

Lesson 11: Configuring DirectAccess

MOAC 70-411: Administering
Windows Server 2012

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

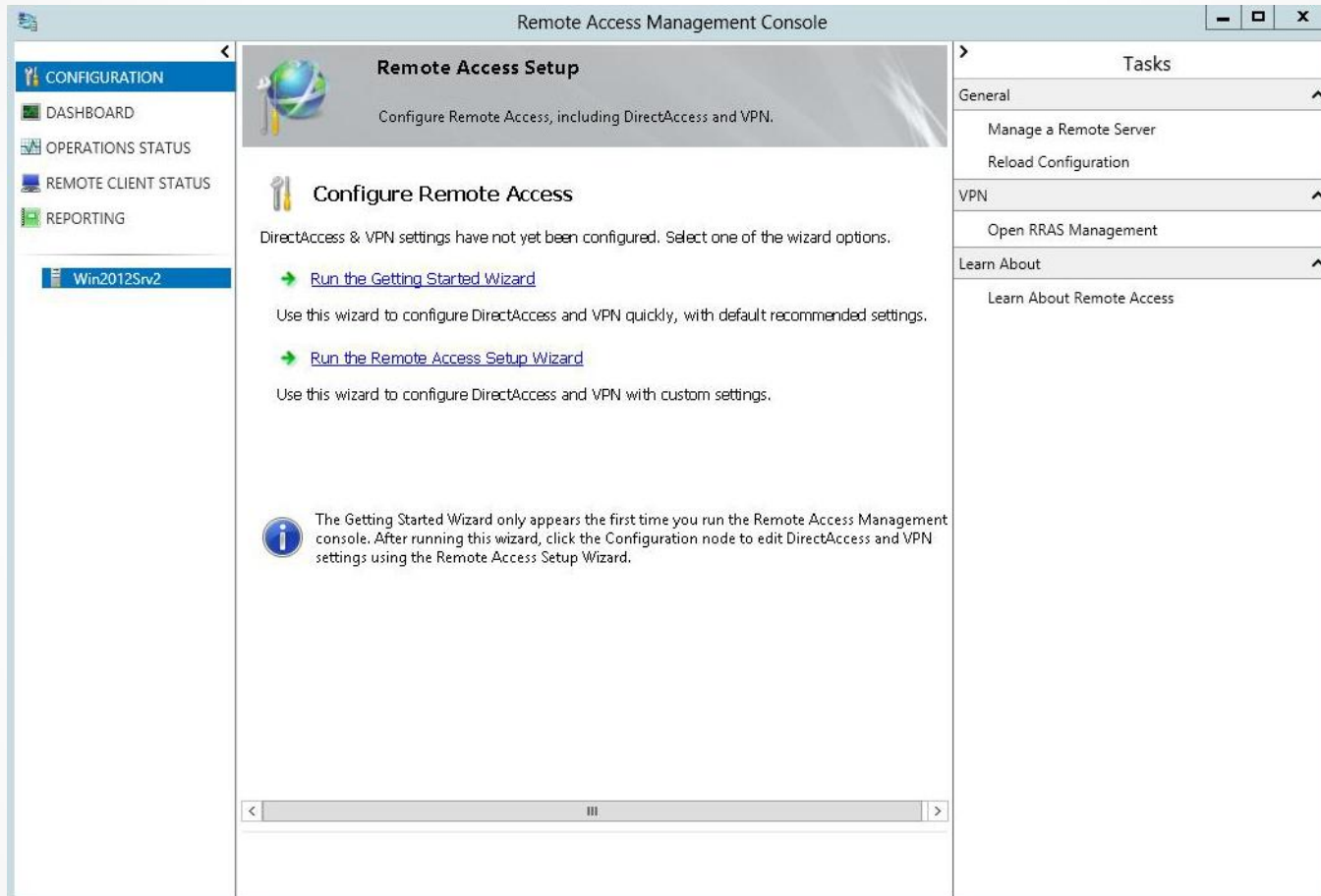
- Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, or Windows Server 2012

Client must be joined to an Active Directory domain

Running the DirectAccess Getting Started Wizard

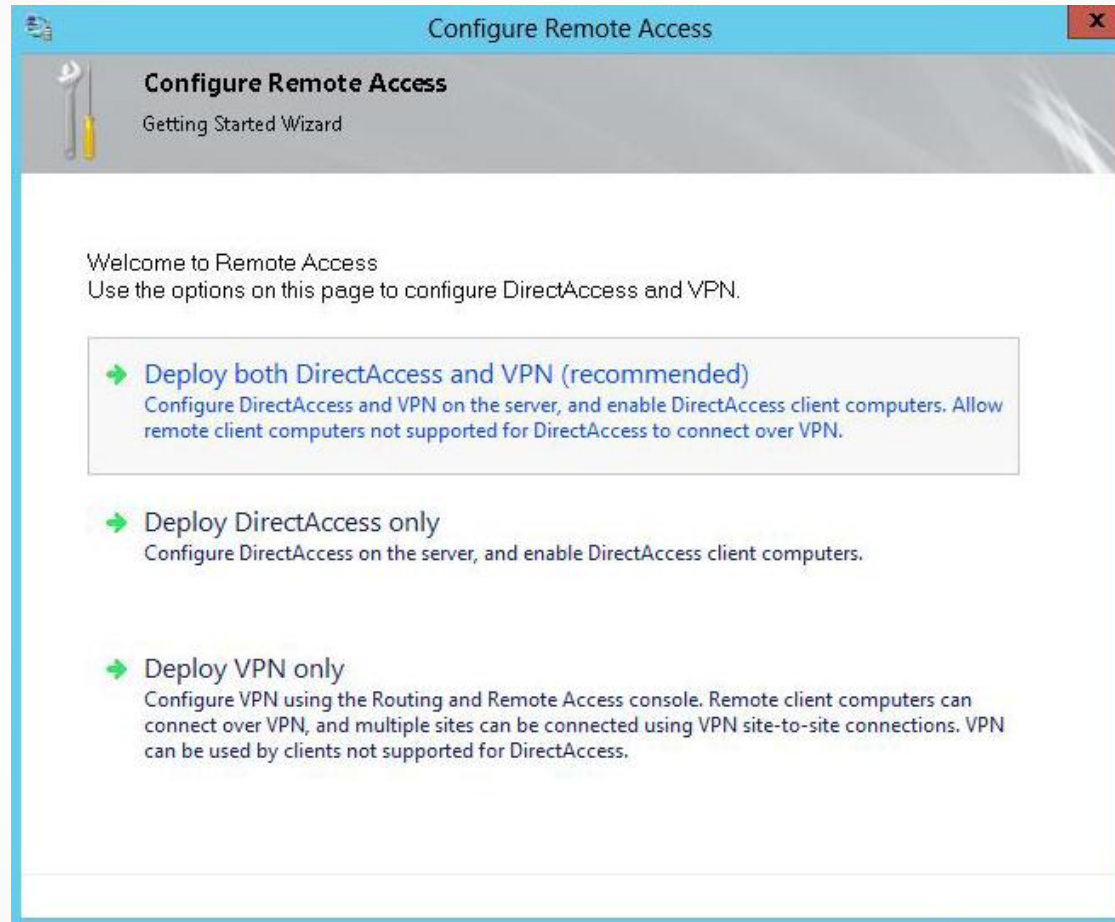
- Configures DirectAccess
- Can run from Remote Access Management console

Run the DirectAccess Getting Started Wizard



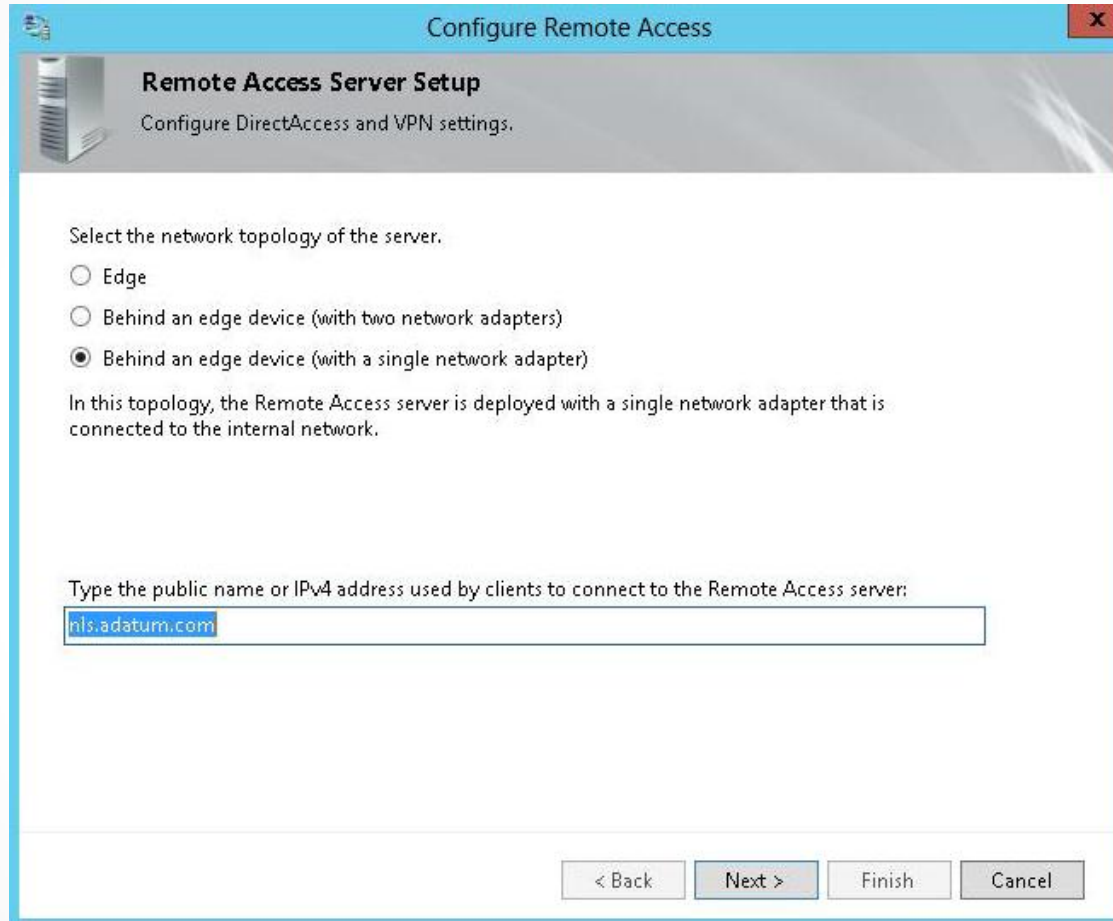
Opening the Remote Access Management console

