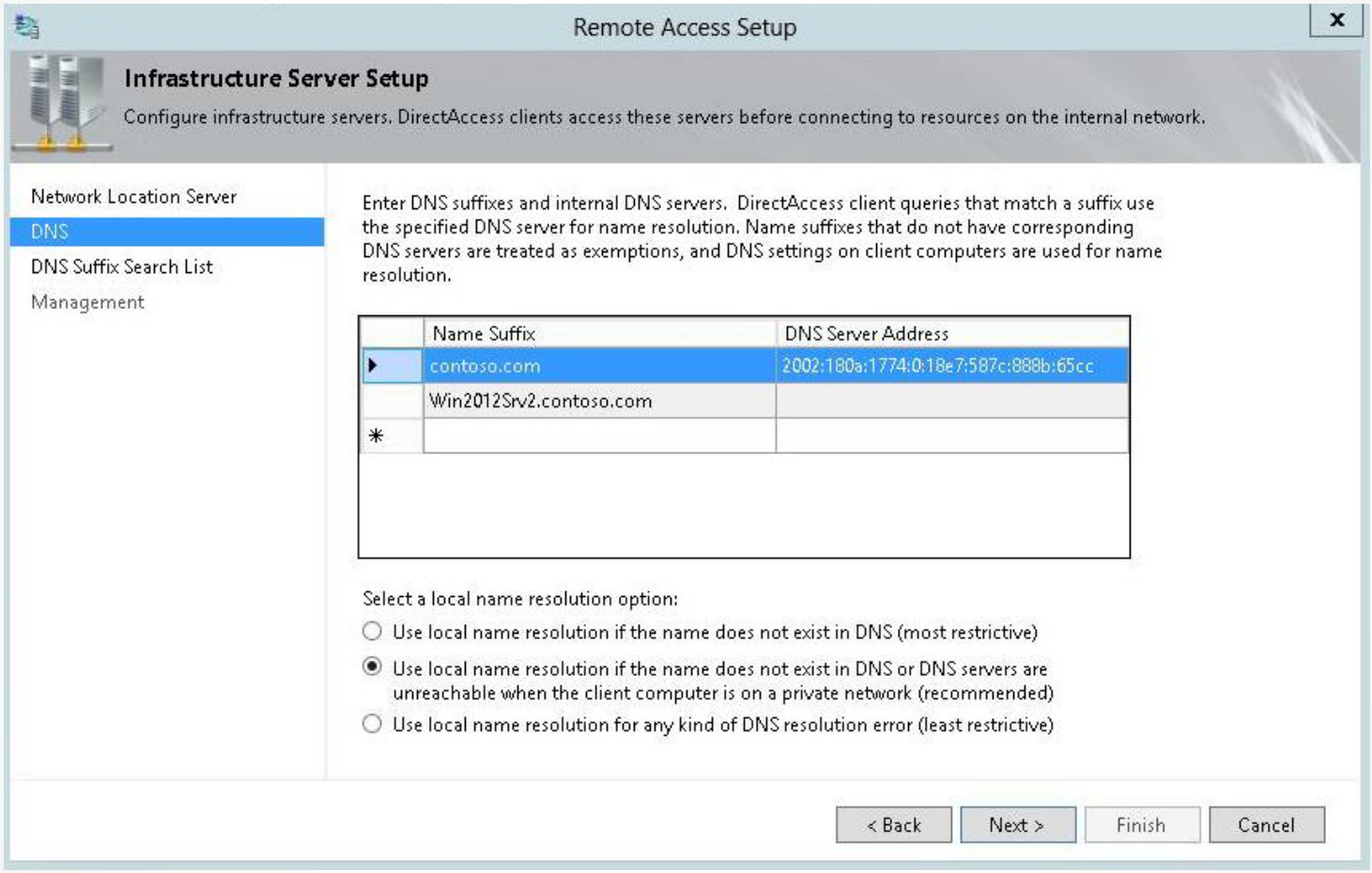
- DirectAccess clients use the ***network location server (NLS)*** to determine their locations.
- To configure an NLS:
  - Install IIS on a Windows server.
  - For a website, bind a name and associate a NLS DNS name to the IP address.
  - Make sure the server is highly available.
- Ensure that DirectAccess clients can correctly detect when they are on the Internet.