Run the DirectAccess Getting Started Wizard



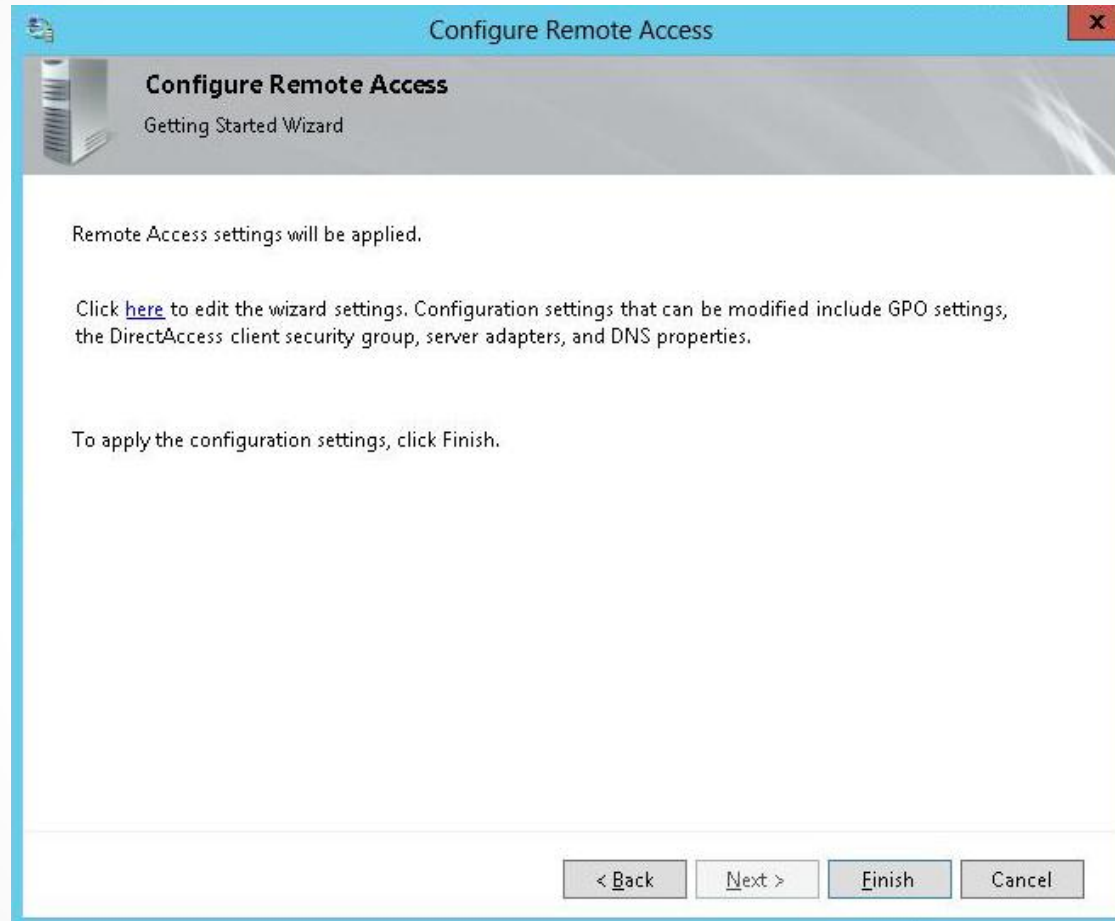
Starting the Configure Remote Access Wizard

Run the DirectAccess Getting Started Wizard



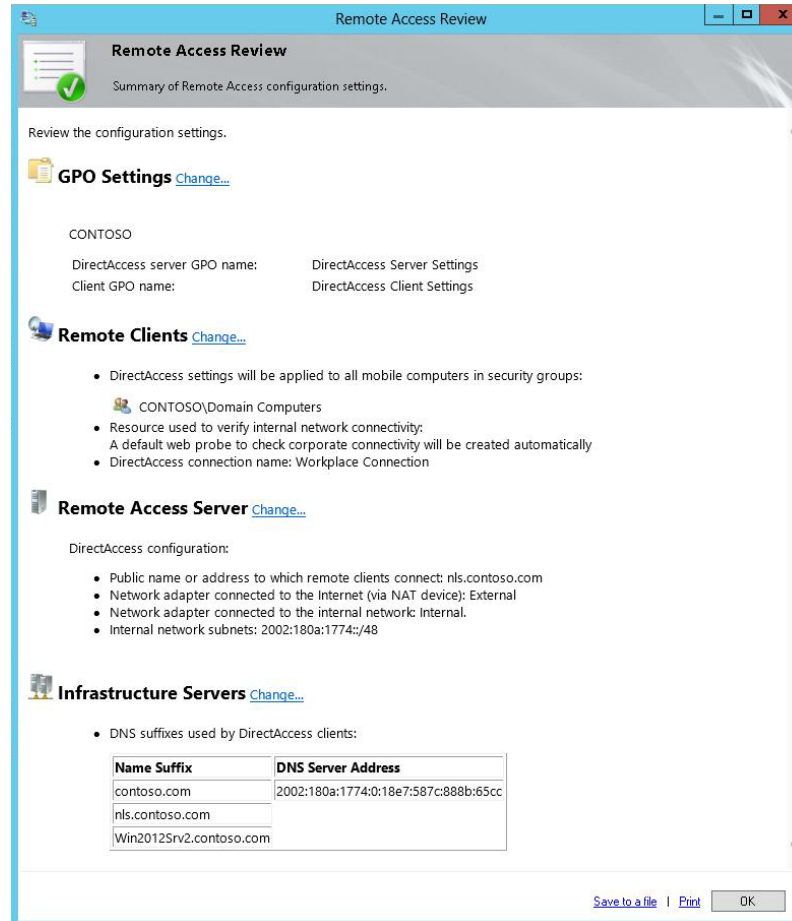
Selecting a topology on the Configure DirectAccess and VPN Settings page

Run the DirectAccess Getting Started Wizard



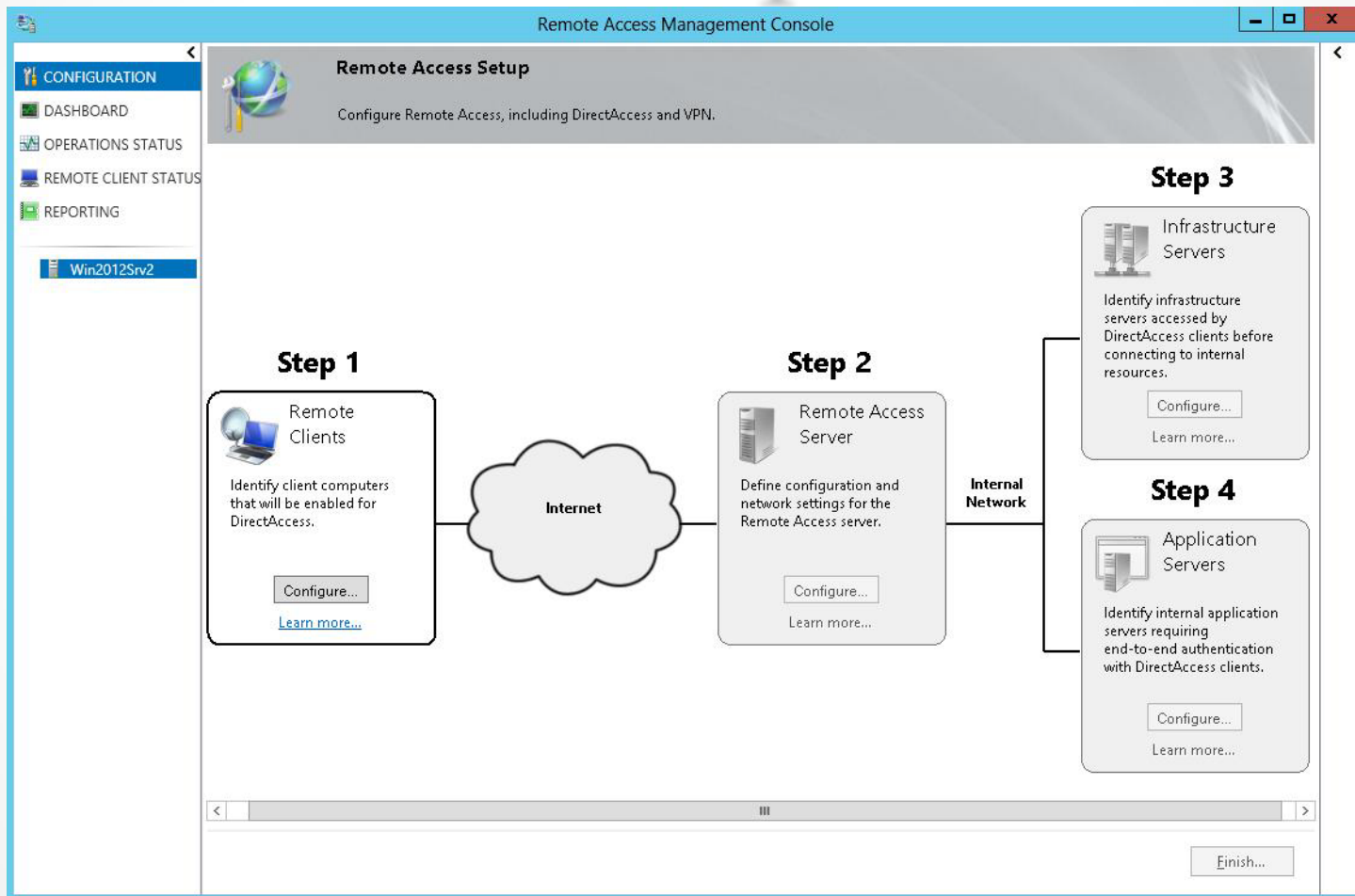
Finishing the Getting Started Wizard

Run the DirectAccess Getting Started Wizard



Viewing the settings applied using the Getting Started Wizard

Running the Remote Access Setup Wizard



Implementing Client Configuration

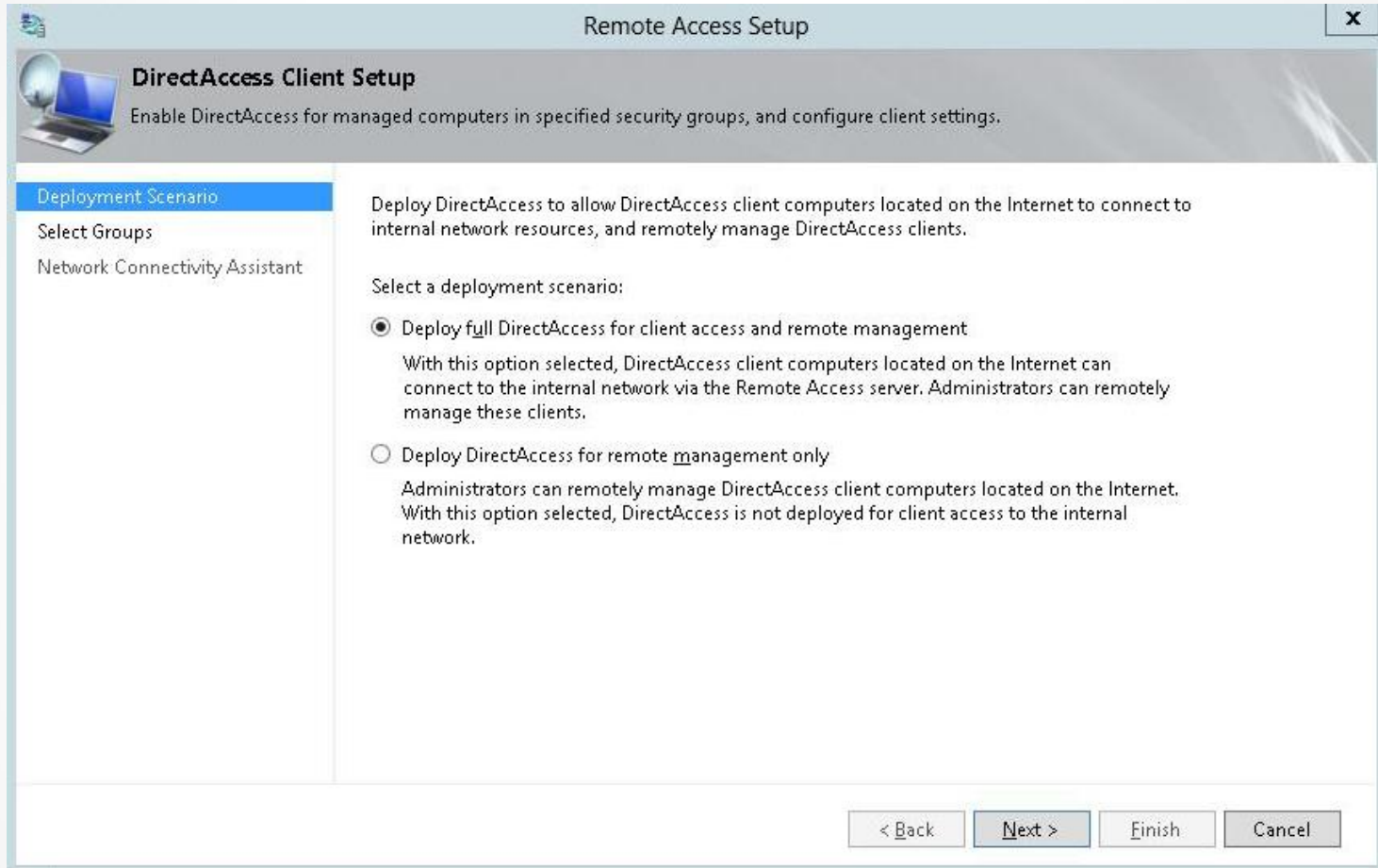
DirectAccess Connectivity Assistant (DCA)

- Windows 7 and Windows Server 2008 R2

Network Connectivity Assistant (NCA)

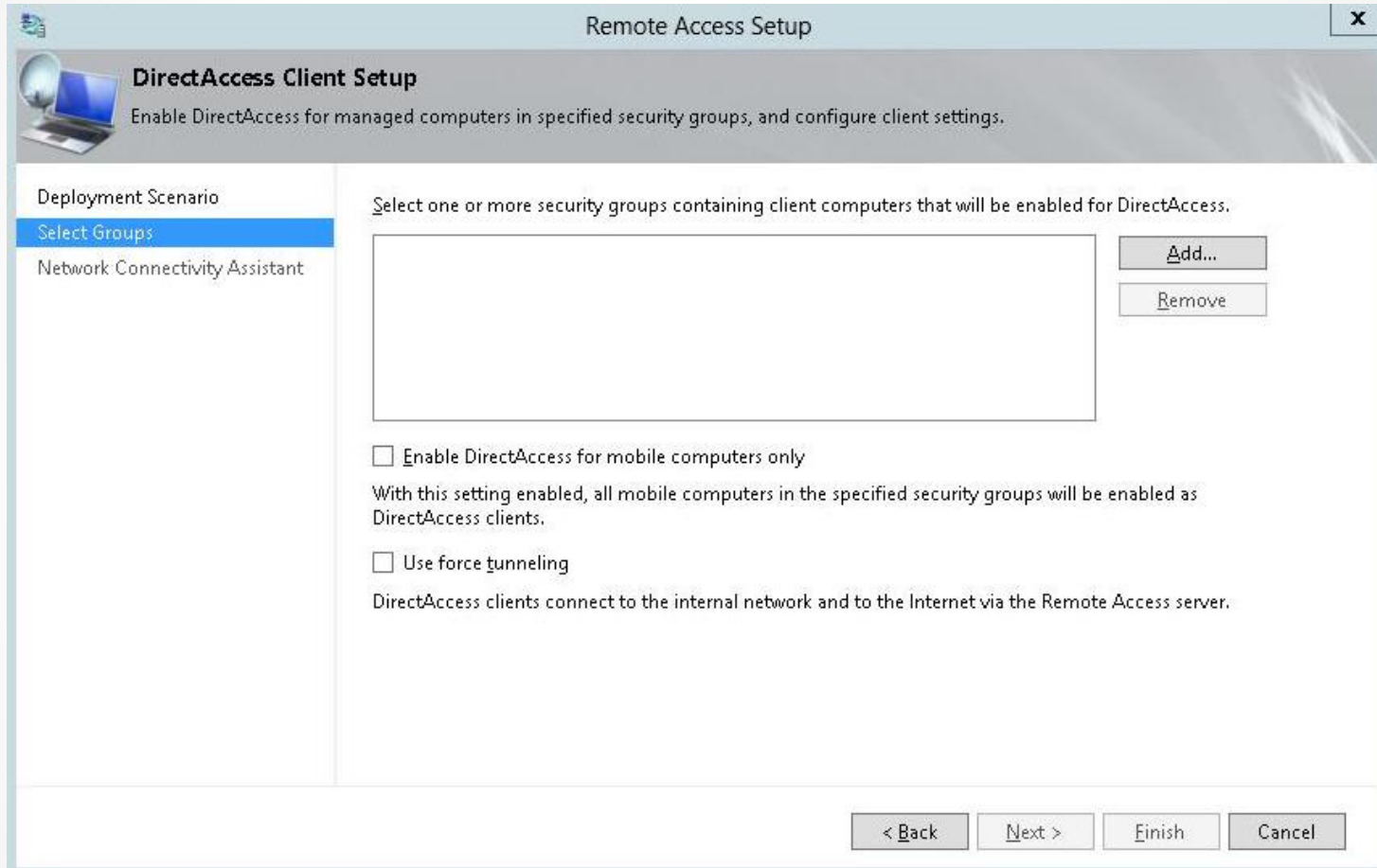
- Windows 8

Configure Remote Clients



Specifying the deployment scenario

Configure Remote Clients



Selecting client groups

Configure Remote Clients

The screenshot shows the 'Remote Access Setup' window with the 'DirectAccess Client Setup' step selected. The left sidebar contains three options: 'Deployment Scenario', 'Select Groups', and 'Network Connectivity Assistant', with the latter being highlighted. The main area contains a description of the Network Connectivity Assistant (NCA) and a table for resources that validate connectivity to the internal network. Below the table are input fields for 'Helpdesk email address' and 'DirectAccess connection name', and a checkbox for 'Allow DirectAccess clients to use local name resolution'. At the bottom right, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Remote Access Setup

DirectAccess Client Setup
Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Deployment Scenario
Select Groups
Network Connectivity Assistant

The Network Connectivity Assistant (NCA) runs on DirectAccess client computers to provide DirectAccess connectivity information, diagnostics, and remediation support.

Resources that validate connectivity to internal network:

	Resource	Type
*		

Helpdesk email address:

DirectAccess connection name:

Allow DirectAccess clients to use local name resolution

< Back Next > Finish Cancel

Configuring the Network Connectivity Assistant

Configure Remote Clients

Configure Corporate Resources for NCA

Specify a corporate URL or FQDN that is always accessible to DirectAccess clients:

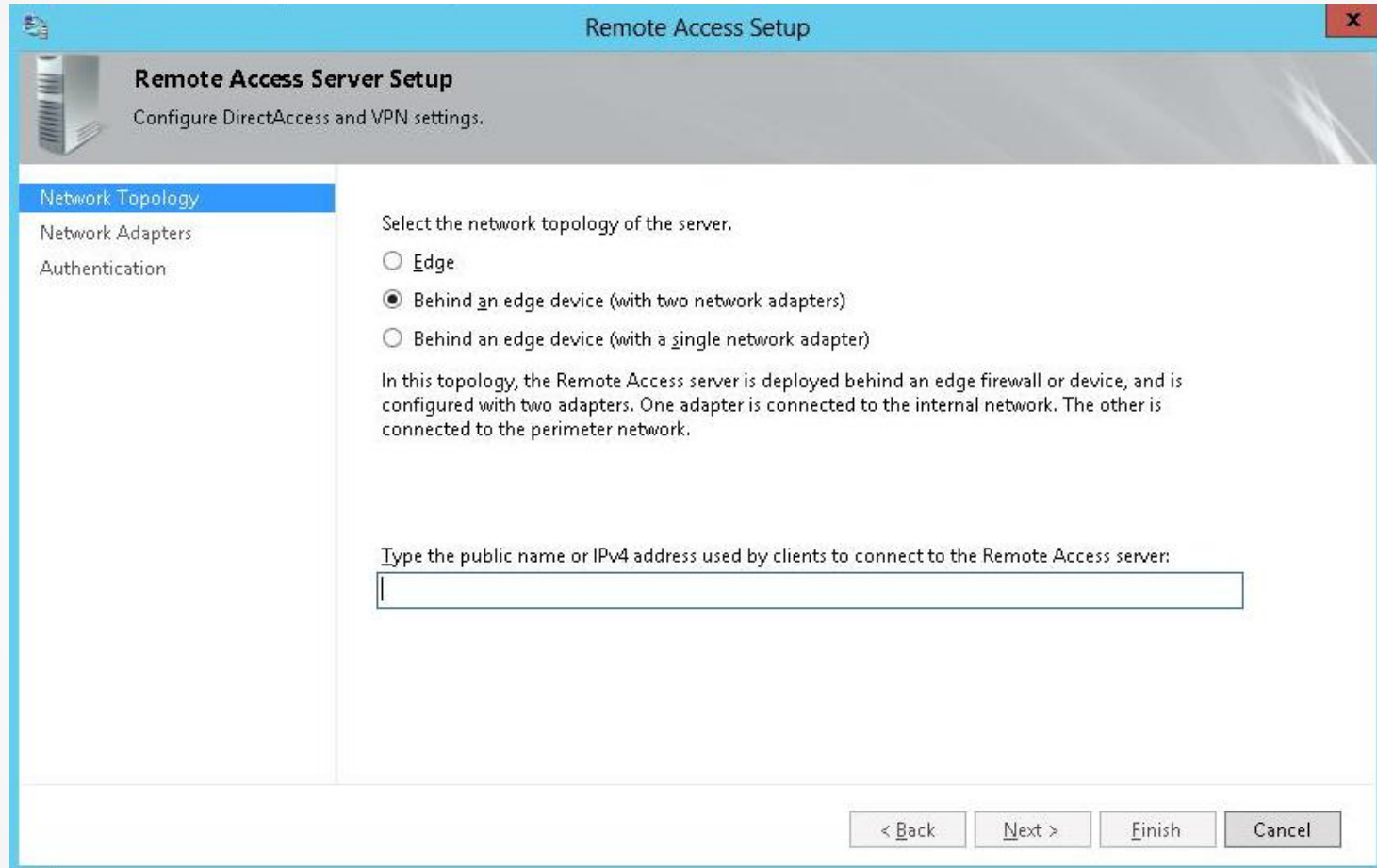
HTTP Validate

Examples: http://myserver.domain.com; myserver.domain.com

Add Cancel

Configuring corporate resources for NCA

Configure the DirectAccess Remote Access Server



Specifying the network topology

Configure the DirectAccess Remote Access Server

The screenshot shows the 'Remote Access Setup' wizard window. The title bar reads 'Remote Access Setup' with a close button. The main window has a header 'Remote Access Server Setup' with a sub-header 'Configure DirectAccess and VPN settings.' and a server icon. On the left is a navigation pane with 'Network Adapters' selected. The main area contains instructions to select network adapters for external and internal networks, with dropdown menus and 'Details...' buttons. Below that is a section for selecting a certificate to authenticate IP-HTTPS connections, with a checkbox and a 'Browse...' button. An information icon and message are at the bottom left. At the bottom right are '< Back', 'Next >', 'Finish', and 'Cancel' buttons.

Remote Access Setup

Remote Access Server Setup
Configure DirectAccess and VPN settings.

Network Topology
Network Adapters
Prefix Configuration
Authentication

Select the network adapters on the Remote Access server.

Adapter connected to the external network: Adapter connected to the internal network:

External Details... Internal Details...

2001:db8:85a3:42:0:8a2e:370:7334 2002:180a:1774:0:18e7:587c:888b:65cc

Select the certificate used to authenticate IP-HTTPS connections:

Use a self-signed certificate created automatically by DirectAccess

 Browse...

Transition technologies are enabled for IPv4 support.

< Back Next > Finish Cancel

Configuring the network adapters

Configure the DirectAccess Remote Access Server

The screenshot shows the 'Remote Access Setup' wizard window. The title bar reads 'Remote Access Setup'. The main window has a header 'Remote Access Server Setup' with the subtitle 'Configure DirectAccess and VPN settings.' On the left is a navigation pane with four items: 'Network Topology', 'Network Adapters', 'Prefix Configuration' (which is selected and highlighted in blue), and 'Authentication'. The main content area contains the following text: 'IPv6 settings displayed on this page have been detected on the internal network.' Below this, there are two configuration fields. The first is labeled 'Internal network IPv6 prefixes:' and contains a text box with the value '2002:180a:1774::/48' and an example below it: 'Example: 2001:db8:ef3e::/48;2001:db8:ef3f::/48'. The second is labeled 'IPv6 prefix assigned to DirectAccess client computers:' and contains a text box with the value '2002:180a:1774:1000::/64' and an example below it: 'Example: 2001:db8:ef3e:ad45::/64'. At the bottom right of the window are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Specifying the IPv6 prefixes

Configure the DirectAccess Remote Access Server

The screenshot shows the 'Remote Access Setup' window with the 'Authentication' step selected in the left-hand navigation pane. The main area contains instructions and configuration options for DirectAccess client authentication.

Remote Access Server Setup
Configure DirectAccess and VPN settings.

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 and Network Access Protection (NAP) compliance.

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

Enable Windows 7 client computers to connect via DirectAccess

Enforce corporate compliance for DirectAccess clients with NAP

< Back Next > Finish Cancel

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

The screenshot shows the 'Remote Access Setup' window with the 'Infrastructure Server Setup' step selected. The window title is 'Remote Access Setup' and it has a close button (X) in the top right corner. The main heading is 'Infrastructure Server Setup' with a sub-heading 'Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.' Below this, there is a left-hand navigation pane with the following items: 'Network Location Server' (highlighted), 'DNS', 'DNS Suffix Search List', and 'Management'. The main content area for 'Network Location Server' contains the following text: 'Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.' There are two radio button options: the first is selected and reads 'The network location server is deployed on a remote web server (recommended)', followed by the text 'Type in the URL of the network location server:' and an empty text box with a 'Validate' button to its right; the second option is unselected and reads 'The network location server is deployed on the Remote Access server', followed by the text 'Select the certificate used to authenticate the network location server:' and a 'Use a self-signed certificate' checkbox with an empty text box and a 'Browse...' button to its right. At the bottom of the main content area, there is an information icon (i) followed by the text: 'The network location server must be highly available to DirectAccess client computers inside the internal network, and inaccessible to DirectAccess clients located on the Internet. Clients must be able to contact the CRL for the site.' At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Specifying the Network Location server

Configure the DirectAccess Infrastructure Servers

The screenshot shows the 'Remote Access Setup' window, specifically the 'Infrastructure Server Setup' step. The window title is 'Remote Access Setup' with a close button (X) in the top right corner. Below the title bar, there is a header area with a server icon and the text 'Infrastructure Server Setup' and 'Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.'

On the left side, there is a navigation pane with the following items: 'Network Location Server', 'DNS' (highlighted in blue), 'DNS Suffix Search List Management', and 'Management'.

The main content area contains the following text: 'Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.'

Below this text is a table with two columns: 'Name Suffix' and 'DNS Server Address'. The table has three rows:

	Name Suffix	DNS Server Address
▶	contoso.com	2002:180a:1774:0:18e7:587c:888b:65cc
	Win2012Srv2.contoso.com	
*		

Below the table, there is a section titled 'Select a local name resolution option:' with three radio button options:

- Use local name resolution if the name does not exist in DNS (most restrictive)
- Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)
- Use local name resolution for any kind of DNS resolution error (least restrictive)

At the bottom right of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Specifying the DNS servers

Configure the DirectAccess Infrastructure Servers

Remote Access Setup

Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server
DNS
DNS Suffix Search List
Management

Add additional suffixes to search for short unqualified name in multiple locations. If a query fails for a suffix, the other suffixes are appended to the name and the DNS query is repeated for the alternate FQDN.

Configure DirectAccess clients with DNS client suffix search list

Detected domain suffixes:

Domain suffixes to use:

<Primary DNS suffix of client>
contoso.com

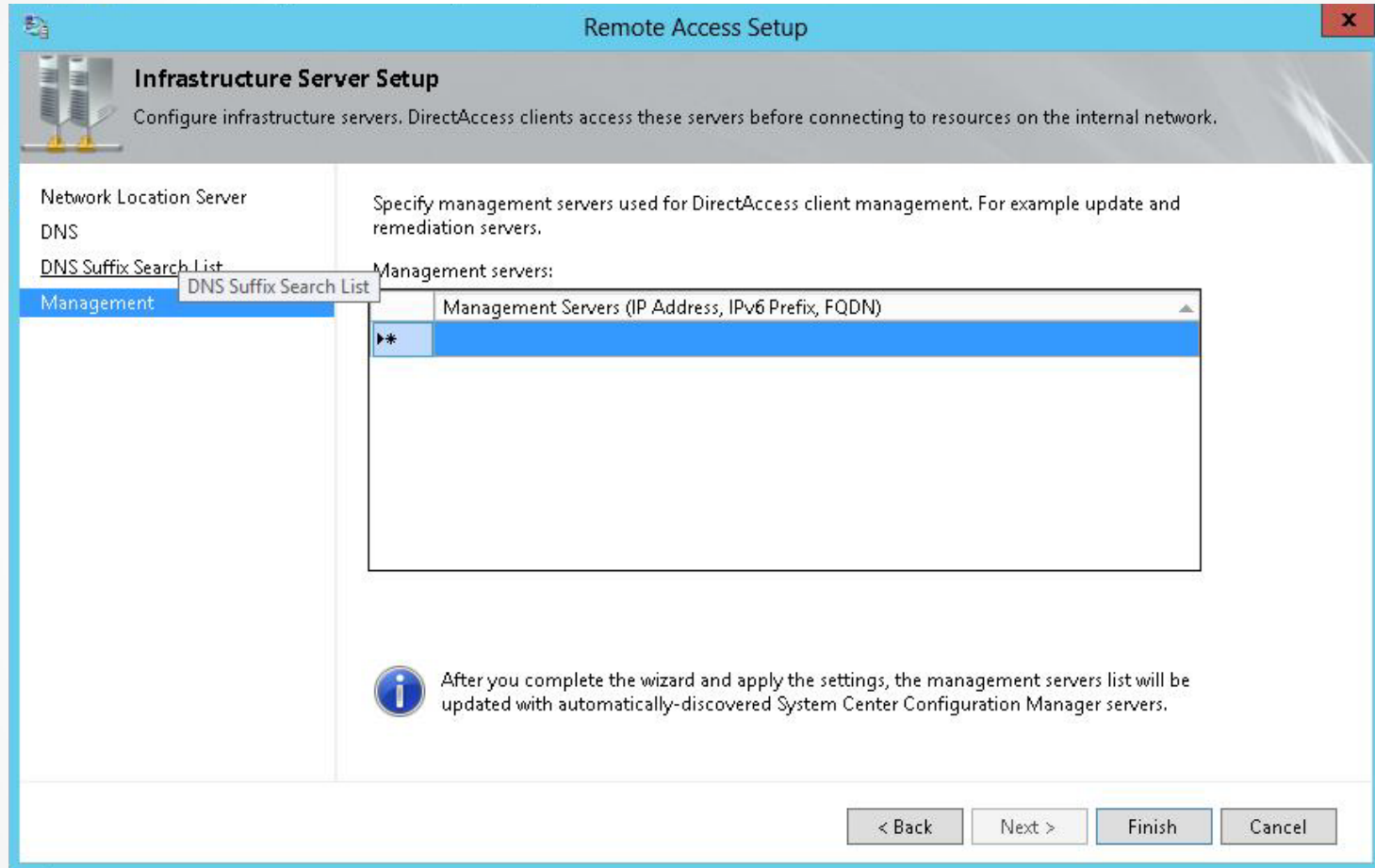
New Suffix:

i The primary domain DNS suffix appears first in the list.