Configure the DirectAccess Infrastructure Servers



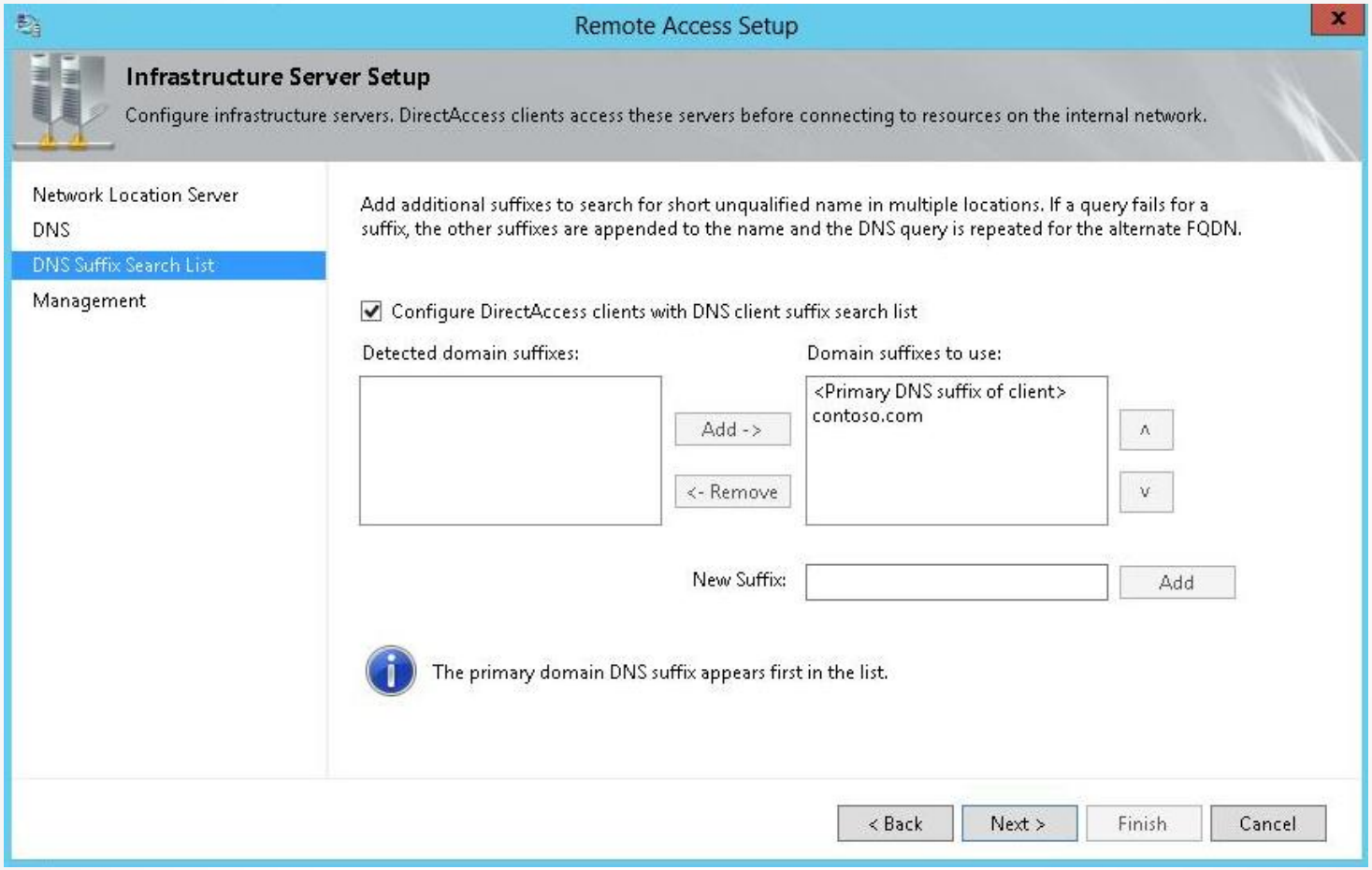
Specifying the Network Location server

Configure the DirectAccess Infrastructure Servers



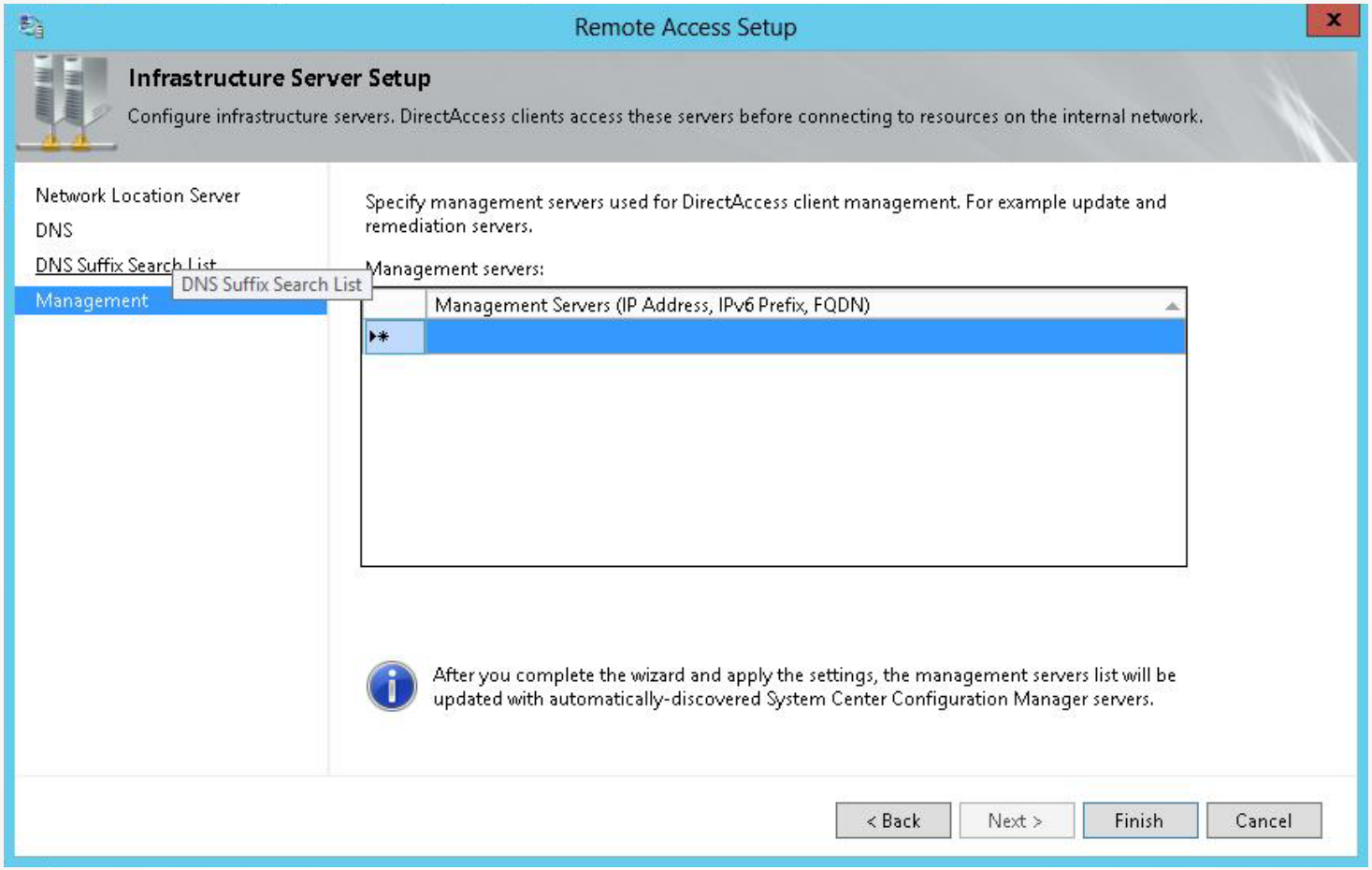
Specifying the DNS servers

Configure the DirectAccess Infrastructure Servers



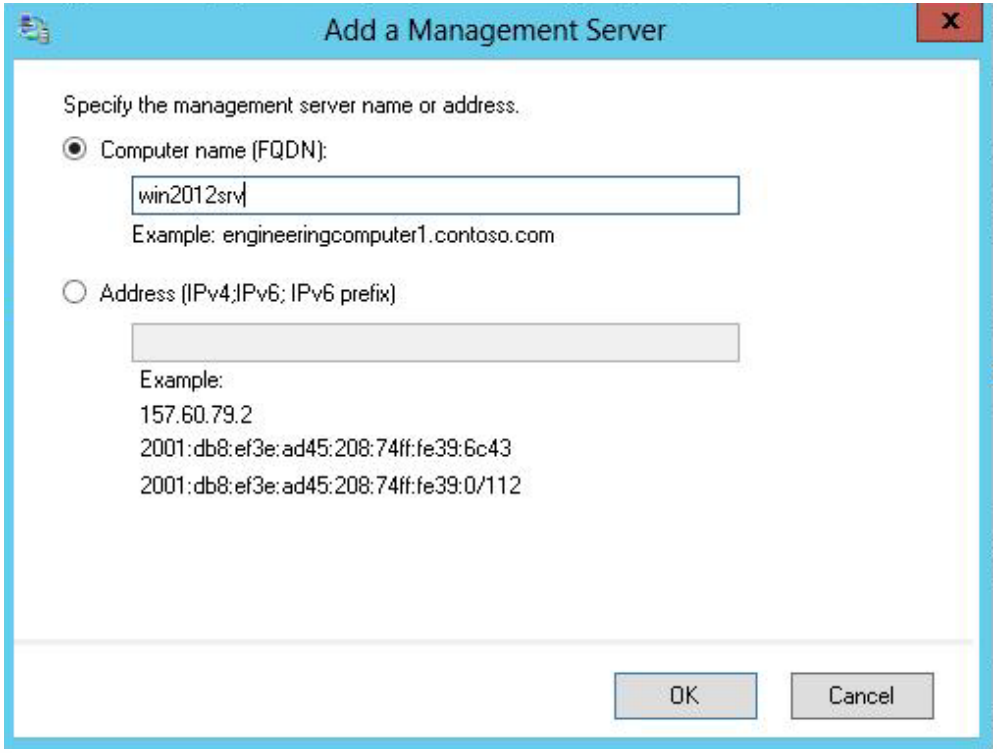
Specifying the DNS Suffix Search List

Configure the DirectAccess Infrastructure Servers



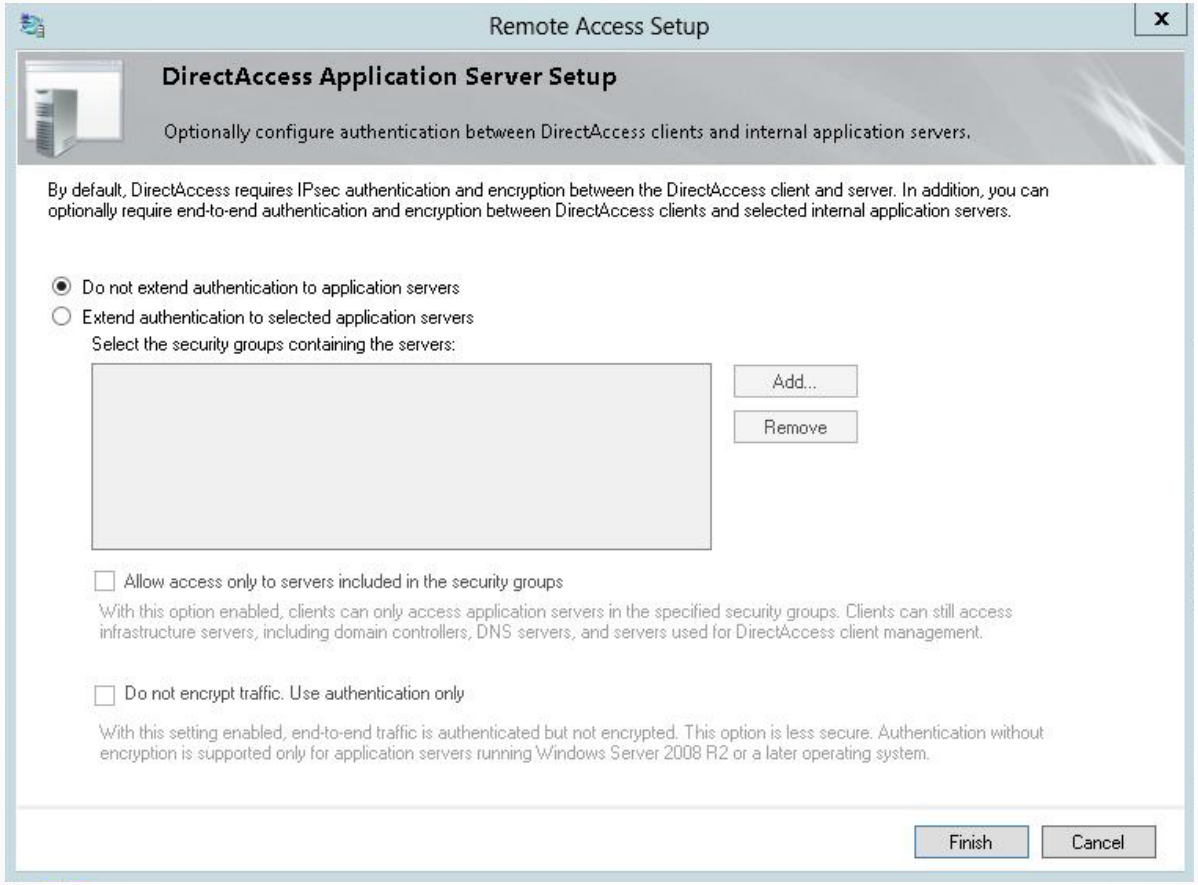
Specifying the management servers

Configure the DirectAccess Infrastructure Servers



Adding a management server

Configure Application Servers for DirectAccess



Specifying the DirectAccess application servers

Configuring DNS for DirectAccess

- DirectAccess requires internal and external DNS.
- DirectAccess requires two external DNS A records:
  - DirectAccess server, such as directaccess.contoso.com
  - Certificate Revocation List (CRL), such as crl.contoso.com
- Internally, DNS needs the DNS records for the NLS server and one for the CRL.

Configuring DNS for DirectAccess

- ISATAP provides a transition between networks that are based on IPv4 to IPv6.
- If you need to use ISATAP, remove ISATAP from the DNS global query block list by executing this command:

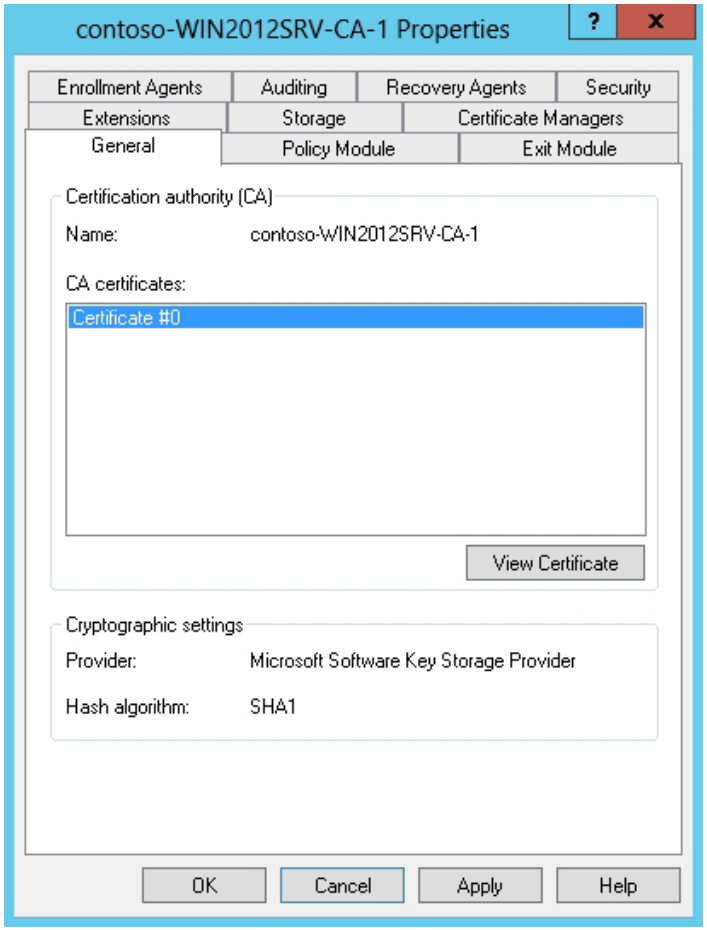
```
dnscmd /config /globalqueryblocklist
isatap
```

Configuring Certificates for DirectAccess

The DirectAccess server requires these certificates:

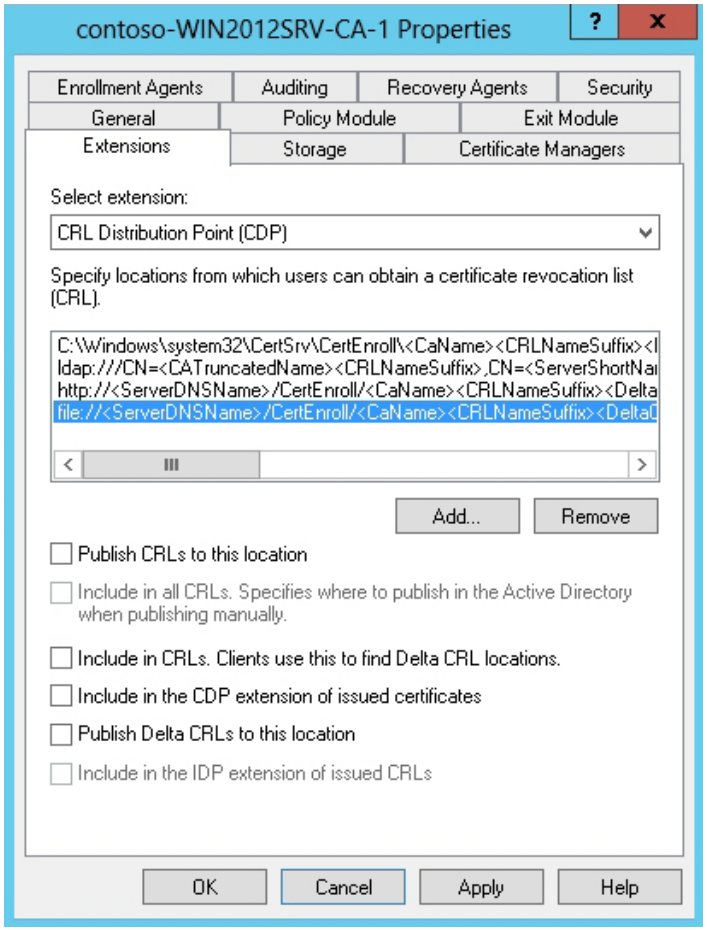
- The IP-HTTPS listener on the DirectAccess server requires a Web site certificate
- The DirectAccess client must be able to contact the server hosting the CRL for the certificate.
- The DirectAccess server requires a computer server to establish the IPsec connections with the DirectAccess clients.