< Back Next > Finish Cancel

Specifying the DNS Suffix Search List

Configure the DirectAccess Infrastructure Servers



Specifying the management servers

Configure the DirectAccess Infrastructure Servers

Specify the management server name or address.

Computer name (FQDN):

Example: engineeringcomputer1.contoso.com

Address (IPv4;IPv6; IPv6 prefix)

Example:

157.60.79.2

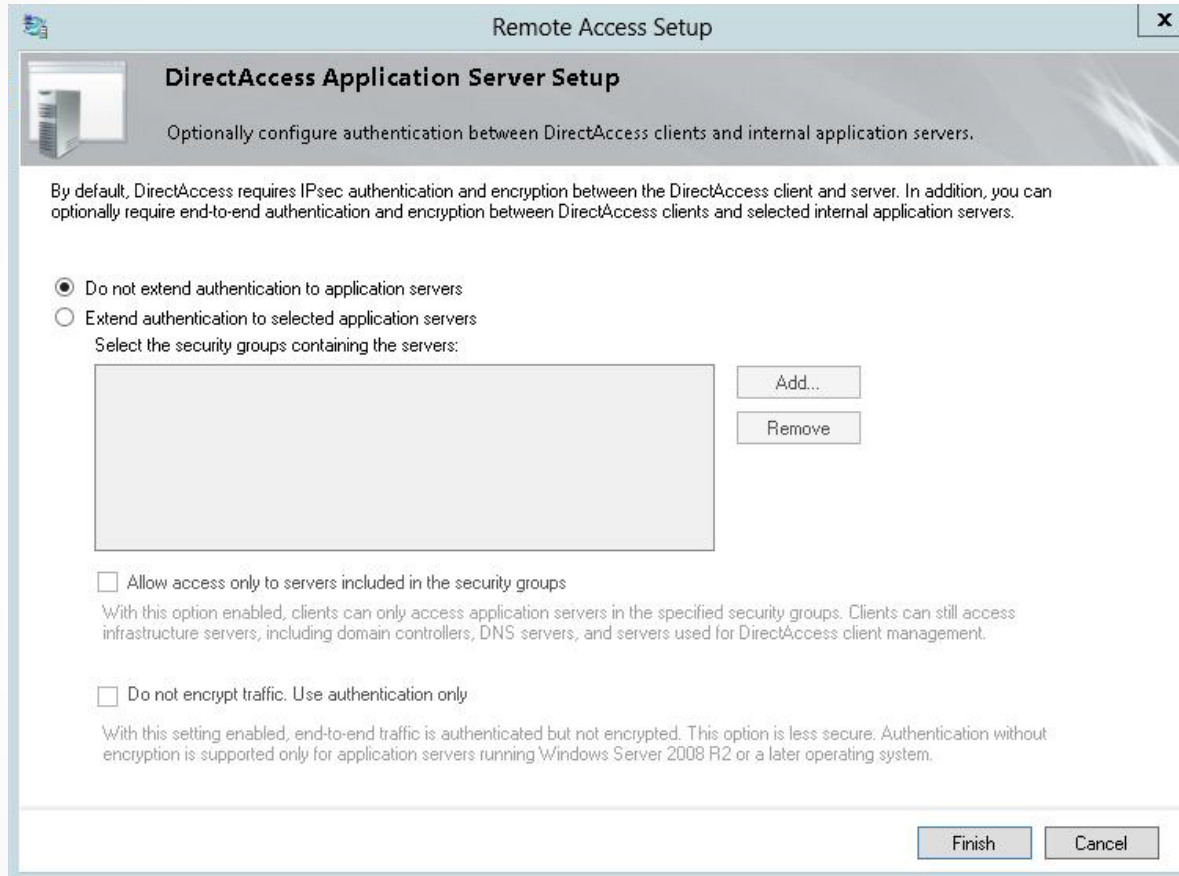
2001:db8:ef3e:ad45:208:74ff:fe39:6c43

2001:db8:ef3e:ad45:208:74ff:fe39:0/112

OK Cancel

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:

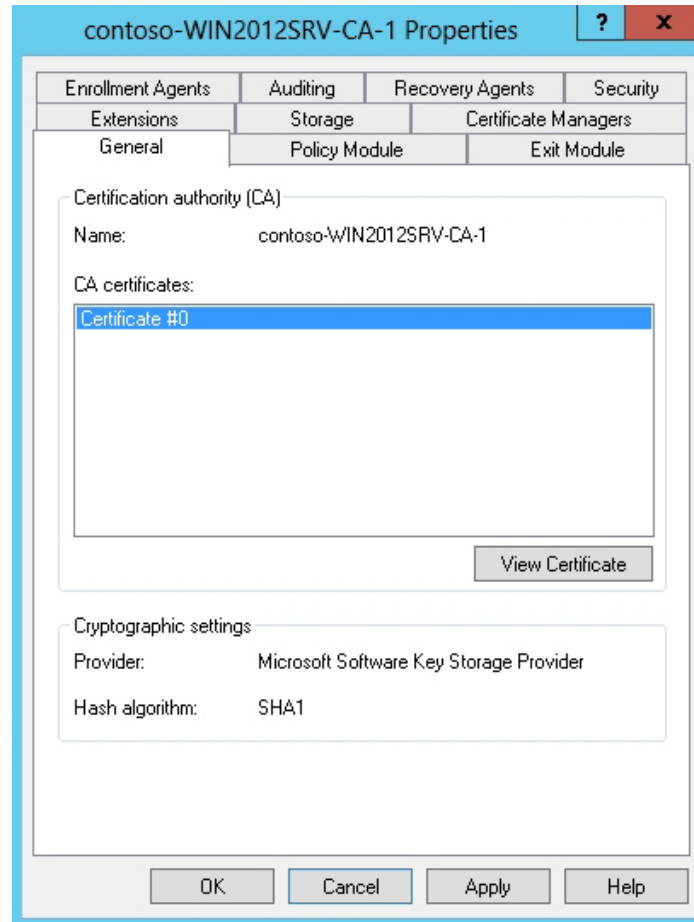
```
dnscmd /config /globalqueryblocklist  
isatap
```

Configuring Certificates for DirectAccess

The DirectAccess server requires these certificates:

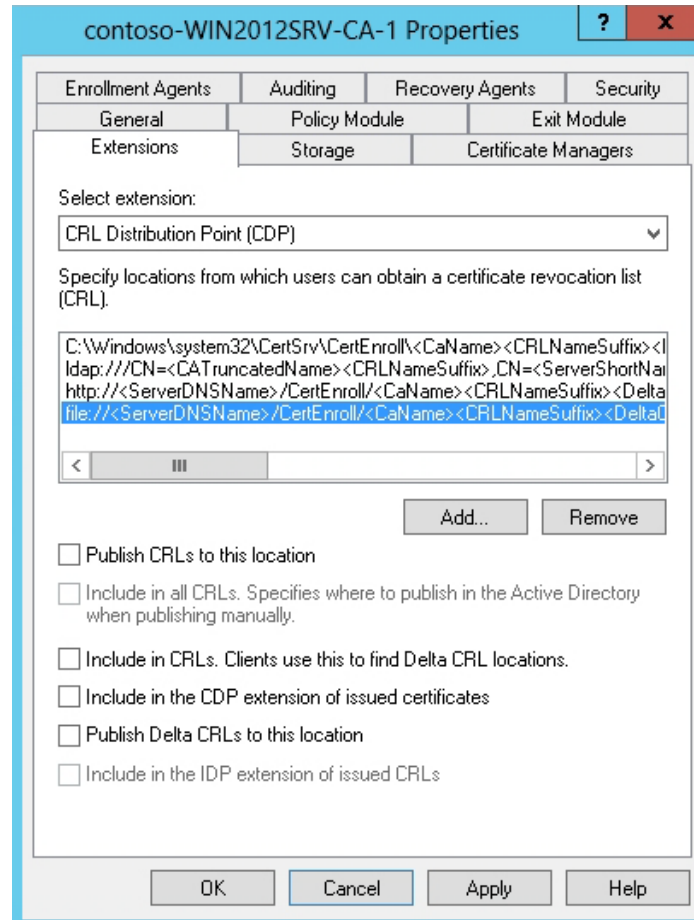
- The IP-HTTPS listener on the DirectAccess server requires a Web site certificate
- The DirectAccess client must be able to contact the server hosting the CRL for the certificate.
- The DirectAccess server requires a computer server to establish the IPsec connections with the DirectAccess clients.