Configure Certificate Requirements



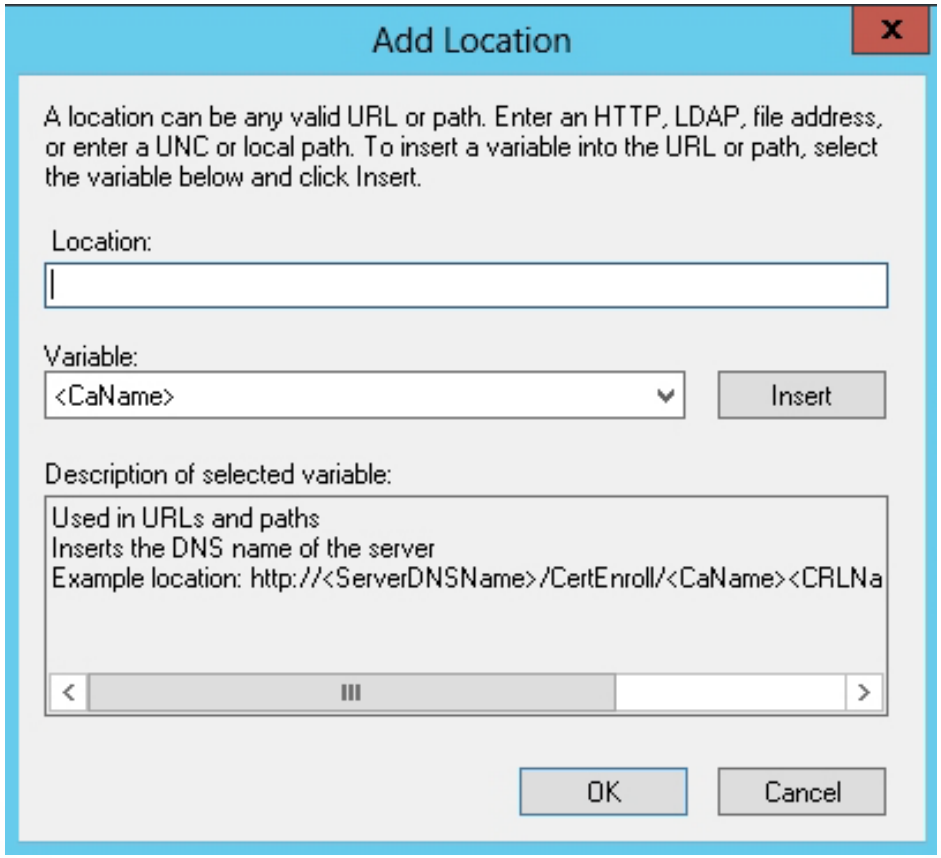
Displaying the CA certificates

Configure Certificate Requirements



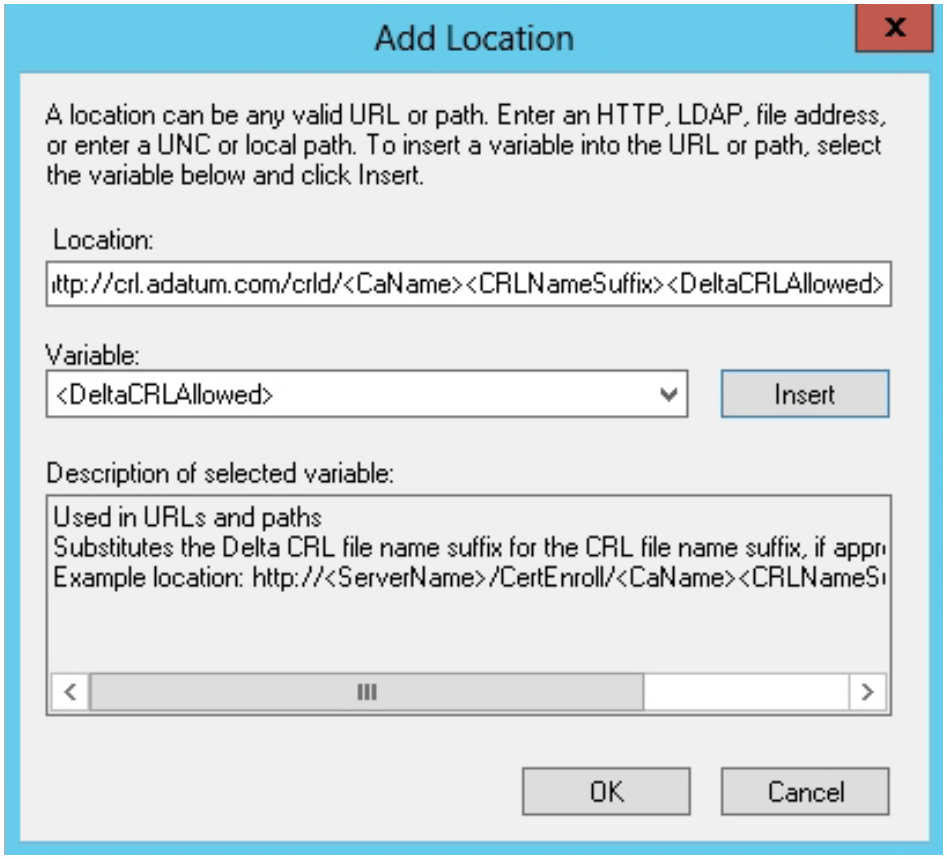
Specifying certificate extensions

Configure Certificate Requirements



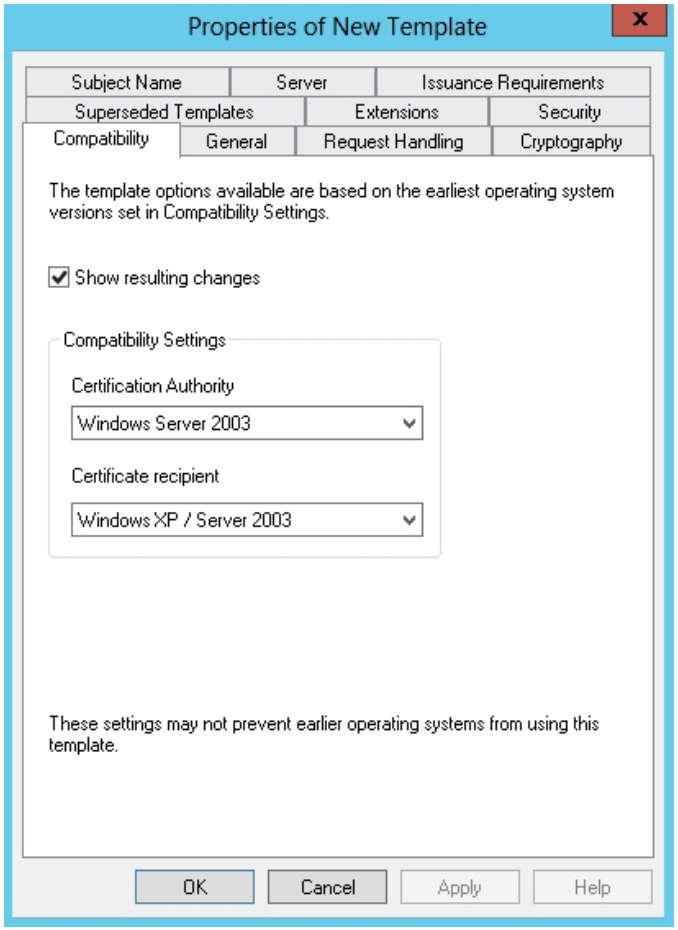
Adding a Location for CRL

Configure Certificate Requirements



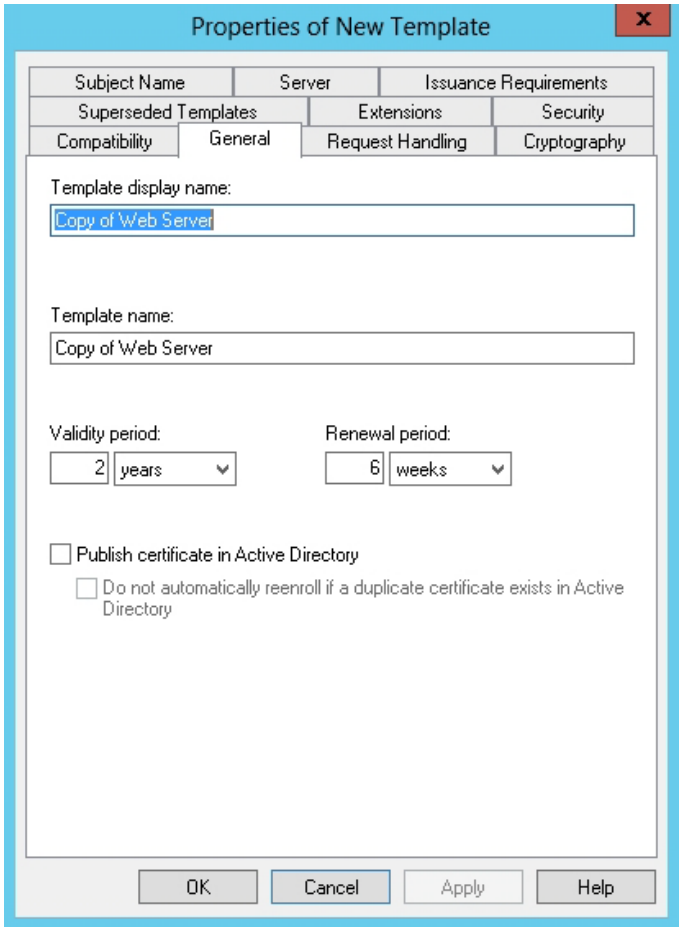
An example location for CRL

Configure Certificate Requirements



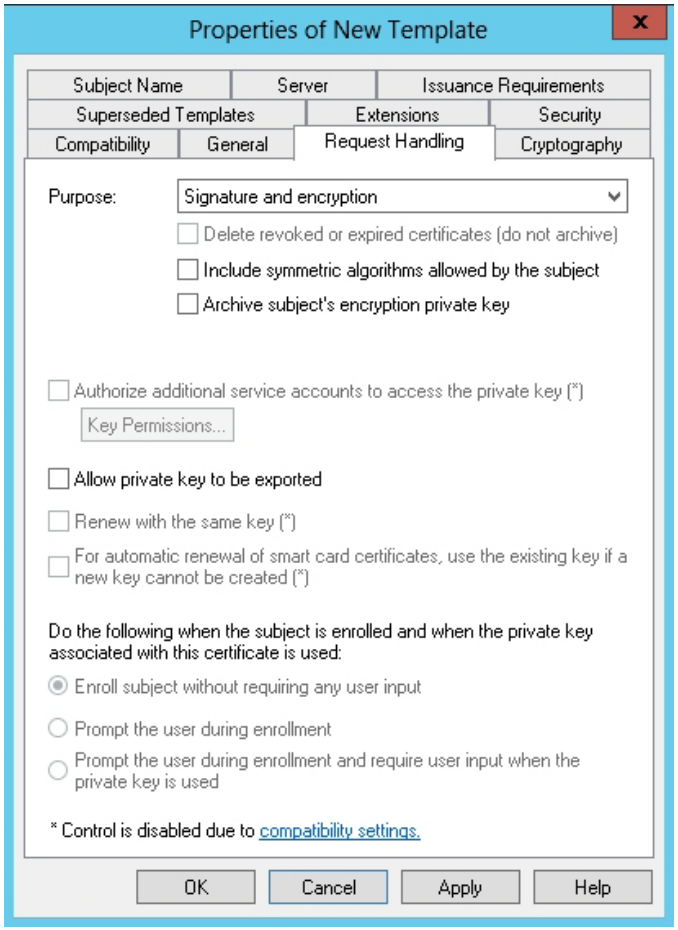
Opening the properties of a certificate template