Configure Certificate Requirements



Displaying the CA certificates

Configure Certificate Requirements



Specifying certificate extensions

Configure Certificate Requirements

Add Location [X]

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:
<CaName> [v] [Insert]

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

[<] [|||] [>]

[OK] [Cancel]

Adding a Location for CRL

Configure Certificate Requirements

Add Location [X]

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
http://crl.adatum.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>

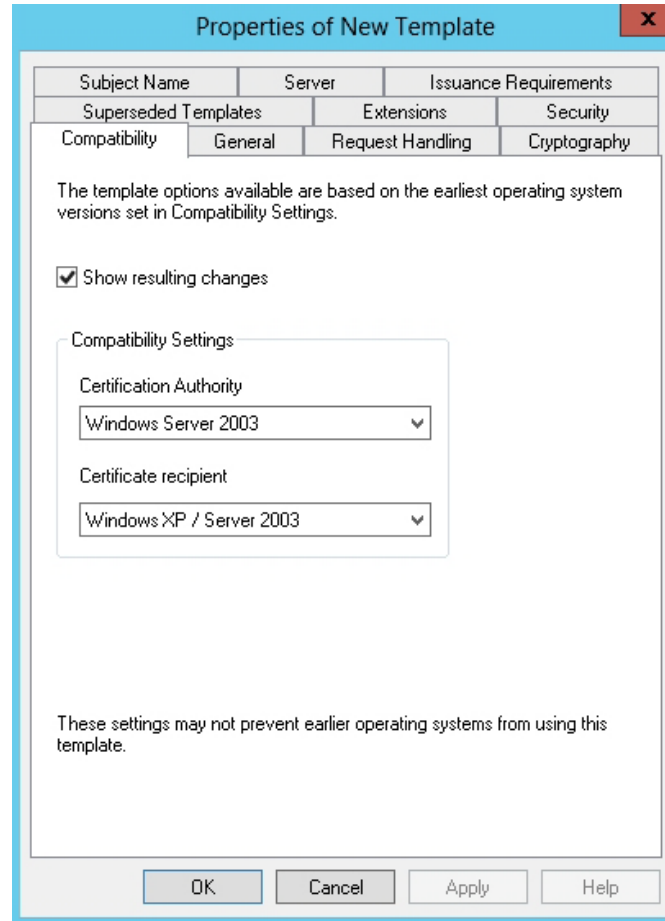
Variable:
<DeltaCRLAllowed> [Insert]

Description of selected variable:
Used in URLs and paths
Substitutes the Delta CRL file name suffix for the CRL file name suffix, if applicable
Example location: http://<ServerName>/CertEnroll/<CaName><CRLNameSuffix>

[OK] [Cancel]

An example location for CRL

Configure Certificate Requirements



Opening the properties of a certificate template

Configure Certificate Requirements

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
		Cryptography

Template display name:
Copy of Web Server

Template name:
Copy of Web Server

Validity period: 2 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

Defining the template display name and template name

Configure Certificate Requirements

Properties of New Template [X]

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
		Cryptography

Purpose:

Delete revoked or expired certificates (do not archive)

Include symmetric algorithms allowed by the subject

Archive subject's encryption private key

Authorize additional service accounts to access the private key (*)

Allow private key to be exported

Renew with the same key (*)

For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

Enroll subject without requiring any user input

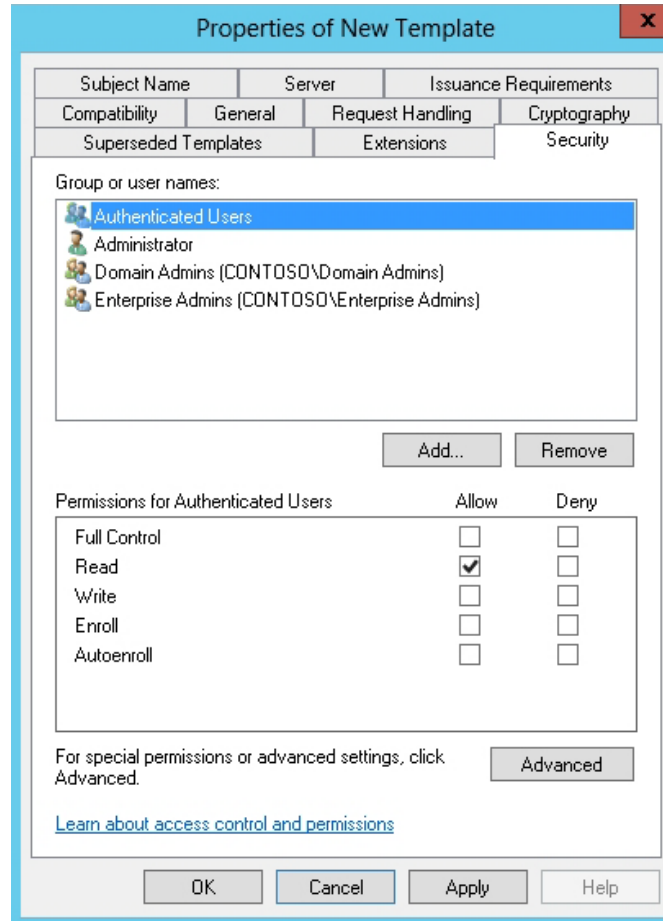
Prompt the user during enrollment

Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to [compatibility settings](#).

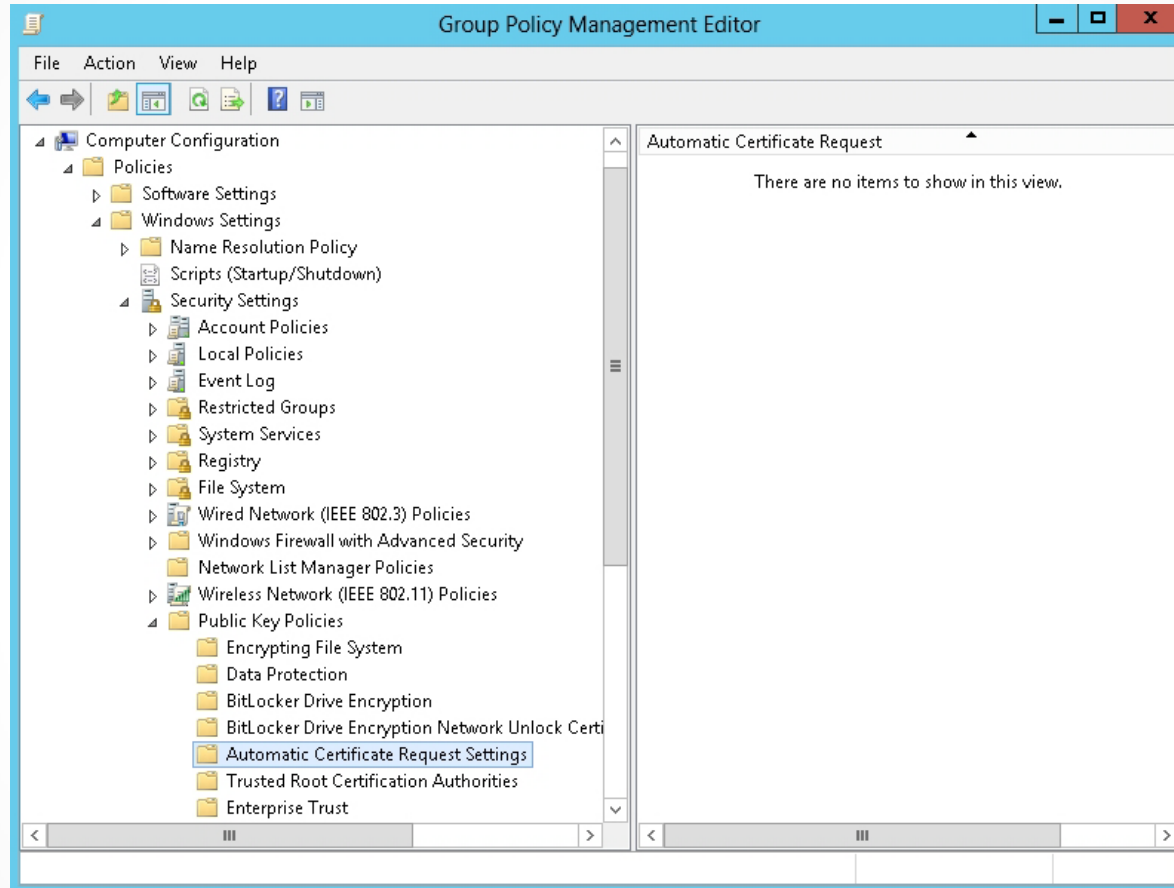
Specifying the purpose of the certificate

Configure Certificate Requirements



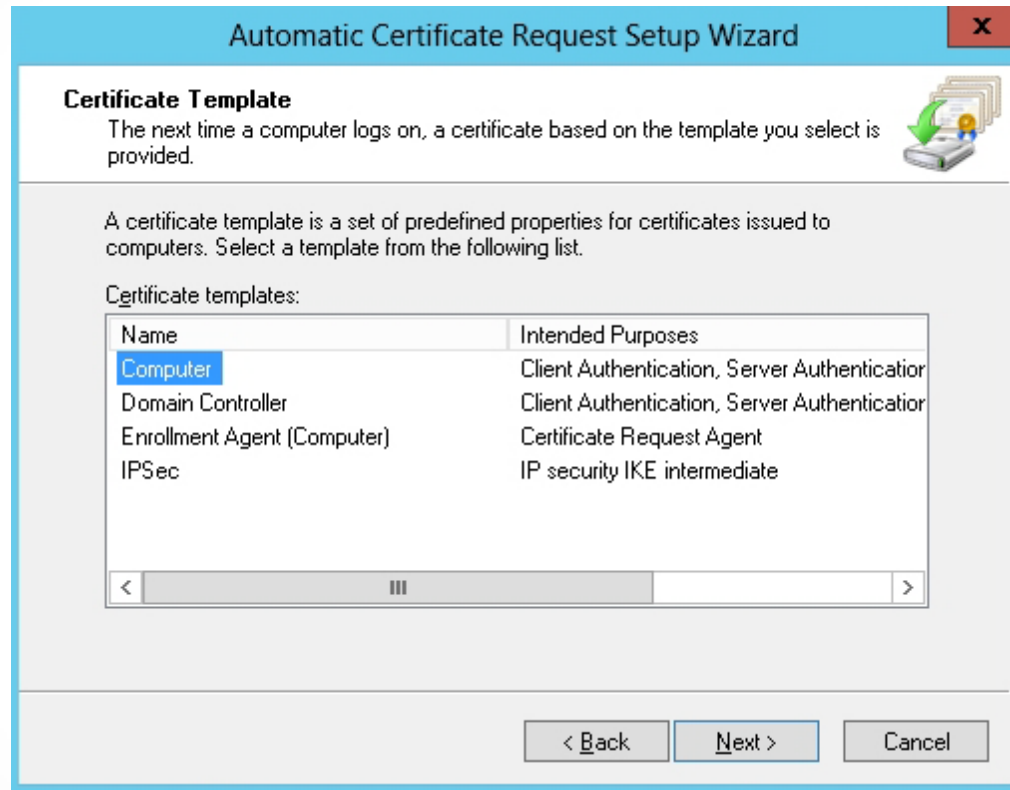
Specifying the permissions assigned to the certificate template