Configure Certificate Requirements



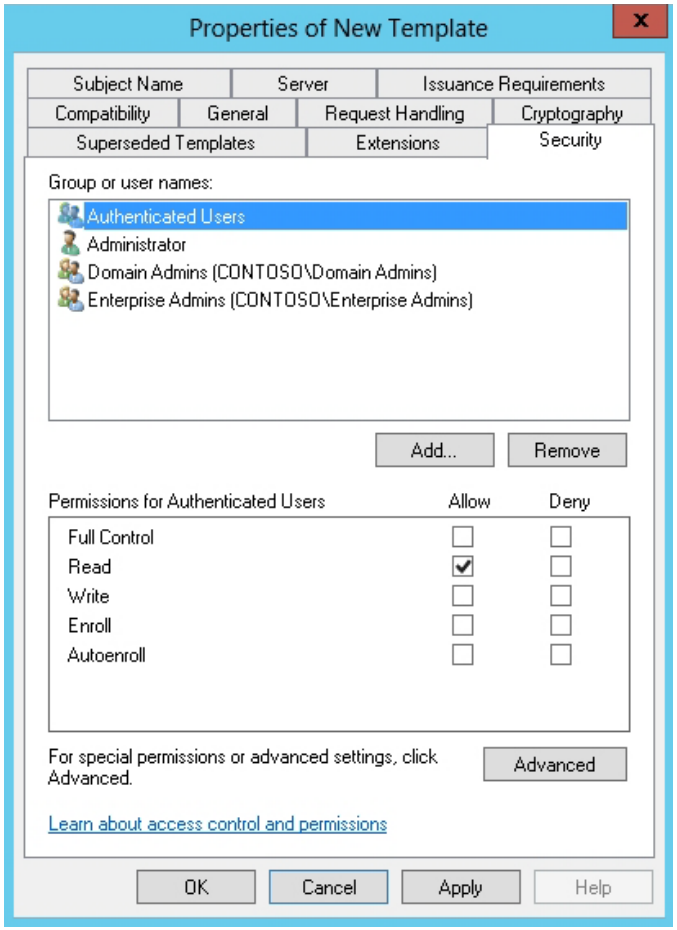
Defining the template display name and template name

Configure Certificate Requirements



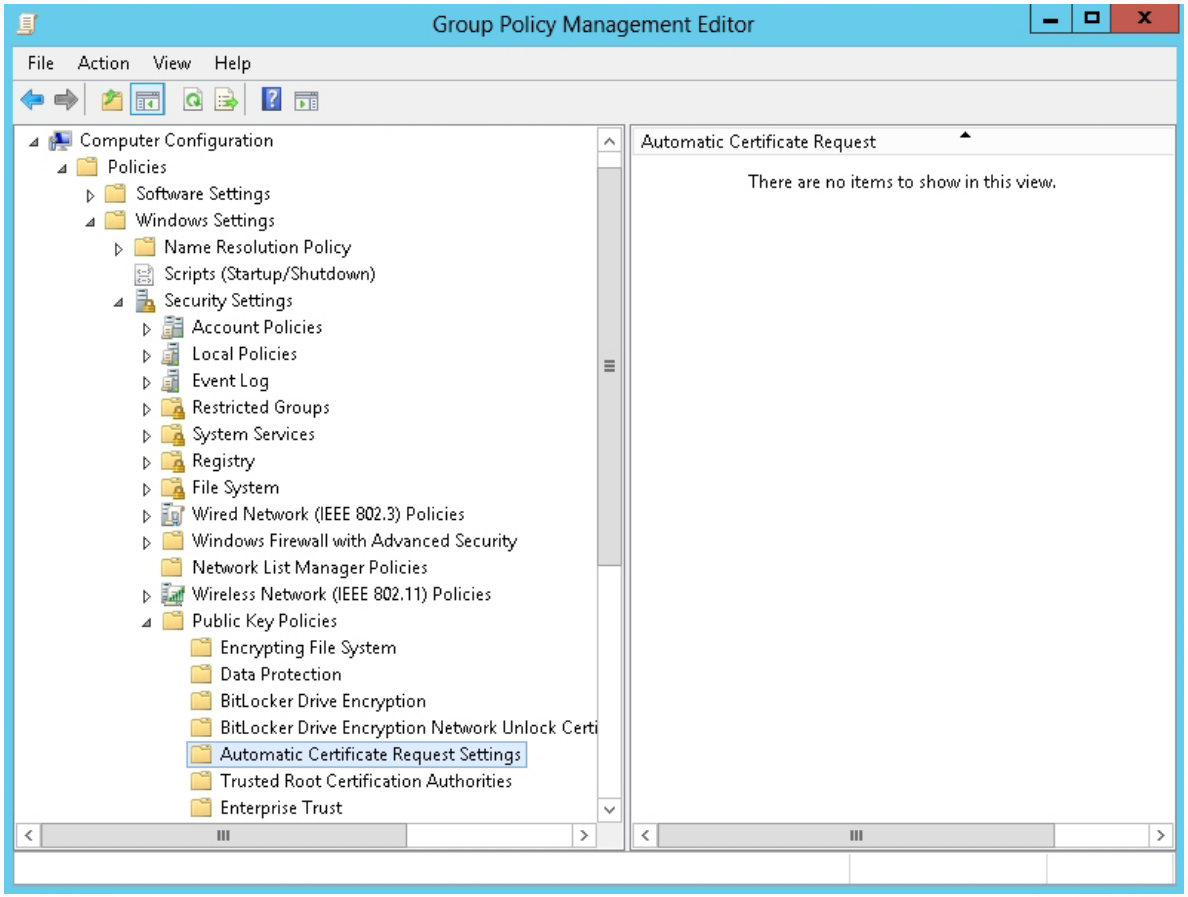
Specifying the purpose of the certificate

Configure Certificate Requirements



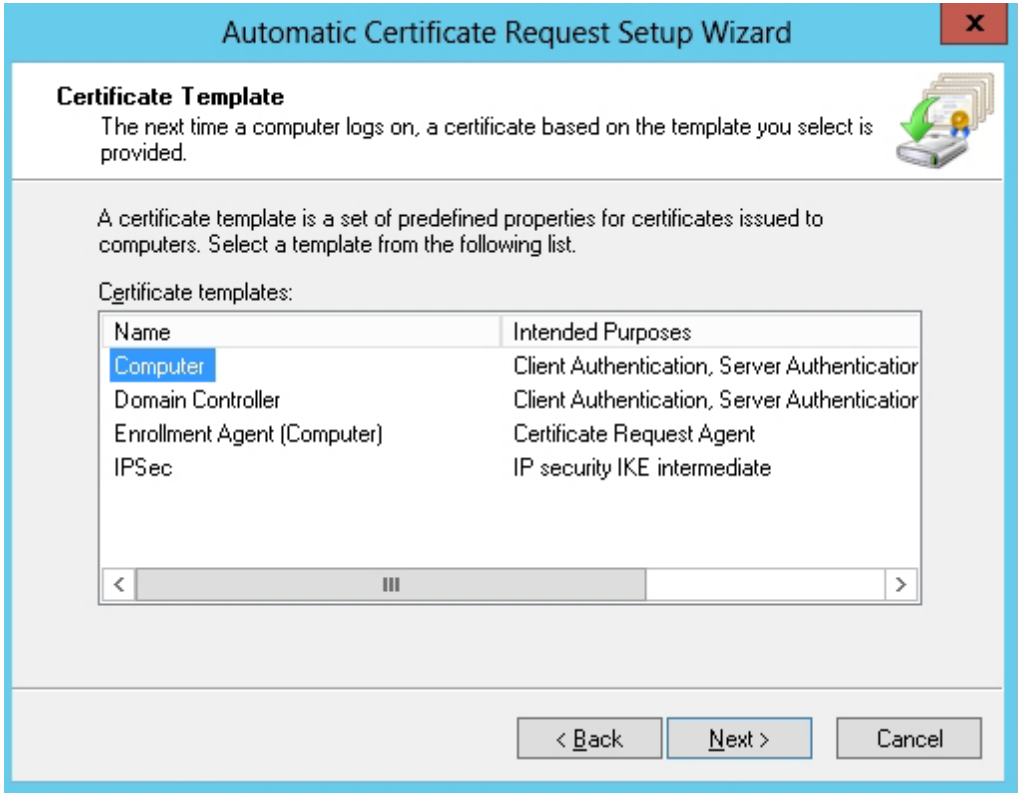
Specifying the permissions assigned to the certificate template