Configure Certificate Requirements



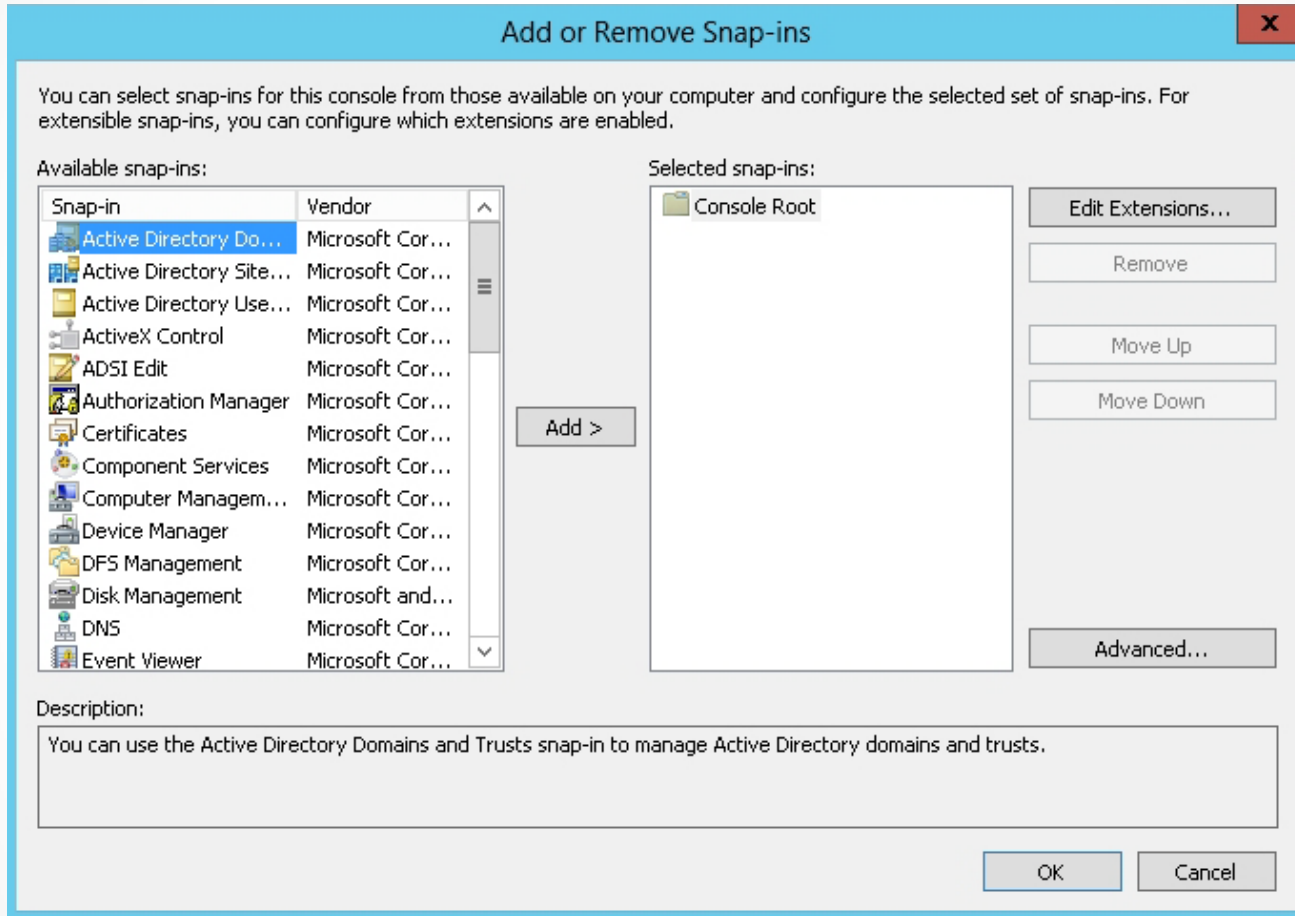
Viewing the Public Key policies

Configure Certificate Requirements



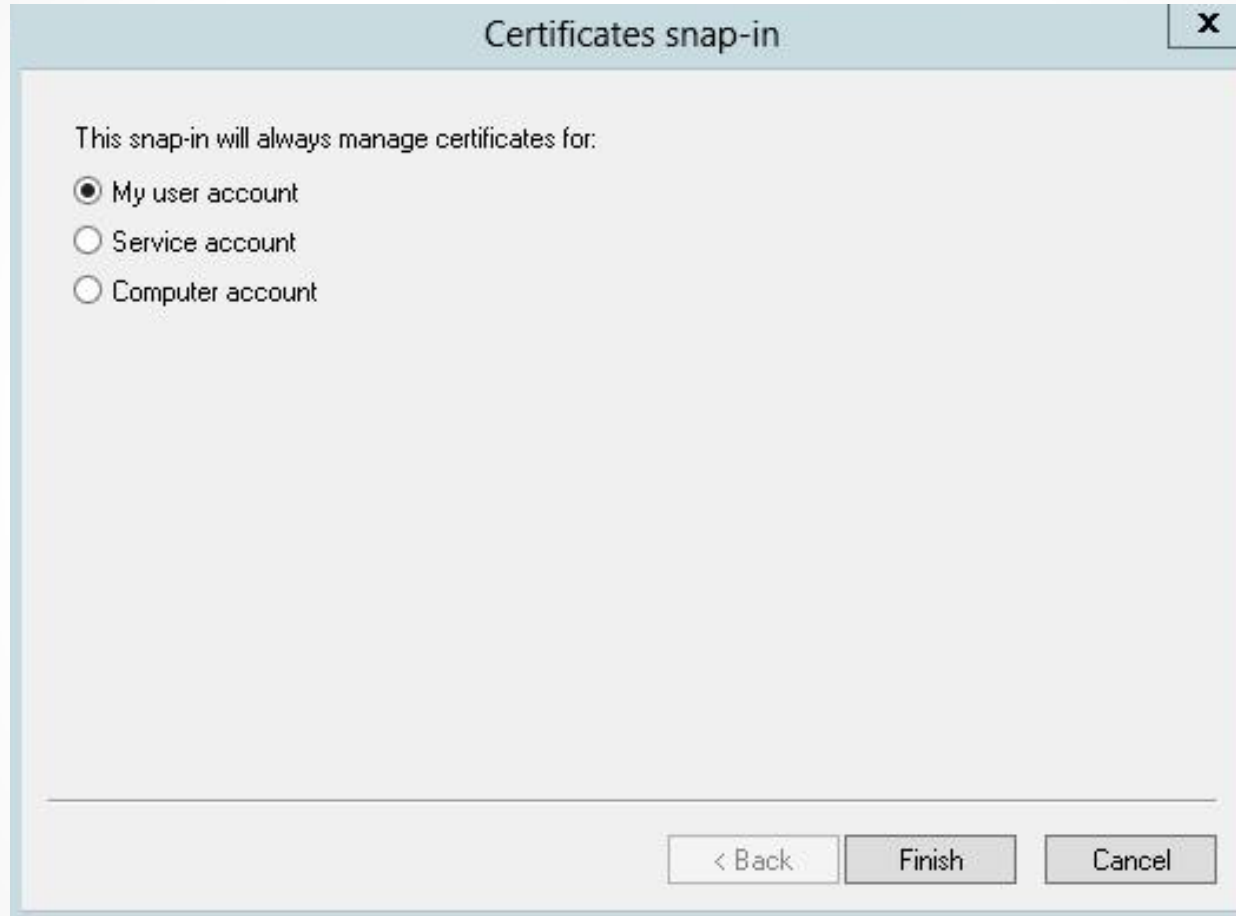
Specifying which certificates are automatically requested

Install a Digital Certificate on the Network Locator Server



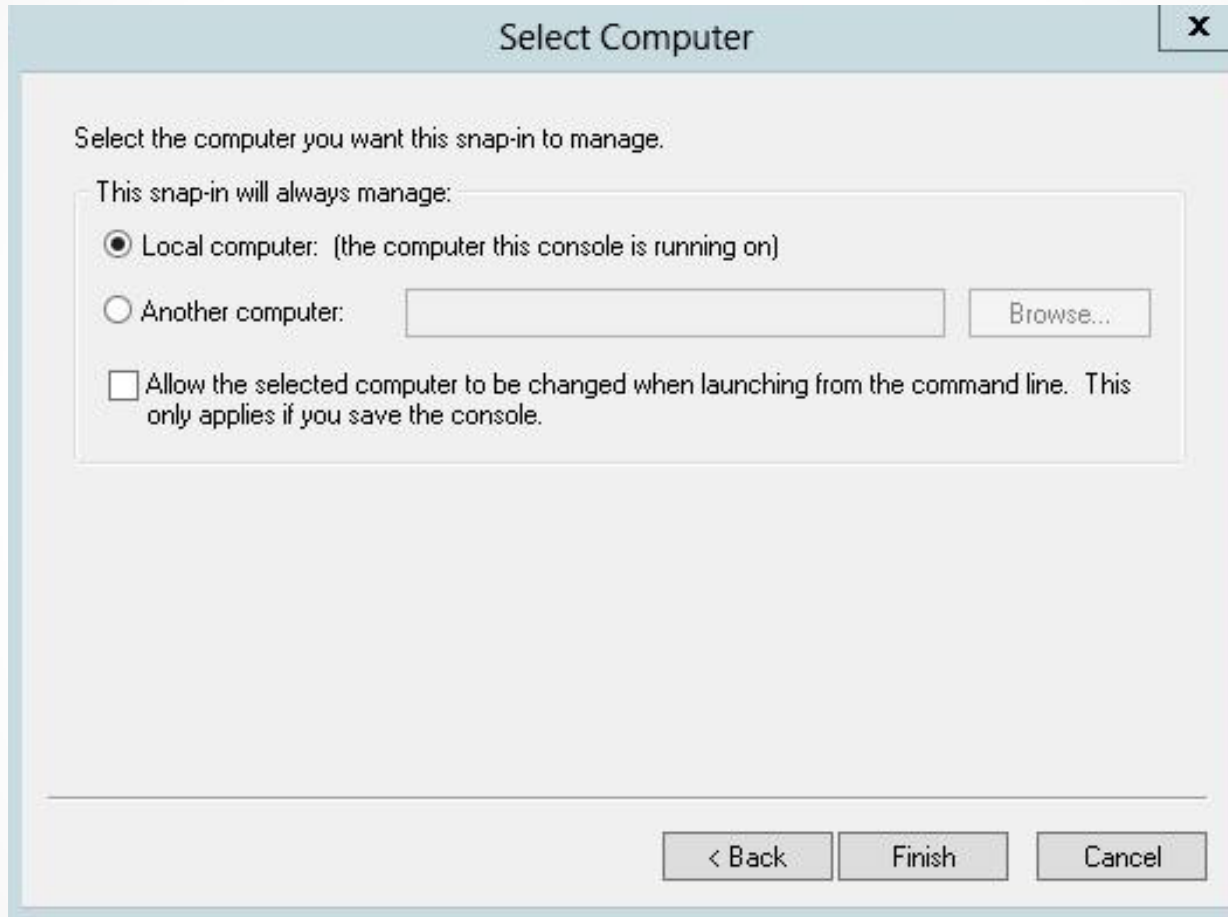
Opening the Add or Remove Snap-ins dialog box

Install a Digital Certificate on the Network Locator Server



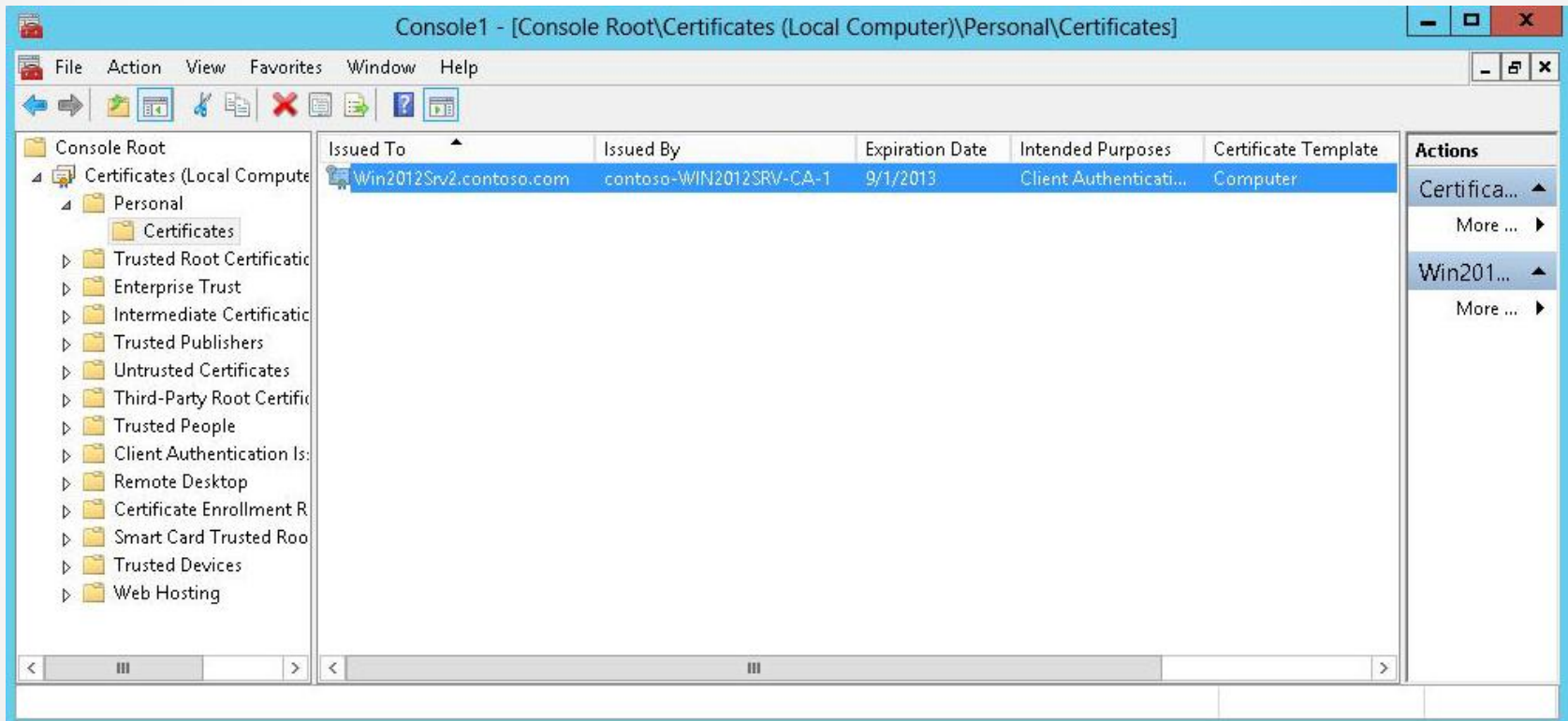
Specifying which certificates to manage

Install a Digital Certificate on the Network Locator Server



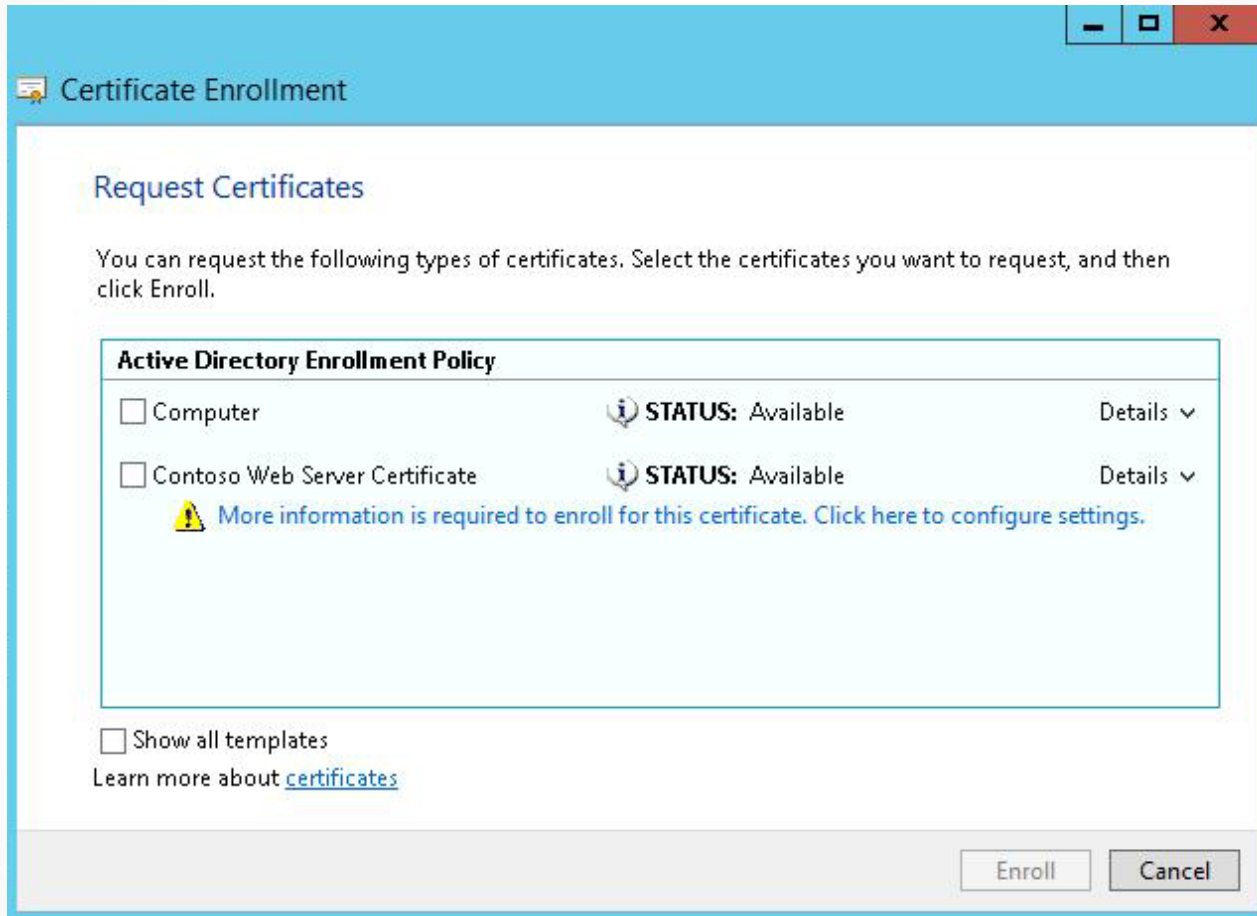
Selecting which computer to connect to

Install a Digital Certificate on the Network Locator Server



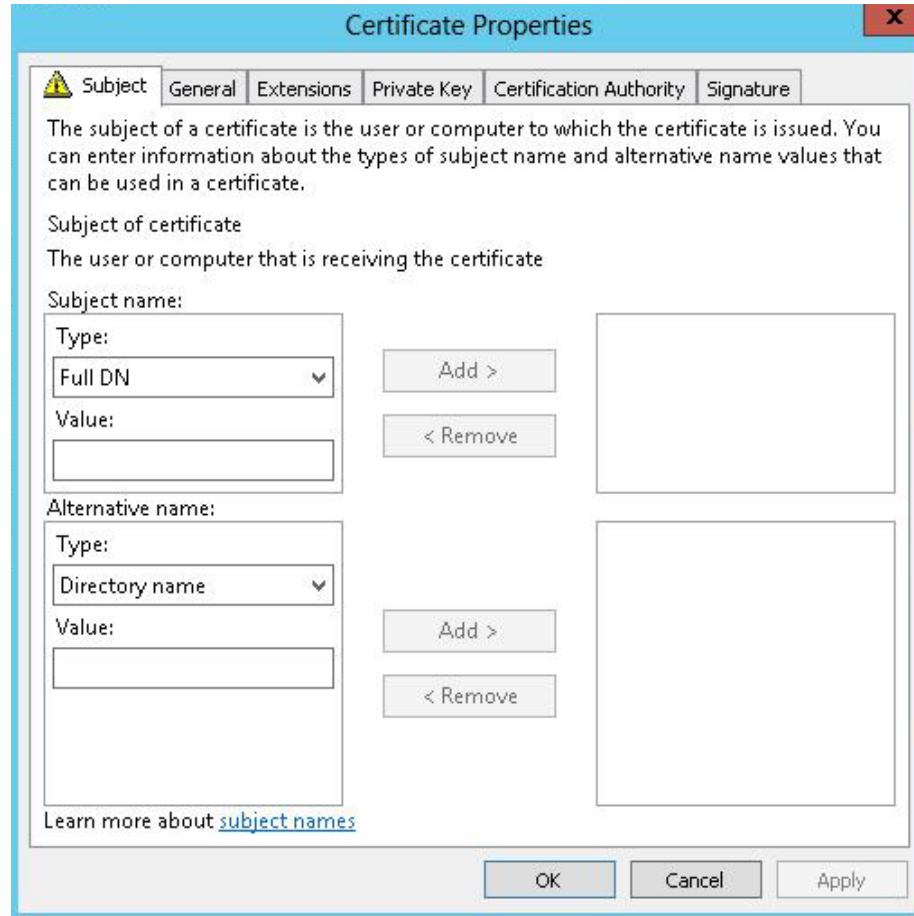
Viewing the computer certificate

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

Add Site Binding

Type: IP address: Port:

Host name:

Require Server Name Indication

SSL certificate:

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.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.