Configure Certificate Requirements



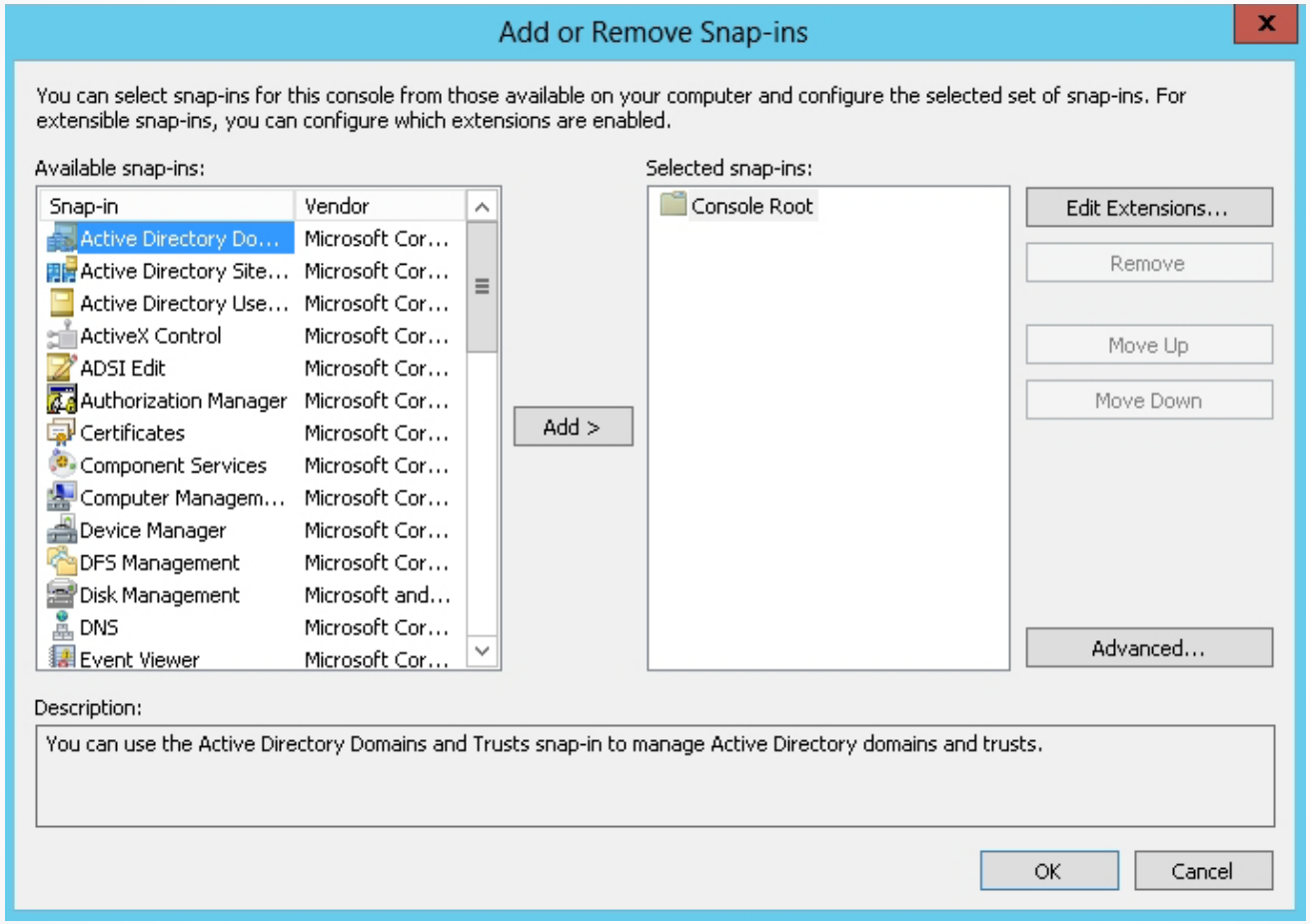
Viewing the Public Key policies

Configure Certificate Requirements



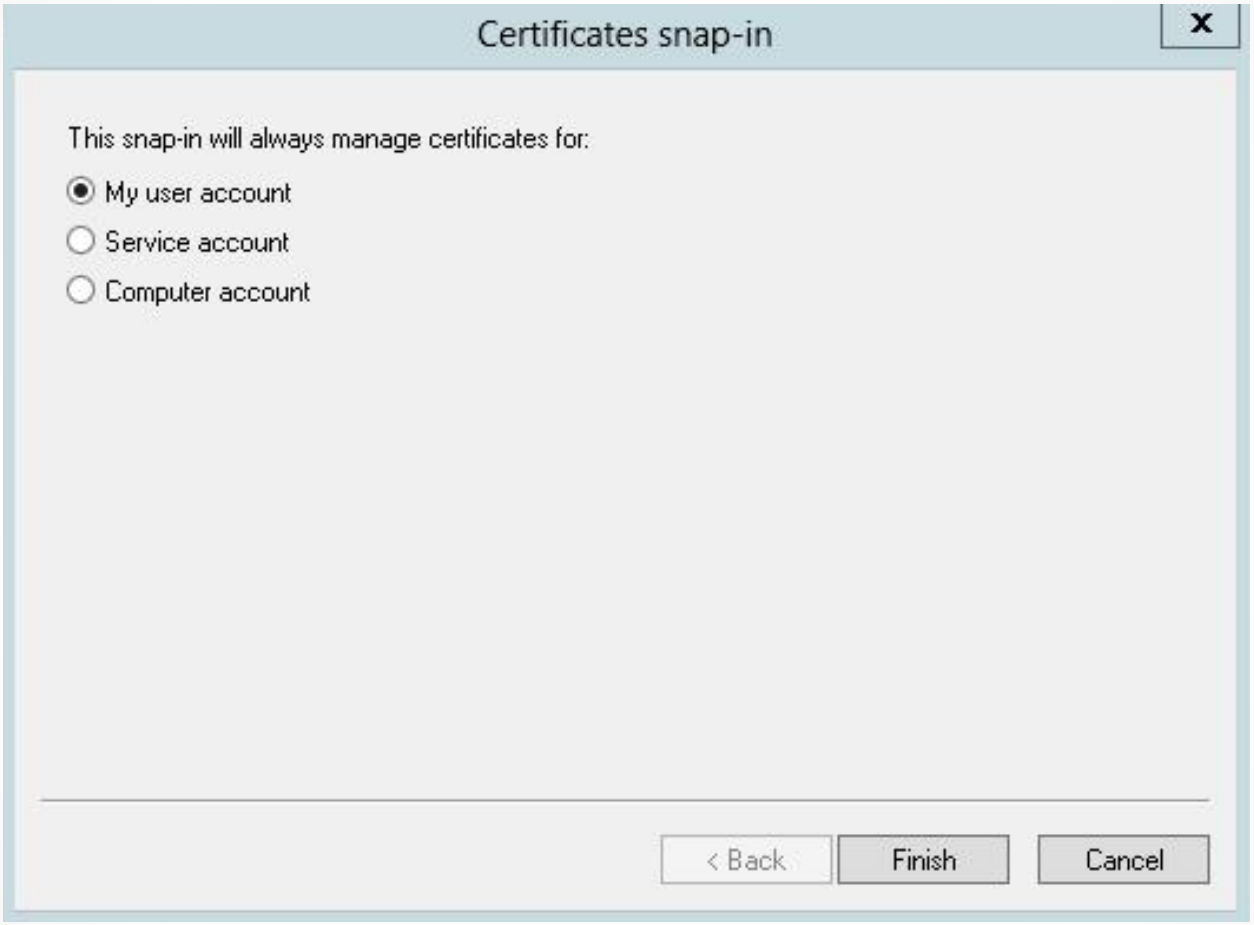
Specifying which certificates are automatically requested

Install a Digital Certificate on the Network Locator Server



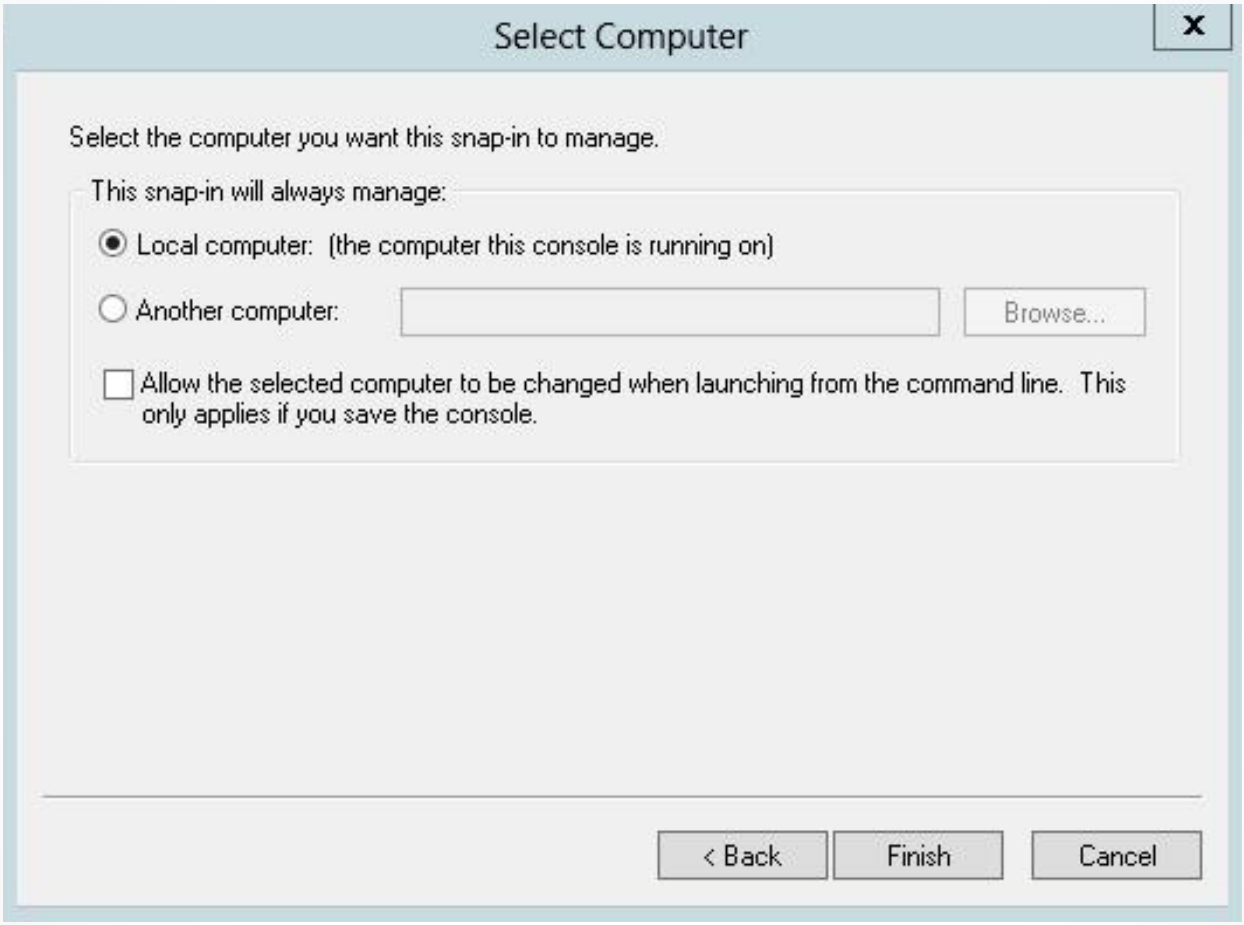
Opening the Add or Remove Snap-ins dialog box

Install a Digital Certificate on the Network Locator Server



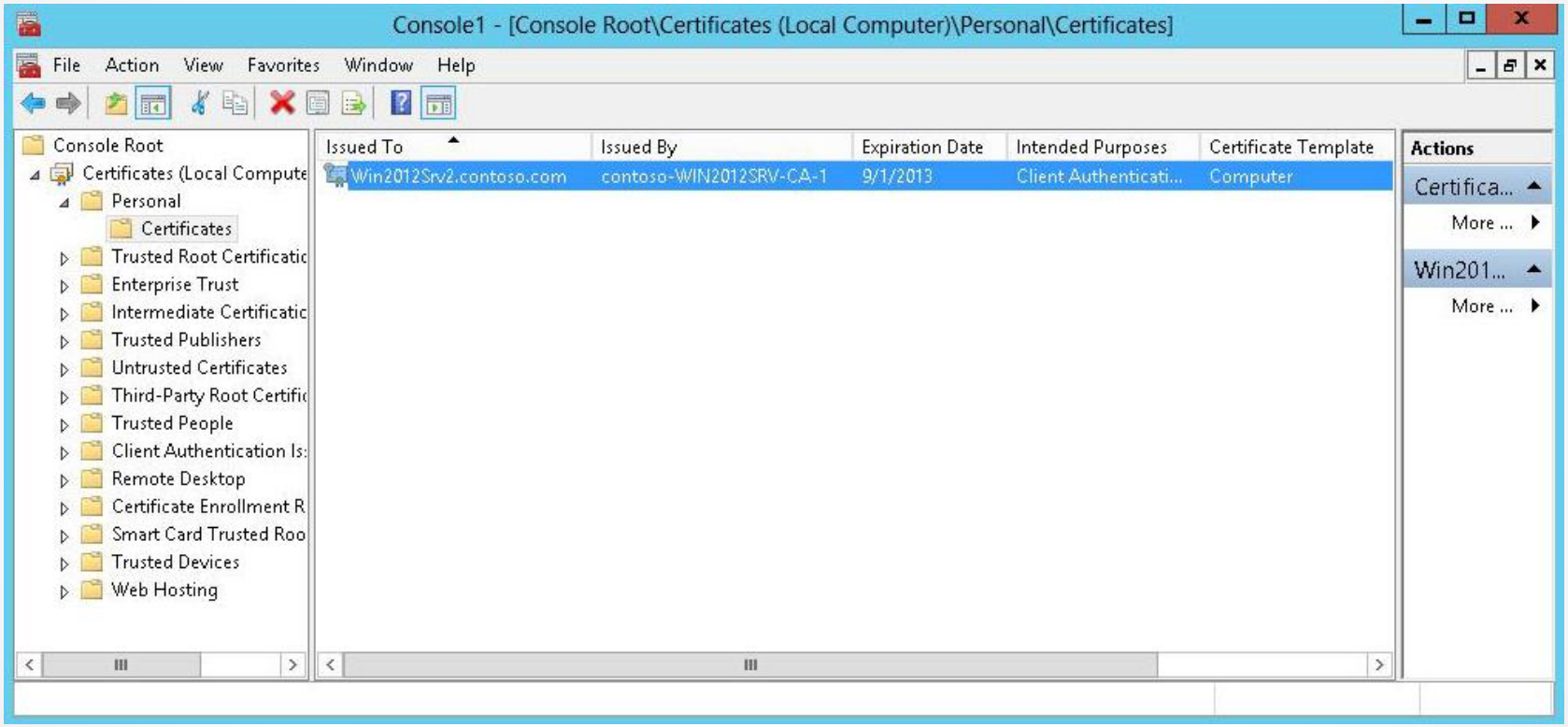
Specifying which certificates to manage

Install a Digital Certificate on the Network Locator Server



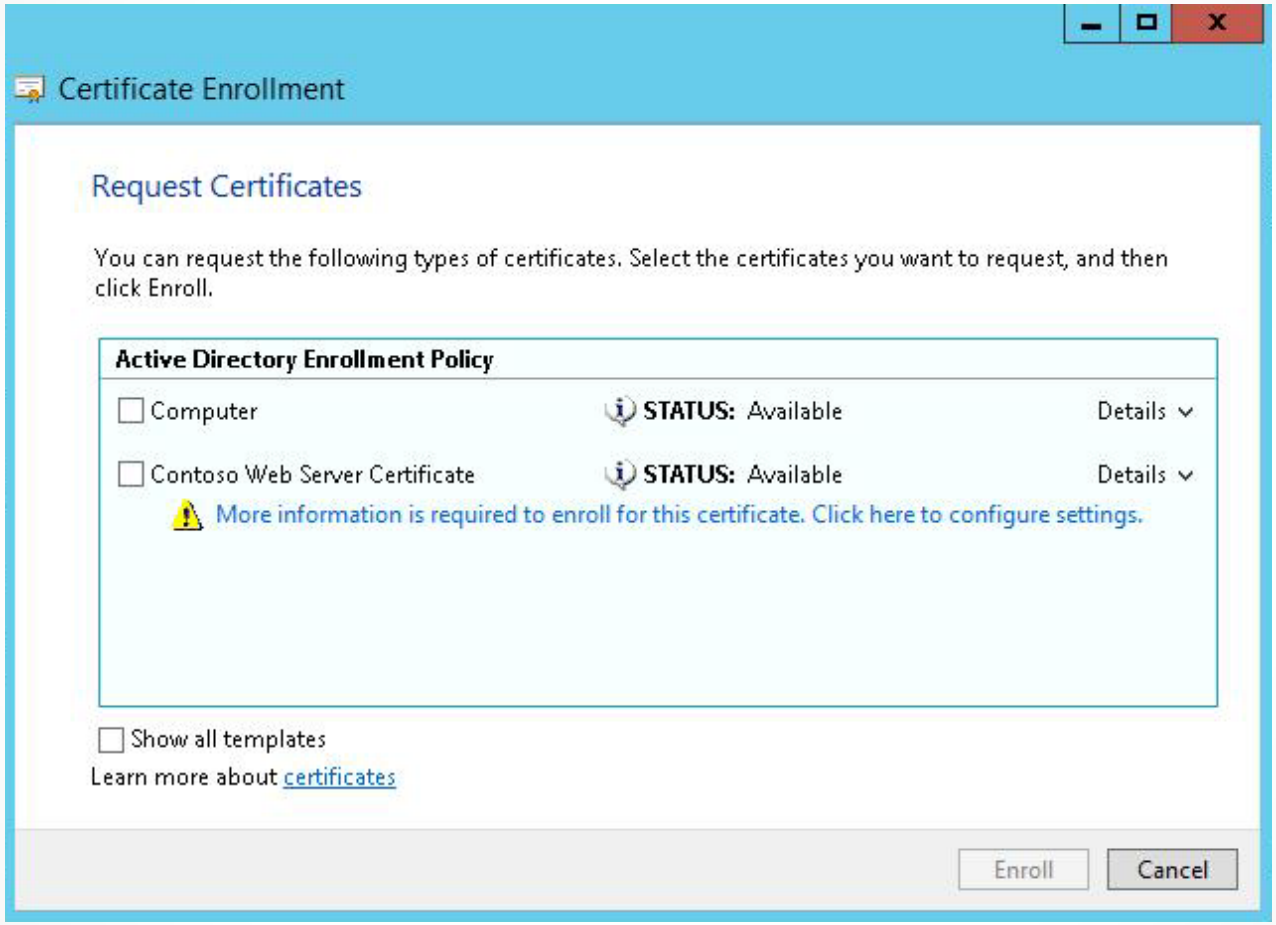
Selecting which computer to connect to

Install a Digital Certificate on the Network Locator Server



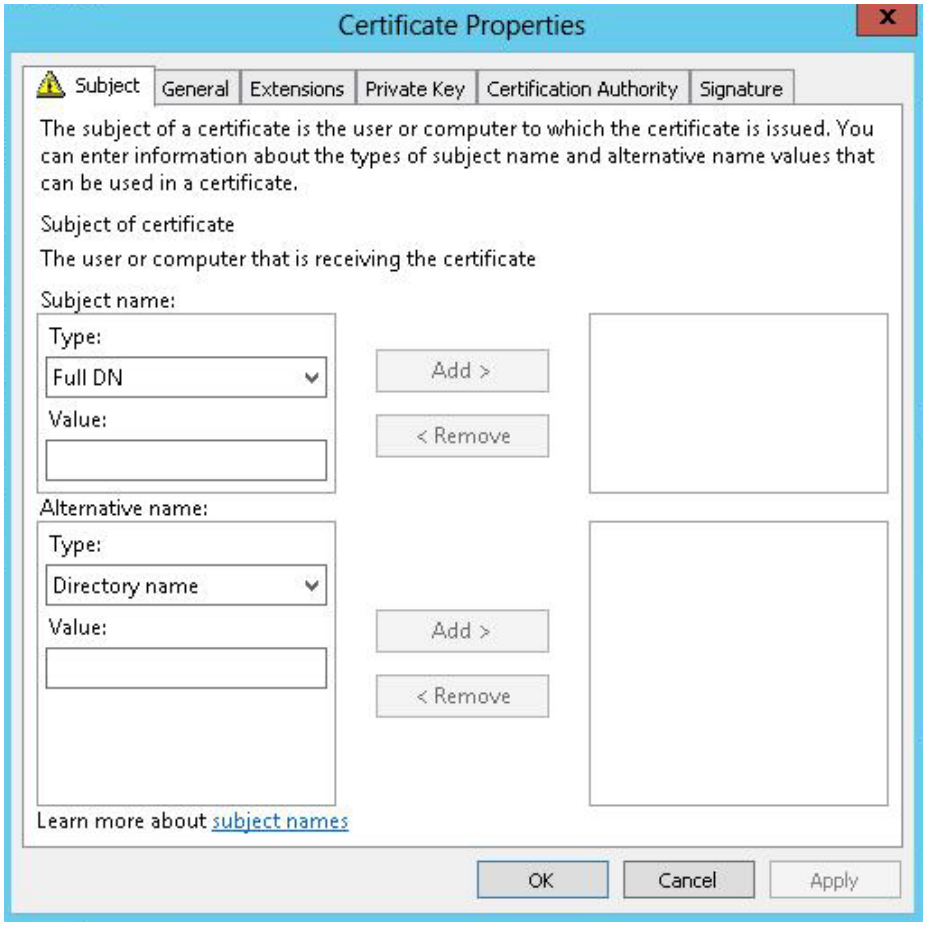
Viewing the computer certificate

Install a Digital Certificate on the Network Locator Server



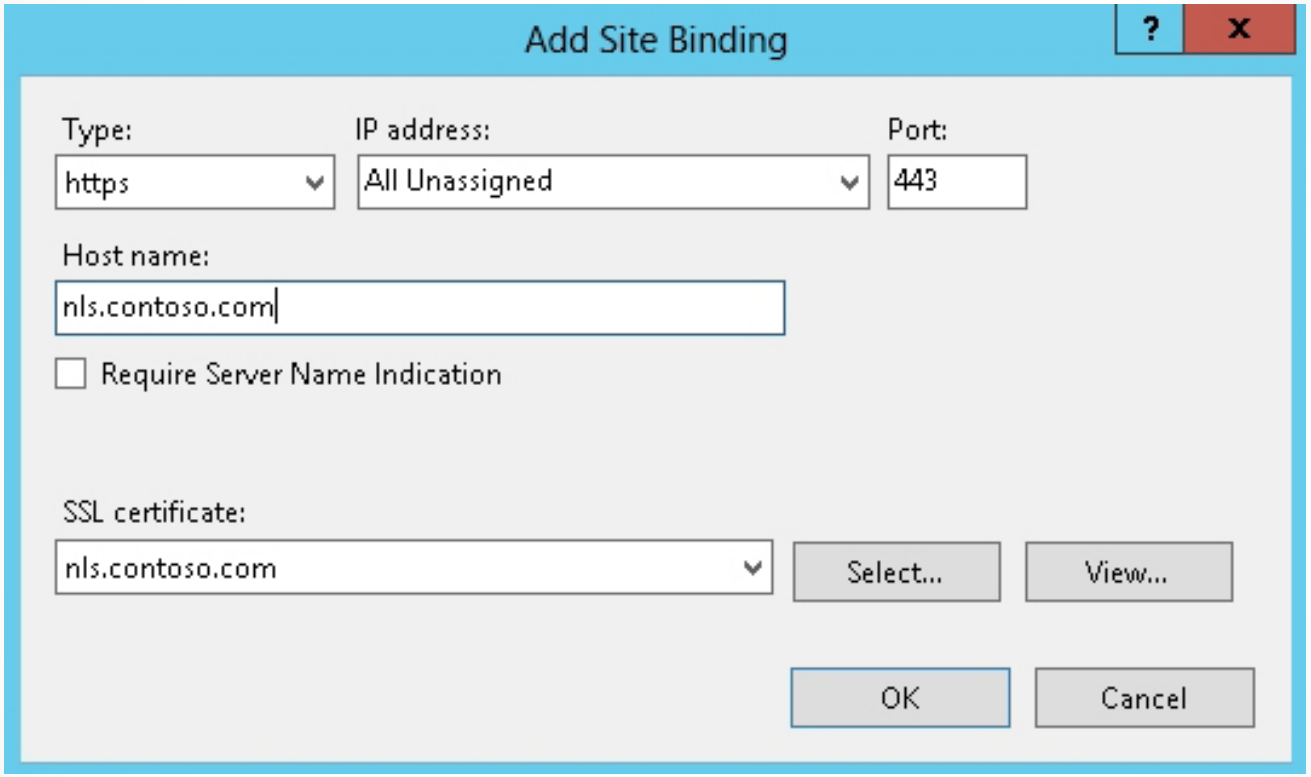
Requesting a certificate

Install a Digital Certificate on the Network Locator Server



Specifying the subject of a certificate

Install a Digital Certificate on the Network Locator Server



Configuring an IIS site binding

Troubleshooting DirectAccess

- The DirectAccess client computer must run Windows 8, Windows 7 Ultimate, or Windows 7 Enterprise edition.
- The DirectAccess client computer must be a member of an Active Directory Domain Services (AD DS) domain and its computer account must be a member of one of the security groups configured with the DirectAccess Setup Wizard.
- The DirectAccess client computer must have received computer configuration Group Policy settings for DirectAccess.
- The DirectAccess client must have a global IPv6 address, which should begin with a 2 or 3.

Troubleshooting DirectAccess

- The DirectAccess client must be able to reach the IPv6 addresses of the DirectAccess server.
- The DirectAccess client on the Internet must correctly determine that it is not on the intranet. You can type the `netsh dnsclient show state` command to view the network location displayed in the Machine Location field (outside corporate network or inside corporate network).
- Use the `netsh namespace show policy` command to show the NRPT rules as configured on the group policy.
- Use the `netsh namespace show effectivepolicy` command to determine the results of network location detection and the IPv6 addresses of the intranet DNS servers.

Troubleshooting DirectAccess

- The DirectAccess client must not be assigned the domain firewall profile.
- The DirectAccess client must be able to reach the organization's intranet DNS servers using IPv6. You can use Ping to attempt to reach the IPv6 addresses of intranet servers.
- The DirectAccess client must be able to communicate with intranet servers using application layer protocols. If File and Printer Sharing is enabled on the intranet server, test application layer protocol access by typing net view \\IntranetFQDN.
- Use the DirectAccess Connectivity Assistant on computers running Windows 7 and Network Connectivity Assistant on computers running Windows 8 to determine the intranet connectivity status and to provide diagnostic information.

Lesson Summary

- DirectAccess provides seamless intranet connectivity to DirectAccess client computers when they are connected to the Internet; connections are automatically established and they provide always-on seamless connectivity.
- The Name Resolution Policy Table (NRPT) is used to determine the behavior of the DNS clients when issuing queries and processing so that internal resources are not exposed to the public via the Internet, and to separate traffic that is not DirectAccess Internet traffic from traffic that is.
- To use DirectAccess, clients must be Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, or Windows Server 2012.

Lesson Summary

- In Windows 8, the DCA was replaced by the Network Connectivity Assistant (NCA).
- The DirectAccess Connectivity Assistant (DCA) provides tools to help users reconnect if a problem occurs and helps with diagnostics used by the help desk. It is also used to detect whether one-time passwords (OTP) are required and helps your system determine whether it is connected to the intranet or the Internet.
- DirectAccess clients use the network location server (NLS) to determine their location. NLS is an internal web server.
- Before deploying DirectAccess, you need to make sure that you have IPv6 and any transitional IPv6 technologies in place, a certificate server, and external and internal DNS entries.